

Discipline: Computer Science and Engineering
Stream: CS4 (Computer Science and Information Security, Cyber Security, Cyber Forensics and Information Security, Information Security)

| | | | | | | |
|-----------|---------------------------|-------------------|---|---|---|--------|
| 221TCS100 | ADVANCED MACHINE LEARNING | CATEGORY | L | T | P | CREDIT |
| | | DISCIPLINE CORE 1 | 3 | 0 | 0 | 3 |

Preamble: This course introduces machine learning concepts and popular machine learning algorithms. It will cover the standard and most popular supervised learning algorithms including linear regression, logistic regression, decision trees, k-nearest neighbour, an introduction to Bayesian learning and the naive Bayes algorithm, support vector machines and kernels and basic clustering algorithms. Dimensionality reduction methods and some applications to real world problems will also be discussed. It helps the learners to develop application machine learning based solutions for real world applications.

Course Outcomes:

After the completion of the course the student will be able to:*

| | |
|------|---|
| CO 1 | Analyse the Machine Learning concepts, classifications of Machine Learning algorithms and basic parameter estimation methods. (Cognitive Knowledge Level: Analyse) |
| CO 2 | Illustrate the concepts of regression and classification techniques (Cognitive Knowledge Level: Apply) |
| CO 3 | Describe unsupervised learning concepts and dimensionality reduction techniques. (Cognitive Knowledge Level: Apply) |
| CO 4 | Explain Support Vector Machine concepts and graphical models. (Cognitive Knowledge Level: Apply) |
| CO 5 | Choose suitable model parameters for different machine learning techniques and to evaluate a model performance. (Cognitive Knowledge Level: Apply) |
| CO6 | Design, implement and analyse machine learning solution for a real world problem. (Cognitive Knowledge Level: Create) |

Program Outcomes (PO)

Outcomes are the attributes that are to be demonstrated by a graduate after completing the course.

PO1: An ability to independently carry out research/investigation and development work in engineering and allied streams

PO2: An ability to communicate effectively, write and present technical reports on complex engineering activities by interacting with the engineering fraternity and with society at large.

PO3: An ability to demonstrate a degree of mastery over the area as per the specialization of the program. The mastery should be at a level higher than the requirements in the appropriate bachelor program

PO4: An ability to apply stream knowledge to design or develop solutions for real world problems by following the standards

PO5: An ability to identify, select and apply appropriate techniques, resources and state-of-the-art tool to model, analyse and solve practical engineering problems.

PO6: An ability to engage in life-long learning for the design and development related to the stream related problems taking into consideration sustainability, societal, ethical and environmental aspects

PO7: An ability to develop cognitive load management skills related to project management and finance which focus on Entrepreneurship and Industry relevance.

Mapping of course outcomes with program outcomes

| | PO 1 | PO 2 | PO 3 | PO 4 | PO 5 | PO 6 | PO 7 |
|------|------|------|------|------|------|------|------|
| CO 1 | ☑ | | ☑ | | ☑ | ☑ | |
| CO 2 | ☑ | | ☑ | ☑ | ☑ | ☑ | |
| CO 3 | ☑ | | ☑ | ☑ | ☑ | ☑ | |
| CO 4 | ☑ | | ☑ | ☑ | ☑ | ☑ | |
| CO 5 | ☑ | | ☑ | ☑ | ☑ | ☑ | |
| CO 6 | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |

Assessment Pattern

| Bloom's Category | End Semester Examination |
|------------------|--------------------------|
| Apply | 60-80% |
| Analyse | 20-40% |
| Evaluate | |
| Create | |

Mark distribution

| Total Marks | CIE | ESE | ESE 2014 Duration |
|-------------|-----|-----|-------------------|
| 100 | 40 | 60 | 2.5 hours |

Continuous Internal Evaluation Pattern:

Evaluation shall only be based on application, analysis or design based questions (for both internal and end semester examinations).

Continuous Internal Evaluation : 40 marks

Micro project/Course based project : 20 marks

Course based task/Seminar/Quiz : 10 marks

Test paper, 1 no. : 10 marks

The project shall be done individually. Group projects not permitted.

Test paper shall include minimum 80% of the syllabus.

Course based task/test paper questions shall be useful in the testing of knowledge, skills, comprehension, application, analysis, synthesis, evaluation and understanding of the students.

End Semester Examination Pattern:

The end semester examination will be conducted by the University. There will be two parts; Part A and Part B. Part A contain 5 numerical questions with 1 question from each module, having 5 marks for each question. (such questions shall be useful in the testing of knowledge, skills, comprehension, application, analysis, synthesis, evaluation and understanding of the students). Students shall answer all questions.

Part B will contain 7 questions (such questions shall be useful in the testing of overall achievement and maturity of the students in a course, through long answer questions relating to theoretical/practical knowledge, derivations, problem solving and quantitative evaluation), with minimum one question from each module of which student should answer any five. Each question can carry 7 marks.

Total duration of the examination will be 150 minutes.

Course Level Assessment Questions

Course Outcome 1 (CO1):

1. Suppose that X is a discrete random variable with the following probability mass function: where $0 \leq \theta \leq 1$ is a parameter. The following 10 independent observations were taken from such a distribution: $(3, 0, 2, 1, 3, 2, 1, 0, 2, 1)$. What is the maximum likelihood estimate of θ .

| | | | | |
|--------|-------------|------------|-------------------|------------------|
| X | 0 | 1 | 2 | 3 |
| $P(X)$ | $2\theta/3$ | $\theta/3$ | $2(1 - \theta)/3$ | $(1 - \theta)/3$ |

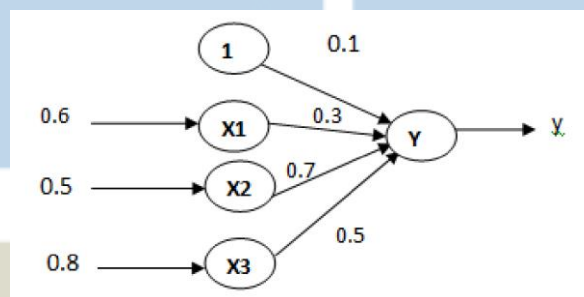
2. What is the difference between Maximum Likelihood estimation (MLE) and Maximum a Posteriori (MAP) estimation?
3. A gamma distribution with parameters α, β has the following density function, where $\Gamma(t)$ is the gamma function.

$$p(x) = \frac{\beta^\alpha}{\Gamma(\alpha)} x^{\alpha-1} e^{-\beta x}$$

If the posterior distribution is in the same family as the prior distribution, then we say that the prior distribution is the conjugate prior for the likelihood function. Using the Gamma distribution as a prior, show that the Exponential distribution is a conjugate prior of the Gamma distribution. Also, find the maximum a posteriori estimator for the parameter of the Exponential distribution as a function of α and β .

Course Outcome 2 (CO2)

1. How can we interpret the output of a two-class logistic regression classifier as a probability?
2. Calculate the output of the following neuron Y if the activation function is a binary sigmoid.



3. Suppose you have a 3-dimensional input $x = (x_1, x_2, x_3) = (2, 2, 1)$ fully connected with weights $(0.5, 0.3, 0.2)$ to one neuron which is in the hidden layer with sigmoid activation function. Calculate the output of the hidden layer neuron.
4. Consider the case of the XOR function in which the two points $\{(0, 0), (1, 1)\}$ belong to one class, and the other two points $\{(1, 0), (0, 1)\}$ belong to the other class. Design a multilayer perceptron for this binary classification problem.
5. Why does a single perceptron cannot simulate simple XOR function? Explain how this limitation is overcome?
6. Consider a naive Bayes classifier with 3 boolean input variables, **X1**, **X2** and **X3**, and one boolean output, **Y**. How many parameters must be estimated to train such a naive Bayes classifier? How many parameters would have to be estimated to learn the above classifier if we do not make the naive Bayes conditional independence assumption?

Course Outcome 3(CO3):

1. Describe the basic operation of k-means clustering.
2. A Poisson distribution is used to model data that consists of non-negative integers. Suppose you observe m integers in your training set. Your model assumption is that each integer is sampled from one of two different Gaussian distributions. You would like to learn this model using the EM algorithm. List all the parameters of the model. Derive the E-step and M-step for this model.
3. A uni-variate Gaussian distribution is used to model data that consists of non-negative integers. Suppose you observe m integers in your training set. Your model assumption is that each integer is sampled from one of two different Gaussian distributions. You would like to learn this model using the EM algorithm. List all the parameters of the model. Derive the E-step and M-step for the model.
4. Suppose you want to cluster the eight points shown below using k -means

| | A_1 | A_2 |
|-------|-------|-------|
| x_1 | 2 | 10 |
| x_2 | 2 | 5 |
| x_3 | 8 | 4 |
| x_4 | 5 | 8 |
| x_5 | 7 | 5 |
| x_6 | 6 | 4 |
| x_7 | 1 | 2 |
| x_8 | 4 | 9 |

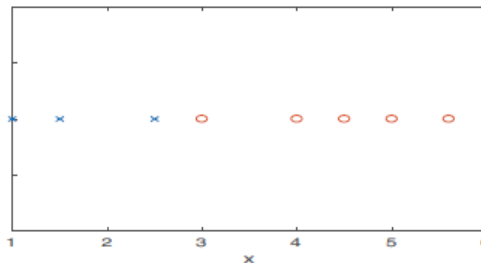
Assume that $k = 3$ and that initially the points are assigned to clusters as follows:

$C1 = \{x_1, x_2, x_3\}$, $C2 = \{x_4, x_5, x_6\}$, $C3 = \{x_7, x_8\}$. Apply the k -means algorithm until convergence, using the Manhattan distance.

Course Outcome 4 (CO4):

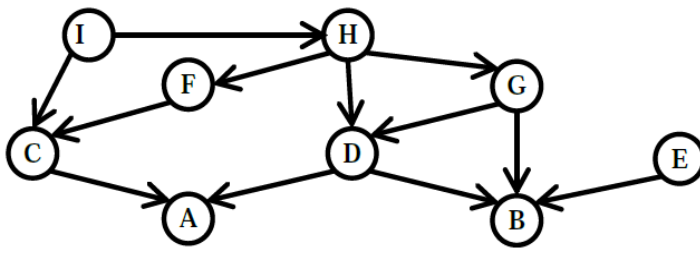
1. Describe how Support Vector Machines can be extended to make use of kernels. Illustrate with reference to the Gaussian kernel $K(x, y) = e^{-y}$, where $y = (x-y)^2$.
2. Suppose that you have a linear support vector machine(SVM) binary classifier. Consider a point that is currently classified correctly, and is far away from the decision boundary. If you remove the point from the training set, and re-train the classifier, will the decision boundary change or stay the same? Justify your answer.
3. What is the primary motivation for using the kernel trick in machine learning algorithms?

4. Show that the Boolean function $(x_1 \wedge x_2) \vee (\neg x_1 \wedge \neg x_2)$ is not linearly separable (i.e. there is no linear classifier $\text{sign}(w_1 x_1 + w_2 x_2 + b)$ that classifies all 4 possible input points correctly). Assume that “true” is represented by 1 and “false” is represented by -1. Show that there is a linear separator for this Boolean function when we use the kernel $K(x, y) = (x \cdot y)^2$ ($x \cdot y$ denotes the ordinary inner product) . Give the weights and the value of b for one such separator.
5. Consider the following one dimensional training data set, 'x' denotes negative examples and 'o' positive examples. The exact data points and their labels are given in the table. Suppose a SVM is used to classify this data. Indicate which are the support vectors and mark the decision boundary. Give the value of the cost function and of the model parameters after training.



| | | | | | | | | |
|---|----|-----|-----|---|---|-----|---|-----|
| x | 1 | 1.5 | 2.5 | 3 | 4 | 4.5 | 5 | 5.6 |
| y | -1 | -1 | -1 | 1 | 1 | 1 | 1 | 1 |

6. Write down the factored conditional probability expression that corresponds to the graphical Bayesian Network shown below.



7. How do we learn the conditional probability tables(CPT) in Bayesian networks if information about some variables is missing? How are these variables called?

Course Outcome 5 (CO5):

- Suppose 10000 patients get tested for flu; out of them, 9000 are actually healthy and 1000 are actually sick. For the sick people, a test was positive for 620 and negative for 380. For healthy people, the same test was positive for 180 and negative for 8820. Construct a confusion matrix for the data and compute the accuracy, precision and recall for the data.
- Given the following data, construct the ROC curve of the data. Compute the AUC.

| Thres hold | TP | TN | FP | FN |
|------------|----|----|----|----|
| 1 | 0 | 25 | 0 | 29 |
| 2 | 7 | 25 | 0 | 22 |
| 3 | 18 | 24 | 1 | 11 |
| 4 | 26 | 20 | 5 | 3 |
| 5 | 29 | 11 | 14 | 0 |
| 6 | 29 | 0 | 25 | 0 |
| 7 | 29 | 0 | 25 | 0 |

3. With an example classification problem, explain the following terms: a) Hyper parameters b) Training set c) Validation sets d) Bias e) Variance.
4. What is ensemble learning? Can ensemble learning using linear classifiers learn classification of linearly non-separable sets?
5. Describe boosting. What is the relation between boosting and ensemble learning?
6. Classifier A attains 100% accuracy on the training set and 70% accuracy on the test set. Classifier B attains 70% accuracy on the training set and 75% accuracy on the test set. Which one is a better classifier. Justify your answer.
7. What are ROC space and ROC curve in machine learning? In ROC space, which points correspond to perfect prediction, always positive prediction and always negative prediction? Why?
8. Suppose there are three classifiers A,B and C. The (FPR, TPR) measures of the three classifiers are as follows – A (0, 1), B (1, 1) , C (1,0.5). Which can be considered as a perfect classifier? Justify your answer.
9. What does it mean for a classifier to have a high precision but low recall?

Model Question Paper

QP CODE:

Reg No: _____

Name: _____

PAGES : 4

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

FIRST SEMESTER M.TECH DEGREE EXAMINATION, MONTH & YEAR

Course Code: 221TCS100

Course Name: ADVANCED MACHINE LEARNING

Max. Marks : 60

Duration: 2.5 Hours

PART A

Answer All Questions. Each Question Carries 5 Marks

1. Explain the principle of the gradient descent algorithm.
2. In a two-class logistic regression model, the weight vector $\mathbf{w} = [4, 3, 2, 1, 0]$. We apply it to some object that we would like to classify; the vectorized feature representation of this object is $\mathbf{x} = [-2, 0, -3, 0.5, 3]$. What is the probability, according to the model, that this instance belongs to the positive class?
3. Expectation maximization (EM) is designed to find a maximum likelihood setting of the parameters of model when some of the data is missing. Does the algorithm converge? If so, do you obtain a locally or globally optimal set of parameters?
4. What is the basic idea of a Support Vector Machine?
5. What is the trade-off between bias and variance? (5x5=25)

Part B

(Answer any five questions. Each question carries 7 marks)

6. Suppose x_1, \dots, x_n are independent and identically distributed(iid) samples from a distribution with density (7)

$$f_X(x|\theta) = \begin{cases} \frac{\theta x^{\theta-1}}{3^\theta}, & 0 \leq x \leq 3 \\ 0, & \text{otherwise} \end{cases}$$

Find the maximum likelihood estimate (MLE) for θ .

7. Derive the gradient descent training rule assuming for the target function $o_d = w_0 + w_1 x_1 + \dots + w_n x_n$. Define explicitly the squared cost/error function E , assuming that a set of training examples D is provided, where each training example $d \in D$ is associated with the target output t_d . (7)

8. Cluster the following eight points representing locations into three clusters: (7)
 $A1(2, 10), A2(2, 5), A3(8, 4), A4(5, 8), A5(7, 5), A6(6, 4), A7(1, 2), A8(4, 9)$.

Initial cluster centers are: $A1(2, 10), A4(5, 8)$ and $A7(1, 2)$.

The distance function between two points $a = (x1, y1)$ and $b = (x2, y2)$ is defined as $D(a, b) = |x2 - x1| + |y2 - y1|$

Use **k**-Means Algorithm to find the three cluster centers after the second iteration.

9. Describe Principal Component Analysis. What criterion does the method minimize? What is the objective of the method? Give a way to compute the solution from a matrix X encoding the features. (7)

10. Consider a support vector machine whose input space is 2-D, and the inner products are computed by means of the kernel $K(x, y) = (x \cdot y + 1)^2 - 1$ ($x \cdot y$ denotes the ordinary inner product). Show that the mapping to feature space that is implicitly defined by this kernel is the mapping to 5-D given by (7)

$$\mathbf{x} = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \rightarrow \phi(\mathbf{x}) = \begin{bmatrix} x_1^2 \\ x_2^2 \\ \sqrt{2} x_1 x_2 \\ \sqrt{2} x_1 \\ \sqrt{2} x_2 \end{bmatrix} .$$

11. How does random forest classifier work? Why is a random forest better than a decision tree? (7)



12. Consider a two-class classification problem of predicting whether a photograph contains a man or a woman. Suppose we have a test dataset of 10 records with expected outcomes and a set of predictions from our classification algorithm. Compute the confusion matrix, accuracy, precision, recall, sensitivity and specificity on the following data. (7)

| Sl.No. | Actual | Predicted |
|--------|--------|-----------|
| 1 | man | woman |
| 2 | man | man |
| 3 | woman | woman |
| 4 | man | man |
| 5 | man | woman |
| 6 | woman | woman |
| 7 | woman | man |
| 8 | man | man |
| 9 | man | woman |
| 10 | woman | woman |

Syllabus

Module-1 (Parameter Estimation and Regression) 8 hours

Overview of machine learning: supervised, semi-supervised, unsupervised learning, reinforcement learning. Basics of parameter estimation: Maximum Likelihood Estimation (MLE), Maximum a Posteriori Estimation (MAP). Gradient Descent Algorithm, Batch Gradient Descent, Stochastic Gradient Descent. Regression algorithms: least squares linear regression, normal equations and closed form solution, Polynomial regression.

Module-2 (Regularization techniques and Classification algorithms) 9 hours

Overfitting, Regularization techniques - LASSO and RIDGE. Classification algorithms: linear and non-linear algorithms, Perceptrons, Logistic regression, Naive Bayes, Decision trees. Neural networks: Concept of Artificial neuron, Feed-Forward Neural Network, Back propagation algorithm.

Module-3 (Unsupervised learning) 8 hours

Unsupervised learning: clustering, k-means, Hierarchical clustering, Principal component analysis,

Density-based spatial clustering of applications with noise (DBSCAN). Gaussian mixture models: Expectation Maximization (EM) algorithm for Gaussian mixture model.

Module-4 (Support Vector Machine and Graphical Models) 7 hours

Support vector machines and kernels: Max margin classification, Nonlinear SVM and the kernel trick, nonlinear decision boundaries, Kernel functions. Basics of graphical models - Bayesian networks, Hidden Markov model - Inference and estimation.

Module-5 (Evaluation Metrics and Sampling Methods) 8 hours

Classification Performance Evaluation Metrics: Accuracy, Precision, Precision, Recall, Specificity, False Positive Rate (FPR), F1 Score, Receiver Operator Characteristic (ROC) Curve, AUC. Regression Performance Evaluation Metrics: Mean Absolute Error (MAE), Root Mean Squared Error (RMSE), R Squared/Coefficient of Determination. Clustering Performance Evaluation Metrics: Purity, Jaccard index, Normalized Mutual Information, Clustering Accuracy, Silhouette Coefficient, Dunn’s Index. Boosting: AdaBoost, gradient boosting machines. Resampling methods: cross-validation, bootstrap. Ensemble methods: bagging, boosting, random forests Practical aspects in machine learning: data preprocessing, overfitting, accuracy estimation, parameter and model selection Bias-Variance tradeoff

Course Plan

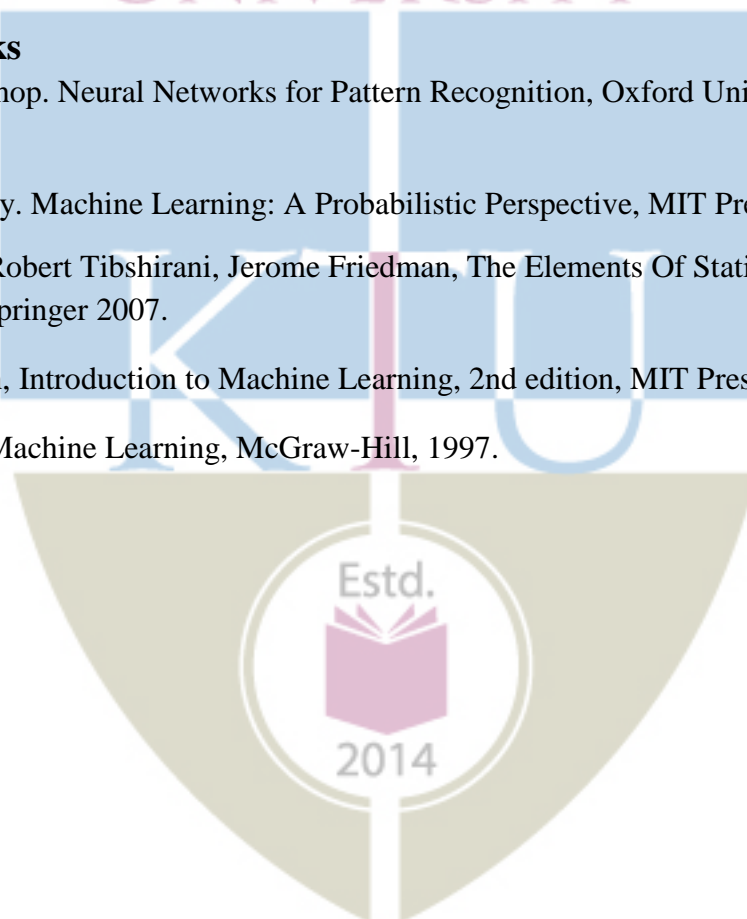
| No | Topics | No. of Lectures (40) |
|-----|---|----------------------|
| 1 | Module-1 (Parameter Estimation and Regression) 8 hours | |
| 1.1 | Overview of machine learning: supervised, semi-supervised, unsupervised learning, reinforcement learning. | 1 |
| 1.2 | Basics of parameter estimation: Maximum Likelihood Estimation (MLE) | 1 |
| 1.3 | Basics of parameter estimation: Maximum Likelihood Estimation (MLE) - Examples | 1 |
| 1.4 | Basics of parameter estimation: Maximum a Posteriori Estimation (MAP) | 1 |
| 1.5 | Basics of parameter estimation: Maximum a Posteriori Estimation (MAP) - Example | 1 |
| 1.6 | Gradient Descent Algorithm, Batch Gradient Descent, Stochastic Gradient Descent | 1 |
| 1.7 | Regression algorithms: least squares linear regression, normal equations and closed form solution | 1 |
| 1.8 | Polynomial regression | 1 |
| 2 | Module-2 (Regularization techniques and Classification algorithms) 9 hours | |

| | | |
|-----|--|--|
| 2.1 | Overfitting, Regularization techniques - LASSO and RIDGE | |
| 2.2 | Classification algorithms: linear and non-linear algorithms | |
| 2.3 | Perceptrons | |
| 2.4 | Logistic regression | |
| 2.5 | Naive Bayes | |
| 2.6 | Decision trees | |
| 2.7 | Neural networks: Concept of Artificial neuron | |
| 2.8 | Feed-Forward Neural Network | |
| 2.9 | Back propagation algorithm | |
| 3 | Module-3 (Unsupervised learning) 8 hours | |
| 3.1 | Unsupervised learning: clustering, k-means | |
| 3.2 | Hierarchical clustering | |
| 3.3 | Principal component analysis | |
| 3.4 | Density-based spatial clustering of applications with noise (DBSCAN) | |
| 3.5 | Gaussian mixture models: Expectation Maximization (EM) algorithm for Gaussian mixture model | |
| 3.6 | Gaussian mixture models: Expectation Maximization (EM) algorithm for Gaussian mixture model | |
| 4 | Module-4 (Support Vector Machine and Graphical Models) 7 hours | |
| 4.1 | Support vector machines and kernels: Max margin classification | |
| 4.2 | Support vector machines: Max margin classification | |
| 4.3 | Nonlinear SVM and the kernel trick, nonlinear decision boundaries | |
| 4.3 | Kernel functions | |
| 4.5 | Basics of graphical models - Bayesian networks | |
| 4.6 | Hidden Markov model - Inference and estimation | |
| 4.7 | Hidden Markov model - Inference and estimation | |
| 4.8 | Hidden Markov model - Inference and estimation | |
| 5 | Module-5 (Evaluation Metrics and Sampling Methods) 8 hours | |
| 5.1 | Classification Performance Evaluation Metrics: Accuracy, Precision, Precision, Recall, Specificity, False Positive Rate (FPR), F1 Score, Receiver Operator Characteristic (ROC) Curve, AUC | |
| 5.2 | Regression Performance Evaluation Metrics: Mean Absolute Error | |

| | | |
|-----|--|--|
| | (MAE), Root Mean Squared Error (RMSE), R Squared/Coefficient of Determination | |
| 5.3 | Clustering Performance Evaluation Metrics: Purity, Jaccard index, Normalized Mutual Information, Clustering Accuracy, Silhouette Coefficient, Dunn's Index | |
| 5.4 | Boosting: AdaBoost, gradient boosting machines. | |
| 5.5 | Resampling methods: cross-validation, bootstrap. | |
| 5.6 | Ensemble methods: bagging, boosting, random forests | |
| 5.7 | Practical aspects in machine learning: data preprocessing, overfitting, accuracy estimation, parameter and model selection | |
| 5.8 | Bias-Variance tradeoff | |

Reference Books

1. Christopher Bishop. Neural Networks for Pattern Recognition, Oxford University Press, 1995.
2. Kevin P. Murphy. Machine Learning: A Probabilistic Perspective, MIT Press 2012.
3. Trevor Hastie, Robert Tibshirani, Jerome Friedman, The Elements Of Statistical Learning, Second edition Springer 2007.
4. Ethem Alpaydin, Introduction to Machine Learning, 2nd edition, MIT Press 2010.
5. Tom Mitchell, Machine Learning, McGraw-Hill, 1997.



| | | | | | | |
|-----------|--------------------------------|-------------------|---|---|---|--------|
| 221TCS007 | FOUNDATIONS OF CRYPTOGRAPHY | CATEGORY | L | T | P | CREDIT |
| | | Program Core 1 | 3 | 0 | 0 | 3 |

Preamble:

The focus of this course will be on definitions and constructions of various cryptographic objects using the concepts of Integer & Modular Arithmetic, Primes & Congruence's, Discrete Logarithms & Elliptic Curve Arithmetic and Graph Theory.

Course Outcomes:

After the completion of the course the student will be able to

| | |
|-------------|---|
| CO 1 | Use the operations and properties of algebraic structures, integer arithmetic, modular arithmetic and polynomial arithmetic in solving problems (Cognitive Knowledge Level: Apply) |
| CO 2 | Develop problem analysing and solving capabilities by learning the operations of Prime numbers, Primitive Roots and related theorems. (Cognitive Knowledge Level: Apply) |
| CO 3 | Examine the concept of Linear congruence and Discrete logarithms. (Cognitive Knowledge Level: Analyze) |
| CO 4 | Examine and assess the key ideas of Elliptic curve arithmetic. (Cognitive Knowledge Level: Evaluate) |
| CO 5 | Develop problem analysing and solving capabilities in Graph theory concepts. (Cognitive Knowledge Level: Analyze) |

Program Outcomes (PO)

Outcomes are the attributes that are to be demonstrated by a graduate after completing the course.

PO1: An ability to independently carry out research/investigation and development work in engineering and allied streams

PO2: An ability to communicate effectively, write and present technical reports on complex engineering activities by interacting with the engineering fraternity and with society at large.

PO3: An ability to demonstrate a degree of mastery over the area as per the specialization of the program. The mastery should be at a level higher than the requirements in the appropriate bachelor program

PO4: An ability to apply stream knowledge to design or develop solutions for real world problems by following the standards

PO5: An ability to identify, select and apply appropriate techniques, resources and state-of-the-art tool to model, analyse and solve practical engineering problems.

PO6: An ability to engage in life-long learning for the design and development related to the stream related problems taking into consideration sustainability, societal, ethical and environmental aspects

PO7: An ability to develop cognitive load management skills related to project management and finance which focus on Entrepreneurship and Industry relevance.

Mapping of course outcomes with program outcomes:

| | PO 1 | PO 2 | PO 3 | PO 4 | PO 5 | PO 6 | PO 7 |
|------|------|------|------|------|------|------|------|
| CO 1 | ☉ | | ☉ | ☉ | ☉ | | |
| CO 2 | ☉ | | ☉ | ☉ | ☉ | | |
| CO 3 | ☉ | | ☉ | ☉ | ☉ | ☉ | |
| CO 4 | ☉ | | ☉ | ☉ | ☉ | ☉ | |
| CO 5 | ☉ | | ☉ | ☉ | ☉ | ☉ | |

Assessment Pattern:

| Bloom's Category | End Semester Examination |
|------------------|--------------------------|
| Apply | 40% |
| Analyse | 25% |
| Evaluate | 15% |
| Create | |

Mark distribution:

| Total Marks | CIE | ESE | ESE Duration |
|-------------|-----|-----|--------------|
| 100 | 40 | 60 | 2.5 hours |

Continuous Internal Evaluation Pattern: 40 marks

- MicroProject/Course based project - 20 marks
- Seminar/quiz - 10 mark
- Internal Exam - 10 mark

End Semester Examination Pattern:

There will be two parts; Part A and Part B. Part A contain 5 questions with 1 question from each module, having 4 marks for each question. Students should answer all questions. Part B contains 2 questions from each module of which a student should answer any one. Each question can have maximum 2 sub-divisions and carries 8 marks.

Syllabus:

Module 1 (Linear Arithmetic)

Integer arithmetic-Divisibility, Greatest Common Divisor Euclid's & extended Euclid's Algorithm for GCD Modular arithmetic - Operations, Properties Polynomial Arithmetic Algebraic structures-Group Ring Field

Module 2 (Prime Numbers)

Prime numbers, Prime & power factorization, Primitive roots, Existence of primitive roots for primes, Fermat's theorem, Primality testing, Euler's theorem, Euler's totient function, Pseudo primes and Carmichael numbers.

Module 3 (Linear Congruence)

Congruences- Definition and properties, Linear congruence- Solutions, Chinese Remainder Theorem (CRT), Wilson's theorem, Discrete logarithms, Quadratic Residues, Reciprocity, Legendre symbol and Jacobi Symbol

Module 4 (Elliptic Curve Arithmetic)

Fundamental theorem of arithmetic, Elliptic curve arithmetic, Prime curves, Binary curves, Addition of two points, Multiplication of a point by a constant.

Module 5 (Graph Theory)

Graphs, Euler tour, Hamiltonian graphs, Euler's formula, Tree- Weighted trees, Shortest path algorithms, Spanning trees

Reference Books:

1. Behrouz A Forouzan, Cryptography and Network Security, 3/e, Tata McGraw-Hill.
2. Charles P Pfleeger, Shari Lawrence Pfleeger, Jonathan Margulies, Security in Computing, 5/e, Prentice Hall.
3. G.A. Jones & J.M. Jones, Elementary Number Theory, Springer UTM, 2007
4. William Stallings, Cryptography and Network Security Principles and Practices, 4/e, Pearson Ed.
5. J. Clark and D. A Holton, A first look at Graph Theory, Allied Publishers (World Scientific) New Delhi 1991.

Course Level Assessment Questions

Course Outcome 1 (CO1):

1. Find GCD (200,15) using Euclid's Algorithm.
2. Factorize: $x^3 - 23x^2 + 142x - 120$.

Course Outcome 2 (CO2):

1. Check whether 561 is a Carmichael number or not.
2. Solve the congruence relation $103x \equiv 57 \pmod{211}$.

Course Outcome 3 (CO3):

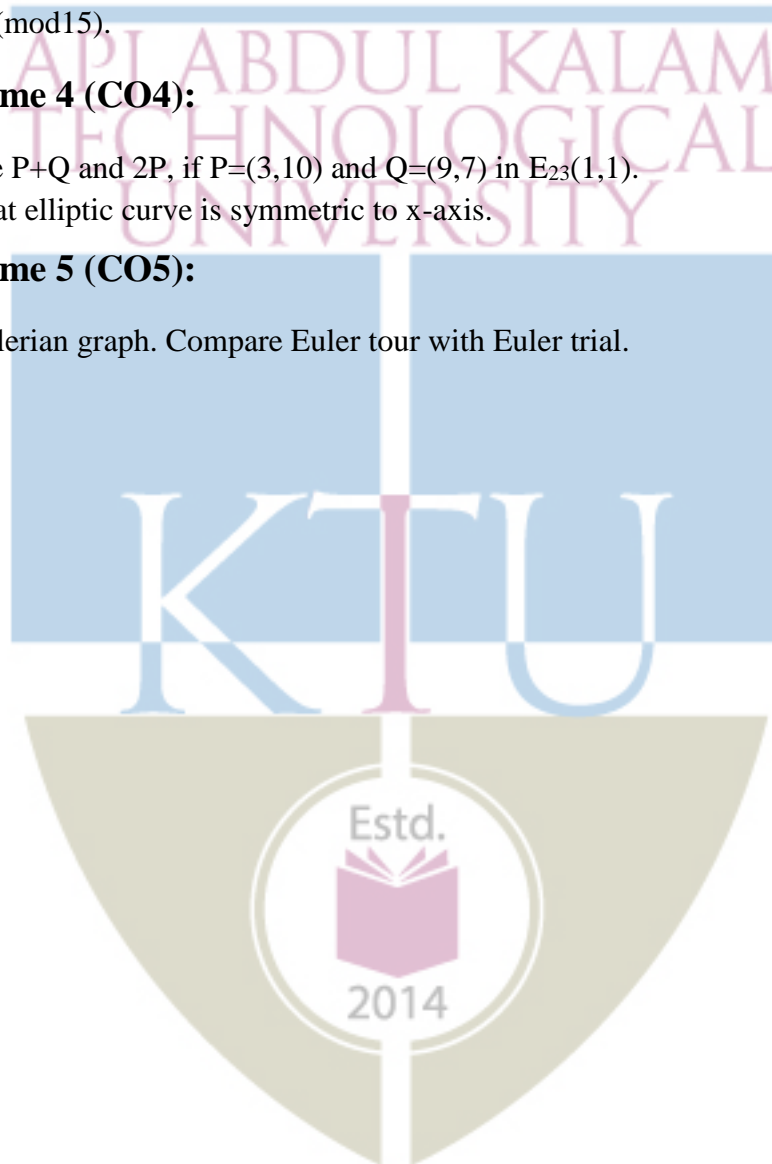
Solve $9x \equiv 6 \pmod{15}$.

Course Outcome 4 (CO4):

1. Compute $P+Q$ and $2P$, if $P=(3,10)$ and $Q=(9,7)$ in $E_{23}(1,1)$.
2. Prove that elliptic curve is symmetric to x-axis.

Course Outcome 5 (CO5):

Construct an Eulerian graph. Compare Euler tour with Euler trail.



Model Question paper

Reg. No.....
.....

Name:

APJ ADUL KALAM TECHNOLOGICAL UNIVERSITY

FIRST SEMESTER M. TECH. DEGREE EXAMINATION

221TCS007 FOUNDATIONS OF CRYPTOGRAPHY

Max. Marks: 60

Duration: 2.5 Hrs.

Part A (Answer All questions)

Each question carries 4 marks

1. Find GCD (200,15) using Euclid's Algorithm.
2. Check whether 561 is a Carmichael number or not.
3. Solve $9x \equiv 6 \pmod{15}$.
4. Prove that elliptic curve is symmetric to x-axis.
5. Construct an Eulerian graph. Compare Euler tour with Euler trail.

Part B

Each question carries 8 marks

6. For $f(x) = (x^7 + x^5 + x^3 + x + 1)$ and $g(x) = (x^3 + x + 1)$ compute the following over Mod2.
 - a. $f(x)+g(x)$
 - b. $f(x)-g(x)$
 - c. $f(x)*g(x)$ and
 - d. $f(x)/g(x)$

(8)

OR

7. Describe the properties of modular arithmetic and modulo operator. (8)
 - a. Discuss pseudoprime numbers with example. (4)
 - b. Factorize: $x^3 - 23x^2 + 142x - 120$. (4)

OR

8. a. State and prove Fermat's theorem. (4)
 - b. Define Euler's totient function. Solve $3^{202} \pmod{13}$. (4)
9. Solve the congruence relation $103x \equiv 57 \pmod{211}$. (8)

OR

10. Using Chinese Remainder Theorem, solve the system of congruence, $x \equiv 2 \pmod{3}$, $x \equiv 3 \pmod{5}$, $x \equiv 2 \pmod{7}$. (8)

11. How will you find PQ in an elliptic curve for any two points P and Q. (8)

OR

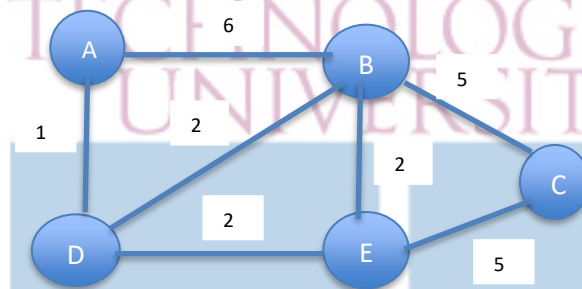
12. Compute $P+Q$ and $2P$, if $P=(3,10)$ and $Q=(9,7)$ in $E_{23}(1,1)$. (8)

13. With the help of suitable examples, explain Hamiltonian path, cycle, circuit and graph.

(8)

OR

14. Find Shortest path from A to C using Dijkstra's Algorithm.



(8)

Course Plan:

| No | Contents | No. of Lecture Hrs |
|-----|--|--------------------|
| 1 | Module 1 - 8 hours | |
| 1.1 | Integer arithmetic-Divisibility, | 1 |
| 1.2 | Greatest Common Divisor | 1 |
| 1.3 | Euclid's & extended Euclid's Algorithm for GCD | 1 |
| 1.4 | Modular arithmetic - Operations, Properties | 1 |
| 1.5 | Polynomial Arithmetic | 1 |
| 1.6 | Algebraic structures-Group | 1 |
| 1.7 | Ring | 1 |
| 1.8 | Field | 1 |
| 2 | Module 2 -8 hours | |
| 2.1 | Prime numbers | 1 |
| 2.2 | Pseudo primes and Carmichael numbers | 1 |
| 2.3 | Prime & power factorization | 1 |
| 2.4 | Primitive roots | 1 |
| 2.5 | Existence of primitive roots for primes | 1 |
| 2.6 | Fermat's theorem | 1 |
| 2.7 | Primality testing | 1 |
| 2.8 | Euler's theorem, Euler's totient function | 1 |
| 3 | Module 3 -8 hours | |

| | | |
|-----|--|---|
| 3.1 | Congruences- Definition and properties | 1 |
| 3.2 | Linear congruence- Solutions | 1 |
| 3.3 | Chinese Remainder Theorem (CRT) | 1 |
| 3.5 | Wilson' s theorem | 1 |
| 3.5 | Discrete logarithms | 1 |
| 3.6 | Quadratic Residues | 1 |
| 3.7 | Reciprocity | 1 |
| 3.8 | Legendre symbol and Jacobi Symbol | 1 |
| 4 | Module 4 – 8 hours | |
| 4.1 | Fundamental theorem of arithmetic(Lecture 1) | 1 |
| 4.2 | Fundamental theorem of arithmetic(Lecture 2) | 1 |
| 4.3 | Elliptic curve arithmetic(Lecture 1) | 1 |
| 4.4 | Elliptic curve arithmetic (Lecture 2) | 1 |
| 4.5 | Prime curves | 1 |
| 4.6 | Binary curves | 1 |
| 4.7 | Addition of two points | 1 |
| 4.8 | Multiplication of a point by a constant | 1 |
| 5 | Module 5 -8 hours | |
| 5.1 | Graphs, Euler tour | 1 |
| 5.2 | Hamiltonian graphs | 1 |
| 5.3 | Euler' formula | 1 |
| 5.4 | Tree- Weighted trees | 1 |
| 5.5 | Shortest path algorithms | 1 |
| 5.6 | Spanning trees | 1 |
| 5.7 | The max-flow min-cut theorem(Lecture 1) | 1 |



| CODE 221TCS008 | INFORMATION SECURITY | CATEGORY | L | T | P | CREDIT |
|-------------------|----------------------|----------------|---|---|---|--------|
| | | Program Core 2 | 3 | 0 | 0 | 3 |

Preamble:

The purpose of this course is to make learners to have thorough knowledge on Information security. This course covers different information security problems and Technologies. This course also covers the concepts in Governance and IT Auditing. The concepts covered in this course enable the learners an understanding of need of Information Security and carryout development activities in the area of Information Security.

Course Outcomes:

After the completion of the course the student will be able to

| | |
|-------------|--|
| CO 1 | Judge different threats posed to Information Security in an organization.(Cognitive Knowledge level : Evaluate) |
| CO 2 | Demonstrate different Access Controls and Authentication Methodologies and should be able to apply cryptographic algorithm on input text. (Cognitive Knowledge level : Apply) |
| CO 3 | Experiment different security tools for each areas. (Cognitive Knowledge level : Apply) |
| CO 4 | Implement Information Security Governance and awareness Programs.((Cognitive Knowledge level : Apply) |
| CO 5 | Carryout IT Auditing with different tools based on standard procedure(Cognitive Knowledge level : analysis) |
| CO6 | Implement different Authentication Methods while designing secure systems. (Cognitive Knowledge level : Create) |

Program Outcomes (PO)

Outcomes are the attributes that are to be demonstrated by a graduate after completing the course.

PO1: An ability to independently carry out research/investigation and development work in engineering and allied streams.

PO2: An ability to communicate effectively, write and present technical reports on complex engineering activities by interacting with the engineering fraternity and with society at large.

PO3: An ability to demonstrate a degree of mastery over the area as per the specialization of the program. The mastery should be at a level higher than the requirements in the appropriate bachelor program

PO4: An ability to apply stream knowledge to design or develop solutions for real world problems by following the standards

PO5: An ability to identify, select and apply appropriate techniques, resources and state-of-the-art tool to model, analyse and solve practical engineering problems.

PO6: An ability to engage in life-long learning for the design and development related to the stream related problems taking into consideration sustainability, societal, ethical and environmental aspects

PO7: An ability to develop cognitive load management skills related to project management and finance which focus on Entrepreneurship and Industry relevance.

Mapping of course outcomes with program outcomes

| | PO 1 | PO 2 | PO 3 | PO 4 | PO 5 | PO 6 | PO 7 |
|------|------|------|------|------|------|------|------|
| CO 1 | ☑ | ☑ | ☑ | ☑ | ☑ | | |
| CO 2 | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | |
| CO 3 | ☑ | ☑ | ☑ | | ☑ | | |
| CO 4 | | ☑ | ☑ | | ☑ | | |
| CO 5 | | ☑ | ☑ | | ☑ | | ☑ |
| CO6 | ☑ | ☑ | ☑ | ☑ | ☑ | | |

Assessment Pattern

| Bloom's Category | End Semester Examination (in %) |
|------------------|---------------------------------|
| Apply | 50 |
| Analyze | 30 |
| Evaluate | 20 |

Mark distribution

| Total Marks | CIE | ESE | ESE Duration |
|-------------|-----|-----|--------------|
| 100 | 40 | 60 | 2.5 hours |

Continuous Internal Evaluation Pattern:

Evaluation shall only be based on application, analysis or design based questions (for both internal and end semester examinations).

Continuous Internal Evaluation Pattern: 40 marks

1. Micro Project/Course based project - 20 marks
2. Seminar/quiz - 10 mark
3. Internal Exam - 10 mark

Test paper shall include minimum 80% of the syllabus.

Course based task/test paper questions shall be useful in the testing of knowledge, skills, comprehension, application, analysis, synthesis, evaluation and understanding of the students.

End Semester Examination Pattern:

There will be two parts; Part A and Part B. Part A contains 5 questions with 1 question from each module, having 5 marks for each question. Students should answer all questions. Part B contains 7 questions with minimum one question from each module of which a student should answer any 5. Each question carries 7 marks



Syllabus

MODULE 1

Introduction to Information Security: What Is Security? Key concepts in information security, Critical Characteristics of Information, Components of an Information System, Approaches to Information Security Implementation, Security in the Systems Development Life Cycle. The Need for Security: Introduction, Threats and Attacks, Compromises to Intellectual Property, Deviations to Quality of Services, Espionage or Trespass, Forces of Nature, Human Error or Failure, Information Extortion, Sabotage or Vandalism, Software Attacks, Technical Hardware and Software Failures or Errors, Technological Obsolescence, Theft, Defense In Depth.

MODULE 2

Identification, Authentication and Access Controls: Identification, Authentication, Common Identification and Authentication Methods, Passwords, Biometrics, Hardware Tokens, What Are Access Controls?, Implementing Access Controls, Access Control Models, Physical Access Controls, Cryptography: Introduction, Cipher Methods, Cryptographic Algorithms, Cryptographic Tools, Protocols for Secure Communications

MODULE 3

Security Technology: Intrusion Detection and Prevention Systems: Why use an IDPS? Types of IDPS, IDPS Detection Methods, Strengths and Limitations of IDPS, Deployment and Implementation of an IDPS, Security Information and Event Management (SIEM):Data Aggregation, Analysis, Operational Interface, Scanning and Analysis Tools: Port Scanners, Firewall Analysis Tools, Operating System Detection Tools, Vulnerability Scanners, Biometric Access Controls, Protecting Remote Connections, Scanning and Analysis Tools: Packet Sniffers, Wireless Security Tools, Firewalls, Protecting Remote Connections: Remote Access, VPNs.

MODULE 4

Planning For Security :Information Security Planning and Governance, Information Security Policy, Standards, and Practices, Security Education, Training and Awareness Program, Risk Management: Risk Identification, Risk Assessment, Risk Control Strategies, Selecting a Risk Control Strategy: CBA analysis, CBA formula. Governance Overview: Governance Definition, Information Security Governance, Six Outcomes of Effective Governance, Data, Knowledge, Value of Information, Benefits of Good Governance, ISO/IEC 27001/27002

MODULE 5

The Audit Process: Internal Controls, Determining What to Audit ,Stages of an Audit, Standards, Auditing Cyber Security Programs, Auditing Networking Devices, Auditing Unix and Linux Operating Systems, Auditing End User Computing Devices, Auditing Cloud Computing and Outsourced Operations, Auditing Company Projects, Auditing New/Other Technologies.

Text Books

1. Michael E. Whitman, Herbert J. Mattord, “Principles of Information Security”, 6th edition, Cengage Learning India Private Limited, 2018.
2. Jason Andress ,Fundamentals of Information Security A straight forward Introduction,2019
3. Krag Brotby, Information Security Governance- A practical development and implementation approach,2009.
4. Mike Kegerreis, Mike Schiller and Chris Davis, IT Auditing using controls to protect Information Assets ,Third Edition.

Reference Books

1. S.H. von Solms, Rossouw von Solms, Information Security Governance,2008.
2. Angel R Otero, Information Technology Control and Audit, Fifth Edition

Course Level Assessment Questions

Course Outcome 1 (CO1):

1. Different Types of Attack may occur to Systems. Judge the different attacks/Threats and classify which type of breach occurred.
2. With the help of vulnerabilities and Threats, justify the need of Information Security in an organization.

Course Outcome 2 (CO2):

1. Using different cryptographic algorithms, convert the given plain text to cipher text.

2. Identify suitable security measure using different Access Controls and Authentication methods to secure systems.

Course Outcome 3 (CO3):

1. Use any security methodologies/tools to experiment Security measures for specific area.
2. Using Packet sniffers, Explain how troubleshooting for any network issue can be done.

Course Outcome 4 (CO4):

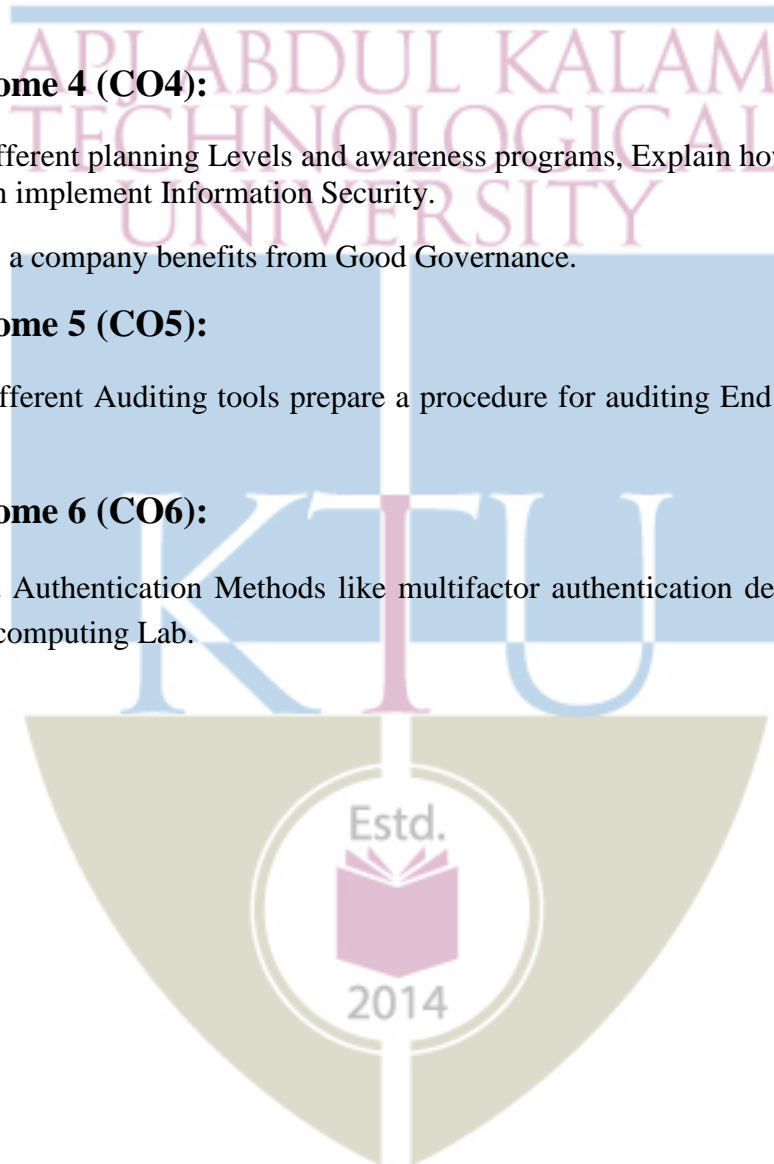
1. Using the different planning Levels and awareness programs, Explain how an IT company can implement Information Security.
2. Explain how a company benefits from Good Governance.

Course Outcome 5 (CO5):

1. Using the different Auditing tools prepare a procedure for auditing End User Computing Devices.

Course Outcome 6 (CO6):

1. Use different Authentication Methods like multifactor authentication develop a utility to secure students computing Lab.



Model Question Paper

QP CODE:

Reg No: _____

Name: _____

PAGES : 2

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

FIRST SEMESTER M. TECH DEGREE EXAMINATION, MONTH & YEAR

Course Code: 221TCS008

Course Name: **INFORMATION SECURITY**

Max. Marks : 60

Duration: 2.5 Hours

PART A

Answer All Questions. Each Question Carries 5 Marks

- | | | |
|----|---|----------|
| 1. | You receive an email from your bank telling you there is a problem with your account. The email provides instructions and a link so you can log into your account and fix the problem. What should you do? and what type of attack is this? | |
| 2. | Differentiate between verification and authentication of an identity? | |
| 3. | Describe Firewalls and How do you Configure and Manage Firewalls? | |
| 4. | What would be the outcomes of effective Governance? | |
| 5. | What are the different stages of an IT Audit? | (5x5=25) |

Part B

(Answer any five questions. Each question carries 7 marks)

- | | | |
|-----|--|-----|
| 6. | If a hacker breaks into a network, copies a few files, defaces a Web page, and steals credit card numbers, how many different threat categories does the attack fall into? Explain | (7) |
| 7. | Justify why an identity card alone might not make an ideal method of authentication. | (7) |
| 8. | Differentiate between Active and Passive vulnerability Scanners? | (7) |
| 9. | A number of direct and obvious benefits will evolve from implementing effective Information Security Governance. Justify | (7) |
| 10. | Develop a procedure on how to perform IT auditing on Company Projects. | (7) |

| | | |
|----|---|-----|
| 11 | Differentiate between signature-based detection, anomaly-based detection, and stateful protocol analysis. | (7) |
| 12 | Illustrate the working of Transposition Cipher and Substitution Cipher with an example. | (7) |

Course Plan (For 3 credit courses, the content can be for 40 hrs and for 2 credit courses, the content can be for 26 hrs. The audit course in third semester can have content for 30 hours).

| No | Contents | No. of Lecture Hrs(40 hrs) |
|-----|--|----------------------------|
| 1 | Module 1 - (7 hrs.) | |
| 1.1 | What Is Security? Key concepts in information security , Critical Characteristics of Information, Components of an Information System, | 1 |
| 1.2 | Approaches to Information Security Implementation, Security in the Systems Development Life Cycle. | 1 |
| 1.3 | The Need for Security: Introduction, Threats and Attacks | 1 |
| 1.4 | Compromises to Intellectual Property, Deviations to Quality of Services, | 1 |
| 1.5 | Espionage or Trespass, Forces of Nature, Human Error or Failure, Information Extortion | 1 |
| 1.6 | Sabotage or Vandalism, Software Attacks Technical Hardware-Software Failures or Errors, Technological Obsolescence | 1 |
| 1.7 | Theft, Defense In Depth | 1 |
| 2 | Module 2 - (9hrs.) | |
| 2.1 | Identification, Authentication | 1 |
| 2.2 | Common Identification and Authentication Methods Passwords, Biometrics, Hardware Tokens | 1 |
| 2.3 | What Are Access Controls?, Implementing Access Controls | 1 |
| 2.4 | Access Control Models, Physical Access Controls | 1 |
| 2.5 | Cryptography: Introduction, Cipher Methods | 1 |
| 2.6 | Cipher Methods | 1 |
| 2.7 | Cryptographic Algorithms | 1 |
| 2.8 | Cryptographic Tools | 1 |
| 2.9 | Protocols for Secure Communications | 1 |
| 3 | Module 3 - (8 hrs) | |
| 3.1 | Intrusion Detection and Prevention Systems, Why use an IDPS?, Types of IDPS | 1 |
| 3.2 | IDPS Detection Methods, Strengths and Limitations of IDPS, | 1 |

| | | |
|-----|---|---|
| 3.3 | Deployment and Implementation of an IDPS | 1 |
| 3.4 | Security Information and Event Management (SIEM) Data Aggregation, Analysis, Operational Interface | 1 |
| 3.5 | Scanning and Analysis Tools: Port Scanners, Firewall Analysis Tools, Operating System Detection Tools, Vulnerability Scanners | 2 |
| 3.5 | Scanning and Analysis Tools: Packet Sniffers, Wireless Security Tools | 1 |
| 3.6 | Firewalls | 1 |
| 3.7 | Protecting Remote Connections: Remote Access, VPNs | 1 |
| 4 | Module 4 - (8 hrs) | |
| 4.1 | Information Security Planning and Governance, Information Security Policy, Standards, and Practices | 1 |
| 4.2 | Security Education, Training and Awareness Program | 1 |
| 4.3 | Risk Management: Risk Identification, Risk Assessment, | 1 |
| 4.4 | Risk Control Strategies, Selecting a Risk Control Strategy: CBA analysis, CBA formula. | 1 |
| 4.5 | Governance Overview: Governance Definition, Information Security Governance, Six Outcomes of Effective Governance | 1 |
| 4.6 | Data, Knowledge, Value of Information, Benefits of Good Governance | 1 |
| 4.7 | Benefits of Good Governance | 1 |
| 4.9 | ISO/IEC 27001/27002 | 1 |
| 5 | Module 5 - (8 hrs) | |
| 5.1 | The Audit Process: Internal Controls, Determining What to Audit | 1 |
| 5.2 | Stages of an Audit, Standards | 1 |
| 5.3 | Auditing Cyber Security Programs | 1 |
| 5.4 | Auditing Networking Devices | 1 |
| 5.5 | Auditing Unix and Linux Operating Systems | 1 |
| 5.6 | Auditing End User Computing Devices | 1 |
| 5.7 | Auditing Cloud Computing and Outsourced Operations, Auditing Company Projects, | 1 |
| 5.8 | Auditing New/Other Technologies | 1 |

| CODE | COURSE NAME | CATEGORY | L | T | P | CREDIT |
|-----------|---------------------------------------|--------------------|---|---|---|--------|
| 22IECS033 | CYBER FORENSICS AND INCIDENT RESPONSE | Program Elective 1 | 3 | 0 | 0 | 3 |

Preamble: The course on Cyber Forensics and incident response aims at exploring an in-depth study on Cyber Forensics and Cyber security, the forensic investigation process and principles and the different types of cybercrimes and threats. The course also focuses on the incident responses, and the different types of Forensics. The course gives an understanding on the usage of the forensics analysis tools and a deep understanding of Anti forensics practices and methods. All the above aspects deal with case studies of the respective areas.

Course Outcomes: After the completion of the course the student will be able to

| CO# | Course Outcomes |
|-----|---|
| CO1 | Examine the significance of IT Act 2000 and relate it with respect to current cyber security scenarios. (Cognitive Knowledge Level: Analyze) |
| CO2 | Examine the incident evidence using the incident response tools (Cognitive Knowledge Level: Analyze) |
| CO3 | Utilize the methodologies and tools for detection of image artifacts (Cognitive Knowledge Level: Apply) |
| CO4 | Infer the details of Email headers and contents from Mobile devices (Cognitive Knowledge Level: Apply) |
| CO5 | Use conventional practices and techniques for antiforensics detection (Cognitive Knowledge Level: Apply) |
| CO6 | Review incident response procedures by applying cyber forensic methodologies and tools (Cognitive Knowledge Level: Evaluate) |

Program Outcomes (PO)

Outcomes are the attributes that are to be demonstrated by a graduate after completing the course.

PO1: An ability to independently carry out research/investigation and development work in engineering and allied streams

PO2: An ability to communicate effectively, write and present technical reports on complex engineering activities by interacting with the engineering fraternity and with society at large.

PO3: An ability to demonstrate a degree of mastery over the area as per the specialization of the program. The mastery should be at a level higher than the requirements in the appropriate bachelor program

PO4: An ability to apply stream knowledge to design or develop solutions for real world problems by following the standards

PO5: An ability to identify, select and apply appropriate techniques, resources and state-of-the-art tool to model, analyse and solve practical engineering problems.

PO6: An ability to engage in life-long learning for the design and development related to the stream related problems taking into consideration sustainability, societal, ethical and environmental aspects

PO7: An ability to develop cognitive load management skills related to project management and finance which focus on Entrepreneurship and Industry relevance.

Mapping of course outcomes with program outcomes

| | PO 1 | PO 2 | PO 3 | PO 4 | PO 5 | PO 6 | PO 7 |
|------|------|------|------|------|------|------|------|
| CO 1 | ✓ | | ✓ | ✓ | | ✓ | ✓ |
| CO 2 | ✓ | | ✓ | ✓ | ✓ | ✓ | |
| CO 3 | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ |
| CO 4 | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ |
| CO 5 | ✓ | | ✓ | ✓ | ✓ | ✓ | |
| CO 6 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

Assessment Pattern

| Bloom's Category | End Semester Examination |
|------------------|--------------------------|
| Apply | 60% |
| Analyse | 30% |
| Evaluate | 10% |
| Create | |

Mark distribution

| Total Marks | CIE | ESE | ESE Duration |
|-------------|-----|-----|--------------|
| | | | |

| | | | |
|-----|----|----|-----------|
| 100 | 40 | 60 | 2.5 hours |
|-----|----|----|-----------|

Continuous Internal Evaluation Pattern:

Evaluation shall only be based on application, analysis or design based questions (for both internal and end semester examinations).

Continuous Internal Evaluation: 40 marks

- i. Preparing a review article based on peer reviewed original publications (minimum 10 publications shall be referred) : 15 marks
- ii. Course based task / Seminar/ Data collection and interpretation : 15 marks
- iii. Test paper (1 number) : 10 marks

Test paper shall include minimum 80% of the syllabus.

Course based task/test paper questions shall be useful in the testing of knowledge, skills, comprehension, application, analysis, synthesis, evaluation and understanding of the students.

End Semester Examination Pattern:

The end semester examination will be conducted by the respective College.

There will be two parts; Part A and Part B.

Part A will contain 5 numerical/short answer questions with 1 question from each module, having 5 marks for each question. Students should answer all questions. Part B will contain 7 questions (such questions shall be useful in the testing of overall achievement and maturity of the students in a course, through long answer questions relating to theoretical/practical knowledge, derivations, problem solving and quantitative evaluation), with minimum one question from each module of which student should answer any five. Each question can carry 7 marks

Total duration of the examination will be 150 minutes.

Note: The marks obtained for the ESE for an elective course shall not exceed 20% over the average ESE mark % for the core courses. ESE marks awarded to a student for each elective course shall be normalized accordingly.

For example if the average end semester mark % for a core course is 40, then the maximum eligible mark % for an elective course is $40+20 = 60\%$.

Syllabus

MODULE-1 (CYBER FORENSICS)

Cyber Forensics: Cyber Technology- Technological Aspects of Cyber Forensics- Cybercrimes, Types of Cybercrimes - Governance Aspects of Cyber Forensics- Cyber Security Steps taken to protect ICT and prevent Misuse of Internet -Judicial Aspects of Cyber Forensics- Legal Perspective of Cyber Forensic investigations- IT Act 2000,Social Cyber Media.

MODULE-2: (COMPUTER INCIDENT RESPONSE)

Introduction, Incident Response Team, Stages of Incident Response, Security Incident Response Team Members, Incident Evidence, Incident Response Tools, Incident Response Policies and Procedures.

MODULE-3: (FORENSIC PROCESS AND INVESTIGATIONS)

Computer Forensic Investigations: -Preparing for computer investigations, understanding Public and private investigations, Forensics Process and Forensics Investigation Principles - Forensic Protocol for Evidence Acquisition - Digital Forensics Standards and Guidelines - Digital Evidence – Data Acquisition - storage formats for digital evidence, determining the best acquisition method, Whole Disk Encryption.

Cyber Forensics Tools-Computer Forensics software and hardware tools -Open Source and Proprietary --Challenges in Cyber Forensics, Skills Required to Become a Cyber Forensic Expert- Physical Requirements of a Cyber forensics Lab, Types of Cyber forensics

MODULE-4: (NETWORK AND EMAIL FORENSICS)

Network and Mobile Device Forensics: Forensic Footprints, Seizure of Networking Devices, Network Forensic Artifacts, ICMP Attacks, Drive-By Downloads, Network Forensic Analysis Tools, Case Study: Wireshark. Mobile device forensics, acquisition procedures for cell phones and mobile devices

Email Forensics: Email Components, Email Protocols. Email Formats: RFC 5322, Multipurpose Internet Mail Extensions. Email Threats and Comprehensive Email Security, S/MIME-Operational Description, Message Content Types, Analysis of Email headers.

MODULE-5: (ANTI-FORENSICS AND REPORT WRITING)

Anti-forensic Practices: Data Wiping, Shredding, Data Remanence, Degaussing, Trail Obfuscation- Spoofing, Data Modification, Encryption, Case Study: VeraCrypt, Data Hiding: Steganography and Cryptography, Case Study: SilentEye, Anti-forensics Detection Techniques, Case Study: Stegdetect

Report writing for high tech investigations – importance of reports, guidelines for writing, generating report findings with forensics software tools.

Text Books

1. Nishesh Sharma “Cyber Forensics in India- A Legal Perspective”, Universal Law Publishing, First Edition, March 2017
2. Bill Nelson, Amelia Philipps and Christopher Steuart, “Computer forensics- Guide to computer forensics and investigations”, Course Technology Inc,3rd Edition,2009
3. Leighton Johnson, “Computer Incident Response and Forensics Team Management. Conducting a Successful Incident Response”,Syngress, First Edition,2019
4. William Stallings “Network Security Essentials Applications and Standards” Pearson Education, 4th Edition, 2011.

Reference Books

1. E. Maiwald, “ Fundamentals of Network Security”, McGraw-Hill, First Edition, 2004
2. Niranjana Reddy, “Practical Cyber Forensics: An Incident-Based Approach to Forensic Investigations”, Apress, First Edition, 2019
3. Michael. E. Whitman, Herbet. J. Mattord,“Cyber Security Principles of Information Security”,Course Technology Ptr ,4th Edition,2011.
4. William Stallings “Cryptography and Network Security”,Pearson, 5th Edition,2018

Course Level Assessment Questions

Course Outcome 1 (CO1):

1. Internet has now become the part and parcel of everyday life of an individual. The ICT devices which are used to access the internet are a point of attack to the attackers, intruders and hackers. The need for protecting these ICT devices and to prevent the Misuse of Internet is vital now. Cite the different steps used for mitigation of attacks against the attacks caused on these devices.
2. Investigate the impact of Section 66 in IT Act to General Public

Course Outcome 2 (CO2):

1. Using a suitable incident response tool, examine the hash value of incident evidence.

Course Outcome 3 (CO3):

1. Use any forensics methodologies/tools to extract artefacts of an image obtained from a Windows based system.
2. Digital Evidence is important to trace out the culprits/suspects in a crime. Evidences are stored in digital devices in different storage formats. Suggest the different storage formats used for storing the digital evidence by the different tools and point out the formats which are suitable for the investigators for faster retrieval of information.

Course Outcome 4 (CO4):

1. Use wireshark tool to identify packets that are vulnerable.
2. Examine Email headers of a particular email and report the artefacts obtained.

Course Outcome 5 (CO5):

1. Put on the different anti-forensics practices used to destroy or conceal data in order to prevent others from accessing it.

Course Outcome 6 (CO6):

1. Apply standard operating procedures and cyber forensics tools to report the details of incident evidence and prepare a report based on this.



Model Question Paper

QP CODE:

Reg No: _____

Name: _____

PAGES : 4

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

FIRST SEMESTER M.TECH DEGREE EXAMINATION, MONTH & YEAR

Course Code: 221ECS033

Course Name: CYBER FORENSICS AND INCIDENT RESPONSE

Max. Marks : 60

Duration: 2.5 Hours

PART A

Answer All Questions. Each Question Carries 5 Marks

| | | |
|----|--|----------|
| 1. | Why is it important to take cyber security Steps to protect ICT and prevent misuse of Internet? | |
| 2. | With an example write down the different stages of incident response in investigation? | |
| 3. | Why is it important for a forensic expert to follow the forensic principles during investigations? | |
| 4. | What all artefacts are obtained by applying the network forensics tools on a packet? | |
| 5. | Trace out how encryption is done using Veracrypt. | (5x5=25) |

Part B

(Answer any five questions. Each question carries 7 marks)

| | | |
|----|--|-----|
| 6. | Write down the impact of cybercrimes in society? How these crimes be prevented and showcase the mitigation steps used for the prevention of Cybercrimes. | (7) |
| 7. | (a) There is a well-defined standard Operating procedure for collecting incident responses. Cite the SOP. | (4) |
| | (b) What do you mean by an incident in forensics terms? | (3) |
| 8. | (a) What is the importance of data storage formats in image acquisition? | (4) |
| | (b) List the different Open Source Tools used in Image Acquisition and the purpose they serve. | (3) |

| | | | |
|----|-----|--|-----|
| 9. | | Diagrammatically represent the different types of Computer Forensics Lab and list the equipment's that are housed. Also write down the need of each of the equipments. | (7) |
| 10 | (a) | What is Cyber Security? Discuss the Do's and Don'ts to be followed in using a cyber device. | (3) |
| | (b) | Examine Email headers using a suitable tool and report the discrepancies that are found in the metadata information? | (4) |
| 11 | (a) | Why does data need Cryptography? | (4) |
| | (b) | What is the difference between a Cryptographer and a Crypter? Differentiate by considering a sample scenario and clearly define the points which made them different. | (3) |
| 12 | (a) | Anti-forensics Detection Techniques will help a lot in identifying the anti-forensics activities. Apply an anti-forensic detection methodology and carve out the information available. | (4) |
| | (b) | Finding a crime and preparing an investigation report is important in all types of investigations. What is the significance of reports in high tech investigations? Write down a sample report generated by a forensic tool. | (3) |

Course Plan (For 3 credit courses, the content can be for 40 hrs and for 2 credit courses, the content can be for 26 hrs. The audit course in third semester can have content for 30 hours)



COURSE PLAN

| No. | Topic | No. of Lectures (40) |
|----------|--|-----------------------|
| 1 | Module-1 (Cyber Forensics) (9 hrs) | |
| 1.1 | Cyber Forensics- Introduction | 1 |
| 1.2 | Cyber Technology- Technological Aspects of Cyber Forensics- Lecture 1 | 1 |
| 1.3 | Technological Aspects of Cyber Forensics-Lecture 2 | 1 |
| 1.4 | Cybercrimes, Types of Cybercrimes | 1 |
| 1.5 | Governance Aspects of Cyber Forensics | 1 |
| 1.6 | Cyber Security Steps taken to protect ICT and prevent Misuse of Internet | 1 |
| 1.7 | Judicial Aspects of Cyber Forensics | 1 |
| 1.8 | Legal Perspective of Cyber Forensic investigations | 1 |
| 1.9 | IT Act 2000, Social Cyber Media | 1 |
| 2 | Module-2: (Computer Incident Response)(8 hrs) | |
| 2.1 | Computer Incident Response- Introduction | 1 |
| 2.2 | Incident Response Team | 1 |
| 2.3 | Stages of Incident Response | 1 |
| 2.4 | Security Incident Response Team Members | 1 |
| 2.5 | Incident Evidence | 1 |
| 2.6 | Incident Response Tools-Lecture 1 | 1 |
| 2.7 | Incident Response Tools-Lecture 2 | 1 |

| | | |
|----------|--|---|
| 2.8 | Incident Response Policies and Procedures | 1 |
| 3 | Module-3: (Forensic Process and Investigations)(11 hrs) | |
| 3.1 | Computer Forensic Investigations: -Preparing for computer investigations | 1 |
| 3.2 | Understanding Public and private investigations | 1 |
| 3.3 | Forensics Process and Forensics Investigation Principles | 1 |
| 3.4 | Forensic Protocol for Evidence Acquisition | 1 |
| 3.5 | Digital Forensics Standards and Guidelines | 1 |
| 3.6 | Digital Evidence, Data Acquisition | 1 |
| 3.7 | Storage formats for digital evidence, Determining the best acquisition method, Whole Disk Encryption | 1 |
| 3.8 | Cyber Forensics Tools-Computer Forensics software and hardware tools - Open Source and Proprietary | 1 |
| 3.9 | Challenges in Cyber Forensics | 1 |
| 3.10 | Skills Required to Become a Cyber Forensic Expert, Physical Requirements of a Cyber forensics Lab | 1 |
| 3.11 | Types of Cyber forensics | 1 |
| 4 | Module-4: (Network and Email Forensics)(7 hrs) | |
| 4.1 | Forensic Footprints, Seizure of Networking Devices, Network Forensic Artifacts | 1 |
| 4.2 | ICMP Attacks, Drive-By Download | 1 |
| 4.3 | Network Forensic Analysis Tools, Case Study: Wireshark. | 1 |
| 4.4 | Mobile device forensics, acquisition procedures for cell phones and mobile devices | 1 |

| | | |
|----------|--|---|
| 4.5 | Email Forensics: Email Components, Email Protocols, Email Formats: RFC 5322, Multipurpose Internet Mail Extensions | 1 |
| 4.6 | Email Threats and Comprehensive Email Security, S/MIME-Operational Description, Message Content Types | 1 |
| 4.7 | Analysis of Email headers | 1 |
| 5 | Module-5: (Anti-Forensics and Report Writing) (5 hrs) | |
| 5.1 | Anti-forensic Practices - Data Wiping and Shredding, Data Remanence, Degaussing | 1 |
| 5.2 | Trail Obfuscation: Spoofing, Data Modification, Encryption Case Study: VeraCrypt | 1 |
| 5.3 | Data Hiding: Steganography and Cryptography, Case Study: SilentEye, | 1 |
| 5.4 | Anti-forensics Detection Techniques, Case Study: Stegdetect | 1 |
| 5.5 | Report writing for high tech investigations | 1 |



| CODE | COURSE NAME | CATEGORY | L | T | P | CREDIT |
|-----------|----------------------------|--------------------|---|---|---|--------|
| 221ECS004 | COMPUTATIONAL INTELLIGENCE | PROGRAM ELECTIVE 1 | 3 | 0 | 0 | 3 |

Preamble: The aim of this course is to provide the students with the knowledge and skills required to design and implement effective and efficient Computational Intelligence solutions to problems for which a direct solution is impractical or unknown. This course covers concepts of fuzzy logic, genetic algorithms, and swarm optimization techniques. The learners will be able to provide Fuzzy and AI –based solutions to real world problems.

Course Outcomes:

After the completion of the course the student will be able to

| | |
|------|--|
| CO 1 | Apply fuzzy logic to handle uncertainty and solve engineering problems. (Cognitive Knowledge level : Understand) |
| CO 2 | Apply Fuzzy Logic Inference methods in building intelligent machines. (Cognitive Knowledge level : Apply) |
| CO 3 | Design genetic algorithms for optimized solutions in engineering problems. (Cognitive Knowledge level : Analyze) |
| CO 4 | Analyze the problem scenarios and apply Ant colony system to solve real optimization problems. (Cognitive Knowledge level : Apply) |
| CO 5 | Apply PSO algorithm to solve real world problems. (Cognitive Knowledge level : Apply) |
| CO6 | Design, develop and implement solutions based on computational intelligence concepts and techniques. (Cognitive Knowledge level : Create) |

Program Outcomes (PO)

Outcomes are the attributes that are to be demonstrated by a graduate after completing the course.

PO1: An ability to independently carry out research/investigation and development work in engineering and allied streams

PO2: An ability to communicate effectively, write and present technical reports on complex engineering activities by interacting with the engineering fraternity and with society at large.

PO3: An ability to demonstrate a degree of mastery over the area as per the specialization of the program. The mastery should be at a level higher than the requirements in the appropriate bachelor program

PO4: An ability to apply stream knowledge to design or develop solutions for real world problems by following the standards

PO5: An ability to identify, select and apply appropriate techniques, resources and state-of-the-art tool to model, analyse and solve practical engineering problems.

PO6: An ability to engage in life-long learning for the design and development related to the stream related problems taking into consideration sustainability, societal, ethical and environmental aspects

PO7: An ability to develop cognitive load management skills related to project management and finance which focus on Entrepreneurship and Industry relevance.

Mapping of course outcomes with program outcomes

| | PO 1 | PO 2 | PO 3 | PO 4 | PO 5 | PO 6 | PO 7 |
|------|------|------|------|------|------|------|------|
| CO 1 | | | | ☑ | | ☑ | |
| CO 2 | ☑ | | ☑ | ☑ | ☑ | ☑ | |
| CO 3 | ☑ | | ☑ | ☑ | ☑ | ☑ | |
| CO 4 | ☑ | | ☑ | ☑ | ☑ | ☑ | |
| CO 5 | ☑ | | ☑ | ☑ | ☑ | ☑ | |
| CO 6 | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |

Assessment Pattern

| Bloom's Category | End Semester Examination |
|------------------|--------------------------|
| Apply | 70%-80% |
| Analyse | 30%-40% |
| Evaluate | |
| Create | |

Mark distribution

| Total Marks | CIE | ESE | ESE Duration |
|-------------|-----|-----|--------------|
| 100 | 40 | 60 | 2.5 hours |

Continuous Internal Evaluation Pattern:

Evaluation shall only be based on application, analysis or design based questions (for both internal and end semester examinations).

Continuous Internal Evaluation: 40 marks

- i. Preparing a review article based on peer reviewed original publications (minimum 10 publications shall be referred) : 15 marks
- ii. Course based task / Seminar/ Data collection and interpretation : 15 marks
- iii. Test paper (1 number) : 10 marks

Test paper shall include minimum 80% of the syllabus.

Course based task/test paper questions shall be useful in the testing of knowledge, skills, comprehension, application, analysis, synthesis, evaluation and understanding of the students.

End Semester Examination Pattern:

The end semester examination will be conducted by the respective College.

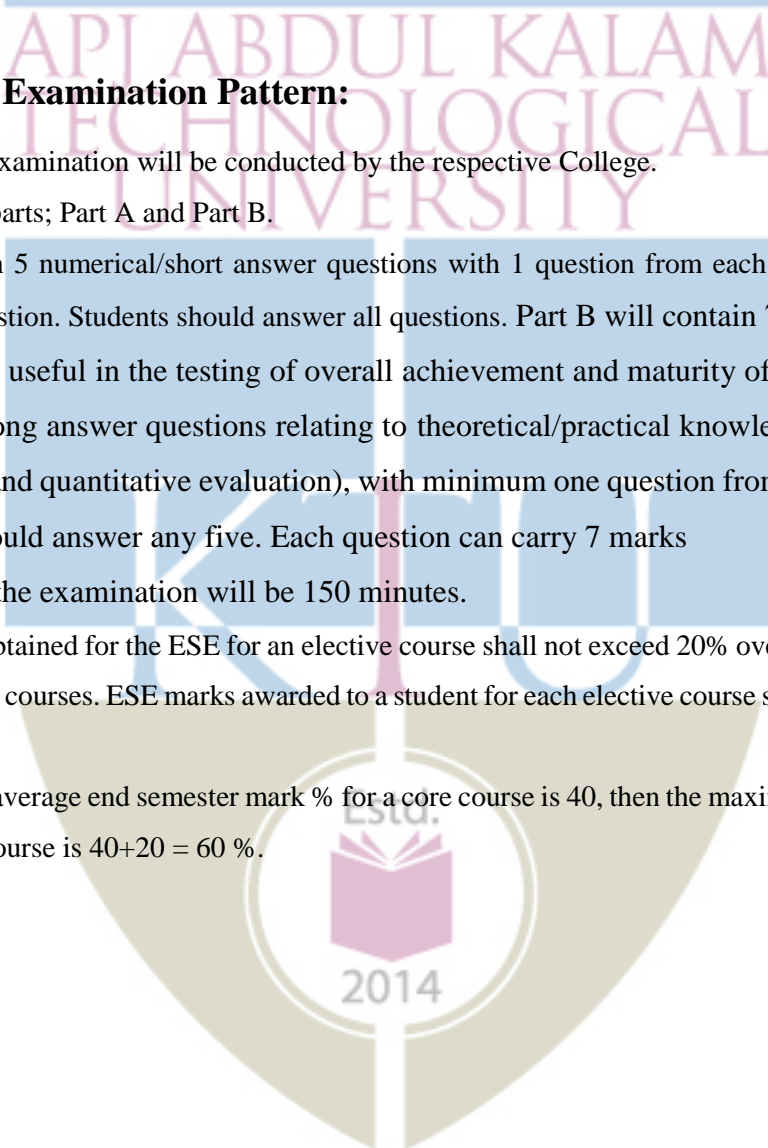
There will be two parts; Part A and Part B.

Part A will contain 5 numerical/short answer questions with 1 question from each module, having 5 marks for each question. Students should answer all questions. Part B will contain 7 questions (such questions shall be useful in the testing of overall achievement and maturity of the students in a course, through long answer questions relating to theoretical/practical knowledge, derivations, problem solving and quantitative evaluation), with minimum one question from each module of which student should answer any five. Each question can carry 7 marks

Total duration of the examination will be 150 minutes.

Note: The marks obtained for the ESE for an elective course shall not exceed 20% over the average ESE mark % for the core courses. ESE marks awarded to a student for each elective course shall be normalized accordingly.

For example if the average end semester mark % for a core course is 40, then the maximum eligible mark % for an elective course is $40+20 = 60$ %.



Syllabus

MODULE 1

FUZZY LOGIC: Crisp sets vs fuzzy sets- Operations and properties of Fuzzy sets. Membership functions: features of membership functions, Fuzzification and methods of membership value assignment-Defuzzification-Lambda(alpha) cuts- Fuzzy Relation and fuzzy composition- Operations on fuzzy relations

MODULE 2

FUZZY SYSTEMS: Linguistic variables and Hedges-Fuzzy Rule Base System-Aggregation of fuzzy rules-Fuzzy Inference System: Mamdani FIS, Larsen Model-Fuzzy reasoning GMP and GMT

MODULE 3

GENETIC ALGORITHMS: Introduction to Genetic Algorithms –chromosomes - fitness functions – Population- GA operators – Elitism – GA parameters – Convergence -. Multi-objective Genetic Algorithm.

MODULE 4

ANT COLONY SYSTEMS: Introduction to ant colony systems, types of ant colony systems, Development of the ant colony system- Applications of ant colony intelligence- Working of ant colony systems

MODULE 5

PARTICLE SWARM OPTIMIZATION: Basic Model of PSO algorithm- Global Best PSO- Local Best PSO- Comparison of 'gbest' to 'lbest' - PSO Algorithm Parameters- Problem Formulation of PSO algorithm.

Velocity clamping- Inertia weight- Constriction Coefficient- Boundary Conditions- Guaranteed Convergence PSO (GCPSO)- Initialization, Stopping Criteria, Iteration Terms and Function Evaluation.

Text Books

1. Samir Roy, UditChakraborty, Introduction to Soft Computing Neuro- Fuzzy Genetic Algorithms, Pearson, 2013

2. N.P. Padhy, Artificial Intelligence and Intelligent systems, Oxford Press, New Delhi, 2005

Reference Books

1. Xin-She Yang School of Science and Technology, Middlesex University London, Nature-Inspired Optimization Algorithms, Elsevier, First edition, 2014
2. Satyobroto Talukder, Blekinge Institute of Technology, Mathematical Modelling and Applications of Particle Swarm Optimization, February 2011
3. Mitchell Melanie, An Introduction to Genetic Algorithm, Prentice Hall, 1998
4. Andries Engelbrecht, Computational Intelligence: An Introduction, Wiley, 2007
5. Marco Dorigo and Thomas Stutzle, "Ant Colony optimization", Prentice Hall of India, New Delhi 2005

Course Level Assessment Questions

Course Outcome 1 (CO1):

1. Let $V = \{A, B, C, D\}$ be the set of four kinds of vitamins, $F = \{f_1, f_2, f_3\}$ be three kinds of fruits containing the vitamins to various extents, and $D = \{d_1, d_2, d_3\}$ be the set of three diseases that are caused by deficiency of these vitamins. Vitamin contents of the fruits are expressed with the help of the fuzzy relation R over $F \times V$, and the extent of which diseases are caused the deficiency of these vitamins is given by the fuzzy relation S over $V \times D$. Relations R and S are given below

$$R = \begin{bmatrix} 0.5 & 0.2 & 0.1 & 0.1 \\ 0.2 & 0.7 & 0.4 & 0.3 \\ 0.4 & 0.4 & 0.8 & 0.1 \end{bmatrix} \quad S = \begin{bmatrix} 0.3 & 0.5 & 0.7 \\ 0.1 & 0.8 & 0.4 \\ 0.9 & 0.1 & 0.2 \\ 0.5 & 0.5 & 0.3 \end{bmatrix}$$

Find the correlation between the amount of certain fruit that should be taken while suffering from a disease.

Course Outcome 2 (CO2)

1. In mechanics, the energy of a moving body is called kinetic energy. Suppose we model mass and velocity as inputs to a moving body and energy as output. Observe the system for a while and the following rule is deduced.

IF x is small and y is high

THEN z is medium

The graphical representation of rule is given below. Let the inputs given are 0.35kg and 55m/s. What will the output using Mamdani inference? Any defuzzification method can be used to obtain the crisp single output.

Course Outcome 3(CO3):

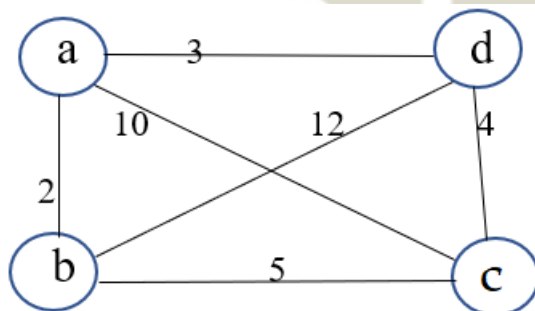
1. Describe how Roulette wheel is used for selection. Draw the Roulette wheel for six chromosomes corresponding to the table given below.

| <i>Chromosome #</i> | <i>Fitness</i> |
|---------------------|----------------|
| 1 | 10 |
| 2 | 5 |
| 3 | 25 |
| 4 | 15 |
| 5 | 30 |
| 6 | 20 |

Course Outcome 4 (CO4):

1. Consider an Ant Colony System based on Ant Quantity model for solving the following Travelling Salesman Problem. Compute the pheromone content at each of the edges after 4 steps(1 iteration). Assume pheromone decay factor $\rho=0.1$, $Q = 120$. Assume initial pheromone of 50 units at each of the edges and that three ants k_1, k_2 and k_3 follow the paths given below in the first iteration.

$k_1 = a b c d a$; $k_2 = a c b d a$; $k_3 = a d c b a$



2. Six jobs go first on machine A, then on machine B, and finally on machine C. The order of the completion of the jobs in the three machines is given in Table

| Jobs | Processing time(hr) | | |
|------|---------------------|-----------|-----------|
| | Machine A | Machine B | Machine C |
| 1 | 8 | 3 | 8 |
| 2 | 3 | 4 | 7 |
| 3 | 7 | 5 | 6 |
| 4 | 2 | 2 | 9 |
| 5 | 5 | 1 | 10 |
| 6 | 1 | 6 | 9 |

Find the sequence of jobs that minimizes the time required to complete the jobs using the ACS model.

Course Outcome 5 (CO5):

1. Consider a particle swarm optimization system composed of three particles and maximum velocity 10. Assume that both the random numbers r_1 and r_2 used for computing the movement of the particle towards the individual best position and social best position are 0.5. Also assume that the space of solutions is the two-dimensional real valued space and the current state of swarm is as follows:

Position of particles: $x_1 = (4,4)$; $x_2 = (8,3)$; $x_3 = (6,7)$
 Individual best positions : $x_1^* = (4,4)$; $x_2^* = (7,3)$; $x_3^* = (5,6)$
 Velocities: $v_1 = (2,2)$; $v_2 = (3,3)$; $v_3 = (4,4)$

What would be the next position of each particle after one iteration of the PSO algorithm if the inertia parameter ω that is used along with current velocity update formula is 0.8 ?

Course Outcome 6 (CO6):

1. Implement travelling salesman problem using appropriate optimization technique.

Model Question Paper

QP CODE:

Reg No: _____

Name: _____

PAGES : 4

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

FIRST SEMESTER M. TECH DEGREE EXAMINATION, MONTH & YEAR

Course Code: 221ECS004

Course Name: Computational Intelligence

Max. Marks : 60

Duration: 2.5 Hours

PART A

Answer All Questions. Each Question Carries 5 Marks

1. Consider the set of Colours $A = \{\text{Blue, Red, Orange, Yellow, Green}\}$, Attributes $B = \{\text{Bright, Warmth, Dullness}\}$, Feelings $C = \{\text{Unpleasant, happiness, Angry}\}$. Given R and S where R is the relationship between colours and their attributes and S is the relationship between colour attributes and feelings created. Find the relationship Q between colours and feelings created

| R | Bright | Warmth | Dullness |
|--------|--------|--------|----------|
| Blue | 0.8 | 0.6 | 0.4 |
| Red | 0.8 | 0.8 | 0.2 |
| Orange | 0.5 | 0.7 | 0.2 |
| Yellow | 0.3 | 0.6 | 0.5 |
| Green | 0.8 | 0.6 | 0.4 |

| S | Unpleasant | Happiness | Angry |
|----------|------------|-----------|-------|
| Bright | 0.2 | 0.8 | 0.6 |
| Warmth | 0.4 | 0.7 | 0.8 |
| Dullness | 0.8 | 0.3 | 0.6 |

| | | |
|----|--|----------|
| 2. | Develop a membership function for “Tall”. Based on that devise membership function for “Very Tall”. Explain how it is done | |
| 3. | Mention the importance of objective (fitness) function in genetic algorithm | |
| 4. | Describe how pheromone is updated. What is elitist / elastic ants ? Are they useful in this scenario? | |
| 5. | What is the significance of pbest and gbest particles in solving problems with particle swarm optimization? | (5x5=25) |

Part B
(Answer any five questions. Each question carries 7 marks)

| | | |
|----|--|-----|
| 6. | (a) Consider the set of fruits $F = \{ \text{Apple, Orange, Lemon, Strawberry, Pineapple} \}$. Let sweet fruits $B = \left\{ \frac{0.8}{\text{Apple}} + \frac{0.6}{\text{Orange}} + \frac{0.2}{\text{Lemon}} + \frac{0.4}{\text{Strawberry}} + \frac{0.7}{\text{Pineapple}} \right\}$ and Sour Fruits $F = \left\{ \frac{0.6}{\text{Apple}} + \frac{0.8}{\text{Orange}} + \frac{0.9}{\text{Lemon}} + \frac{0.7}{\text{Strawberry}} + \frac{0.5}{\text{Pineapple}} \right\}$ Find Fruits that are Sweet or Sour, Sweet but not Sour, Sweet and Sour | (3) |
| | (b) Consider two fuzzy Sets given by $P = \left\{ \frac{0.9}{\text{short}} + \frac{0.3}{\text{medium}} + \frac{0.5}{\text{tall}} \right\}$ $Q = \left\{ \frac{0.7}{\text{positive}} + \frac{0.4}{\text{zero}} + \frac{0.8}{\text{negative}} \right\}$ Find the fuzzy relation for the Cartesian product of P and Q i.e, $R = P \times Q$. Introduce a fuzzy set T given by $T = \left\{ \frac{0.9}{\text{short}} + \frac{0.3}{\text{medium}} + \frac{0.6}{\text{tall}} \right\}$ and Find T o R using max-min composition | (4) |

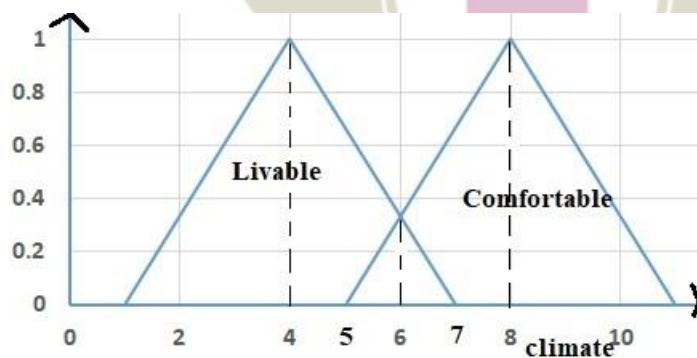
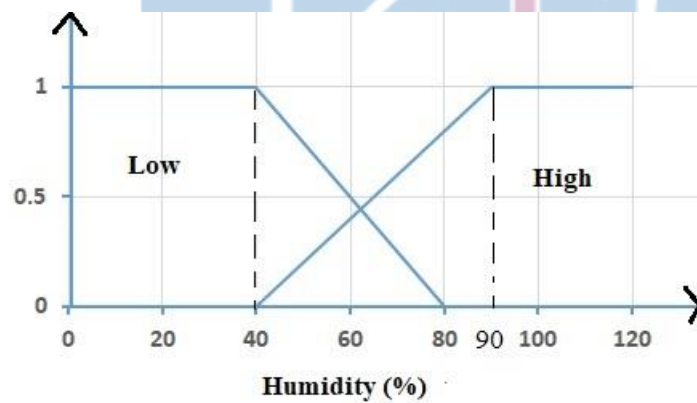
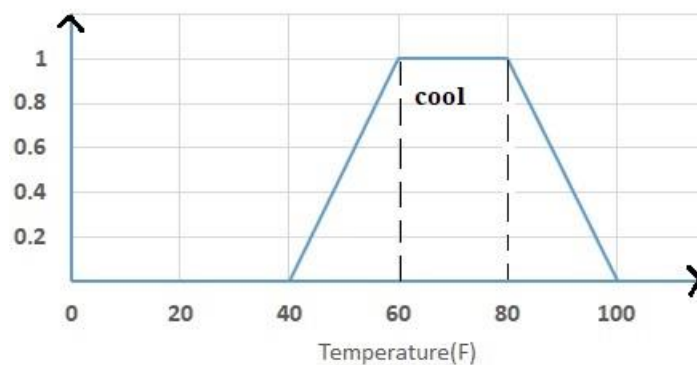
7.

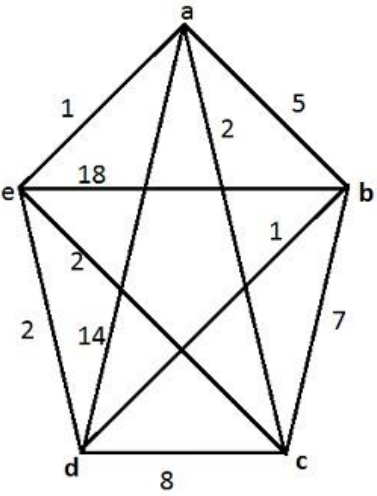
Consider a Fuzzy Inference System for checking climate comfortability of human beings for long time living. The system accepts two inputs – temperature and humidity. The rules and membership functions of FIS is given below. Using Mamdani inference and center of sum, calculate output when the temperature is 50 Fahrenheit and humidity is 50%.

(7)

Rule 1: IF temperature is cool and humidity is low, THEN climate is comfortable.

Rule 2: IF temperature is cool and humidity is high, THEN climate is livable



| | | |
|--------|---|-----|
| | <p>The fuzzy sets “Easy Question Paper” and their corresponding “Student Performance” are given below</p> $\text{Easy_QP} = \left\{ \frac{0.8}{1} + \frac{0.2}{2} + \frac{0.6}{3} + \frac{0.7}{4} \right\}$ $\text{Stud_Perf} = \left\{ \frac{0.3}{a} + \frac{0.4}{b} + \frac{0.8}{c} + \frac{0.9}{d} \right\}$ <p>Find the performance of students c and d for the question paper “Somewhat Easy”</p> $\text{Somewhat_Easy} = \left\{ \frac{0.7}{1} + \frac{0.3}{2} + \frac{0.5}{3} + \frac{0.6}{4} \right\}$ | |
| 8. | Explain any procedure to map a solution to the corresponding chromosome and vice versa in genetic algorithms. Also illustrate it with an example | (7) |
| 9. | Describe two methods used to select individuals from a population for the mating pool in Genetic Algorithms | (7) |
| 10 (a) | <p>Consider the TSP with the following edge costs. Given the evaporation factor $\rho = 0.02$ and initial pheromone at all edges $T_{ij} = 100$</p>  <p>What is the cost of best tour?</p> | (1) |
| (b) | <p>Using the equation $T_{ij}(t+1) = (1-\rho)T_{ij}(t) + \Delta T_{ij}(t,t+1)$, compute the T_{ij} of the edge $\langle a, c \rangle$ when 10 ants uses the edges $\langle a, c \rangle$, using the following models:</p> <ol style="list-style-type: none"> Ant Density Model (Constant $Q=10$) Ant Quantity Model (Constant $Q=100$) <p>where Q is the constant related to the pheromone updation.</p> | (6) |
| 11 | Describe Ant Colony System. What are the different types of Ant systems? | (7) |

| | | |
|-----------|--|------------|
| 12 | <p>Consider a particle swarm optimization system composed of three particles and maximum velocity 10. Assume that both the random numbers r_1 and r_2 used for computing the movement of the particle towards the individual best position and social best position are 0.5. Also assume that the space of solutions is the two-dimensional real valued space and the current state of swarm is as follows:</p> <p style="padding-left: 40px;">Position of particles: $x_1 = (4,4)$; $x_2 = (8,3)$; $x_3 = (6,7)$ Individual best positions: $x_1^* = (4,4)$; $x_2^* = (7,3)$; $x_3^* = (5,6)$ Velocities: $v_1 = (2,2)$; $v_2 = (3,3)$; $v_3 = (4,4)$</p> <p>What would be the next position of each particle after one iteration of the PSO algorithm if the inertia parameter ω that is used along with current velocity update formula is 0.8 ?</p> | (7) |
|-----------|--|------------|

Course Plan (For 3 credit courses, the content can be for 40 hrs and for 2 credit courses, the content can be for 26 hrs. The audit course in third semester can have content for 30 hours).

| No | Topic | No. of Lectures (40) |
|----------|---|----------------------|
| 1 | Module 1 (Fuzzy Logic) | |
| 1.1 | Crisp sets vs fuzzy sets, Operations and properties of Fuzzy sets | 1 |
| 1.2 | Membership functions: features of membership functions | 1 |
| 1.3 | Fuzzification and methods of membership value assignment | 1 |
| 1.4 | Defuzzification-Lambda(alpha) cuts | 1 |
| 1.5 | Fuzzy Relation and fuzzy composition | 1 |
| 1.6 | Operations on fuzzy relations | 1 |
| 2 | Module 2 (Fuzzy Systems) | |
| 2.1 | Linguistic variables and Hedges | 1 |
| 2.2 | Fuzzy Rule Base System-Aggregation of fuzzy rules | 1 |
| 2.3 | Fuzzy Inference System: Mamdani FIS | 1 |
| 2.4 | Larsen Model | 1 |
| 2.5 | Practice Problems on FIS | 1 |
| 2.6 | Fuzzy Reasoning – GMP and GMT (lecture 1) | 1 |
| 2.7 | Fuzzy Reasoning – GMP and GMT (lecture 2) | 1 |
| 2.8 | Practice Problems on Fuzzy Reasoning | 1 |
| 3 | Module 3 (Genetic Algorithms) | |
| 3.1 | Introduction to Genetic algorithm | 1 |

| | | |
|------|--|---|
| 3.2 | chromosomes | 1 |
| 3.3 | Fitness function , Population | 1 |
| 3.4 | GA operators - selection (lecture 1) | 1 |
| 3.5 | GA operators - crossover(lecture 2) | 1 |
| 3.6 | GA operators - mutation(lecture 3) | 1 |
| 3.7 | Elitism, GA parameters ,Convergence of GA | 1 |
| 3.8 | Multi – objective Genetic Algorithm (lecture 1) | 1 |
| 3.9 | Multi – objective Genetic Algorithm (lecture 2) | 1 |
| 4 | Module 4 (Ant Colony Systems) | |
| 4.1 | Introduction, ant colony systems | 1 |
| 4.2 | Types of ant colony systems (lecture 1) | 1 |
| 4.3 | Types of ant colony systems (lecture 2) | 1 |
| 4.4 | Development of the ant colony system | 1 |
| 4.5 | Applications of ant colony intelligence | 1 |
| 4.6 | Working of ant colony systems (lecture 1) | 1 |
| 4.7 | Working of ant colony systems (lecture 2) | 1 |
| 5 | Module 5 (Particle Swarm Optimization) | |
| 5.1 | Basic Model of PSO algorithm- | 1 |
| 5.2 | Global Best PSO | 1 |
| 5.3 | Local Best PSO, Comparison of ‘gbest’ to ‘lbest’ | 1 |
| 5.4 | PSO Algorithm Parameters | 1 |
| 5.5 | Problem Formulation of PSO algorithm (lecture 1) | 1 |
| 5.6 | Problem Formulation of PSO algorithm (lecture 2) | 1 |
| 5.7 | Velocity clamping- Inertia weight | 1 |
| 5.8 | Constriction Coefficient- Boundary Conditions | 1 |
| 5.9 | Guaranteed Convergence PSO (GCPSO) | 1 |
| 5.10 | Initialization, Stopping Criteria, Iteration Terms and Function Evaluation | 1 |



| CODE | COURSE NAME | CATEGORY | L | T | P | CREDIT |
|-----------|--------------------------|--------------------|---|---|---|--------|
| 22IECS034 | WEB APPLICATION SECURITY | Program Elective 1 | 3 | 0 | 0 | 3 |

Preamble: This course basically aims at exploring the fundamentals of Web applications & and an in-depth study of Common Vulnerabilities and exploits. The course also covers the different information Gathering methodologies and the different mitigation and management strategies. The concepts covered in this course also enable the learners in effective use of web application development Technologies and to identify the security threats in computing and to discover the vulnerabilities in web applications.

Course Outcomes: After the completion of the course the student will be able to

| CO# | Course Outcomes |
|-----|--|
| CO1 | Identify the basic type of web application security testing, vulnerabilities and countermeasures. (Cognitive Knowledge Level: Apply) |
| CO2 | Trace out the different Information Gathering methodologies. (Cognitive Knowledge Level: Apply) |
| CO3 | Interpret and detect the different vulnerabilities and exploits prone to systems. (Cognitive Knowledge Level: Apply) |
| CO4 | Discover and detect Web Application Vulnerabilities & threats and adopt mitigation and management Strategies. (Cognitive Knowledge Level: Analyse) |
| CO5 | Investigate the different web application development Technologies. (Cognitive Knowledge Level: Analyse) |
| CO6 | Conduct Penetration testing on Common vulnerabilities and exploits and review the amount of vulnerabilities in it (Cognitive Knowledge Level: Evaluate) |

Program Outcomes (PO)

Outcomes are the attributes that are to be demonstrated by a graduate after completing the course.

PO1: An ability to independently carry out research/investigation and development work in engineering and allied streams

PO2: An ability to communicate effectively, write and present technical reports on complex engineering activities by interacting with the engineering fraternity and with society at large.

PO3: An ability to demonstrate a degree of mastery over the area as per the specialization of the program. The mastery should be at a level higher than the requirements in the appropriate bachelor program



































PO4: An ability to apply stream knowledge to design or develop solutions for real world problems by following the standards

PO5: An ability to identify, select and apply appropriate techniques, resources and state-of-the-art tool to model, analyse and solve practical engineering problems.

PO6: An ability to engage in life-long learning for the design and development related to the stream related problems taking into consideration sustainability, societal, ethical and environmental aspects

PO7: An ability to develop cognitive load management skills related to project management and finance which focus on Entrepreneurship and Industry relevance.

Mapping of course outcomes with program outcomes

| | PO 1 | PO 2 | PO 3 | PO 4 | PO 5 | PO 6 | PO 7 |
|------|---|---|---|---|---|---|---|
| CO 1 |  | |  |  |  |  |  |
| CO 2 |  | |  |  |  |  | |
| CO 3 |  | |  |  |  |  |  |
| CO 4 |  | |  |  |  |  | |
| CO 5 |  | |  |  |  |  | |
| CO 6 |  |  |  |  |  |  |  |

Assessment Pattern

| Bloom's Category | End Semester Examination |
|------------------|--------------------------|
| Apply | 60% |
| Analyse | 30% |
| Evaluate | 10% |
| Create | |

Mark distribution

| Total Marks | CIE | ESE | ESE Duration |
|-------------|-----|-----|--------------|
| 100 | 40 | 60 | 2.5 hours |

Continuous Internal Evaluation Pattern:

Evaluation shall only be based on application, analysis or design-based questions (for both internal and end semester examinations).

Continuous Internal Evaluation: 40 marks

- i. Preparing a review article based on peer reviewed original publications (minimum 10 publications shall be referred) : 15 marks
- ii. Course based task / Seminar/ Data collection and interpretation : 15 marks
- iii. Test paper (1 number) : 10 marks

Test paper shall include minimum 80% of the syllabus.

Course based task/test paper questions shall be useful in the testing of knowledge, skills, comprehension, application, analysis, synthesis, evaluation and understanding of the students.

End Semester Examination Pattern:

The end semester examination will be conducted by the respective College.

There will be two parts; Part A and Part B.

Part A will contain 5 numerical/short answer questions with 1 question from each module, having 5 marks for each question. Students should answer all questions. Part B will contain 7 questions (such questions shall be useful in the testing of overall achievement and maturity of the students in a course, through long answer questions relating to theoretical/practical knowledge, derivations, problem solving and quantitative evaluation), with minimum one question from each module of which student should answer any five. Each question can carry 7 marks

Total duration of the examination will be 150 minutes.

Note: The marks obtained for the ESE for an elective course shall not exceed 20% over the average ESE mark % for the core courses. ESE marks awarded to a student for each elective course shall be normalized accordingly.

For example if the average end semester mark % for a core course is 40, then the maximum eligible mark % for an elective course is $40+20 = 60\%$.

Syllabus

MODULE -1 (INTRODUCTION TO WEB APPLICATION)

Web Application, Web Client, History of Web Application, Web Application Security Terminology, Types of Web Application Security Testing, Web Application Vulnerabilities and Counter measures.

MODULE -2 (RECONNAISSANCE)

Web Application Reconnaissance: Information Gathering, Web Application Mapping. Finding Subdomains- Multiple Applications per Domain, Browser's Built-in Network Analysis Tools, Public Records, Brute Forcing Subdomain, Dictionary Attacks.

MODULE -3 (WEB APPLICATION OFFENSE)

Cross-Site Scripting (XSS)- XSS Discovery & Exploitation, Stored XSS, Reflected XSS. Cross-Site Request Forgery- Query Parameter Tampering. XML External Entity (XXE)- Direct XXE, Indirect XXE. Injection- SQL Injection, Code Injection. Denial of Service- Logical DoS Vulnerabilities, Distributed DoS.

MODULE -4 (SECURING AND HARDENING WEB APPLICATIONS)

Securing Modern Web Applications- Defensive Software Architecture, Vulnerability Discovery, Vulnerability Analysis, Vulnerability Management, Mitigation Strategies. Secure Application Architecture: Authentication and Authorization. Vulnerability Discovery: Security Automation. Vulnerability Management: Common Vulnerability Scoring System. Securing Sessions: Different types of Sessions, Data Transmission Security: SSL/TLS: Certificate Validation Types and Authorities, Creating Self-Signed Certificate for Testing, OWASP Top 10 Vulnerabilities, Penetration Testing.

MODULE -5 (WEB APPLICATION DEVELOPMENT TECHNOLOGIES)

Basic workflow with a text editor, version control system, and web browser, user interface with HTML, styles with CSS, JQuery and JavaScript, AJAX, JavaScript objects, and JSON, Server-side programming with Node.js, Storage with Redis and MongoDB, Cloud uploading Cloud Foundry.

Text Books

1. Ron Lepofsky, "The Manager's Guide to Web Application Security: A Concise Guide to the weaker side of the web", First Edition, Apress, 2015.

2. Andrew Hoffman “Web Application Security: Exploitation and Countermeasures for Modern Web Applications”, O’Reilly, First Edition, 2020.

Reference Books

1. Semmy Purewal “Learning Web App Development”, O’Reilly Media, Inc., First Edition, 2014
2. Jonathan LeBlanc & Tim Messerschmidt ,”Identity and Data Security for Web Development”, O’Reilly, First Edition, 2016
3. Bryan Sullivan, Vincent Liu “Web Application Security, A Beginners Guide”, McGraw-Hill First Edition, 2011

Course Level Assessment Questions

Course Outcome 1 (CO1):

1. Consider an automated teller machine (ATM) in which users provide a personal identification number (PIN) and a card for account access. Give examples of confidentiality, integrity, and availability requirements associated with the system and, in each case, indicate the degree of importance of the requirement.

Course Outcome 2 (CO2):

1. Information about a particular website is crucial for the hackers and intruders to pierce into the system. Explain how the information be gathered and give what all information are crucial for the users to safeguard their systems from intruder attacks. Use any appropriate tool.

Course Outcome 3 (CO3):

1. What is Cross site Scripting? Do analysis on a website by giving an input test case and identify whether it is present on the website?
2. What is SQL injection? Apply test cases and find whether the website is affected by SQL injection?

Course Outcome 4 (CO4):

1. What is vulnerability? Write down its importance. How is it identified?
2. How Vulnerability management is done?

Course Outcome 5 (CO5):

1. Discuss the role of styles in a website. Use a web development technology to design a page by Creating Styles.
2. Explain how data is shared to cloud using Cloud Front.

Course Outcome 6 (CO5):

1. Conduct a penetration testing on the XSS on a website and report the vulnerabilities caused.



Model Question Paper

QP CODE:

Reg No: _____

Name: _____

PAGES : 4

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

FIRST SEMESTER M.TECH DEGREE EXAMINATION, MONTH & YEAR

Course Code: 221ECS034

Course Name: WEB APPLICATION SECURITY

Max. Marks: 60

Duration: 2.5 Hours

PART A

Answer All Questions. Each Question Carries 5 Marks

| | | |
|----|---|----------|
| 1. | How can you identify a Web application vulnerability? | |
| 2. | How is brute forcing applied on a subdomain to extract the details of exposures? | |
| 3. | What is Cross site Request Forgery? How is it identified. | |
| 4. | With examples, differentiate between authentication and Authorization. | |
| 5. | Enumerate how to Structure a user interface with HTML, and include styles with CSS. | (5x5=25) |

Part B

(Answer any five questions. Each question carries 7 marks)

| | | |
|----|---|-----|
| 6. | Apply any three web application vulnerabilities on a website and write down the damages they cause. | (7) |
| 7. | (a) Using a tool trace out the subdomain information about a website. | (4) |
| | (b) Write down the components of a Web Application | (3) |
| 8. | (a) What is XML External Entity(XEE)? Showcase how it affects a website? | (4) |
| | (b) How Vulnerability Management is done using Common Vulnerability Scoring System? | (3) |
| 9. | How a network analysis is done using the Built-in Network Analysis Tools found in a browser? Perform an analysis and report the result. | (7) |
| 10 | (a) What is JSON? Explain its relevance in Website development | (4) |

| | | | |
|----|-----|--|-----|
| | (b) | SSL/TLS validation is important in securing a website. Show how it can be done. | (3) |
| 11 | | Give the different Logical DoS Vulnerabilities with suitable scenarios of exploitation . | (7) |
| 12 | | With a tool, show how server-side programming be done with Node.js | (7) |

Course Plan (For 3 credit courses, the content can be for 40 hrs and for 2 credit courses, the content can be for 26 hrs. The audit course in third semester can have content for 30 hours).

| No | Topic | No. of Lectures (40) |
|-----|--|----------------------|
| 1 | Module -1 (Introduction to Web Application) (6 hrs) | |
| 1.1 | Web Application and Web Client | 1 |
| 1.2 | History of Web Application | 1 |
| 1.3 | Web Application Security Terminology | 1 |
| 1.4 | Types of Web Application Security Testing- Lecture 1 | 1 |
| 1.5 | Types of Web Application Security Testing- Lecture 2 | 1 |
| 1.6 | Web Application Vulnerabilities and Counter measures | 1 |
| 2 | Module -2 (Reconnaissance) (7 hrs) | |
| 2.1 | Web Application Reconnaissance: Information Gathering | 1 |
| 2.2 | Web Application Mapping | 1 |
| 2.3 | Finding Subdomains | 1 |
| 2.4 | Multiple Applications per Domain | 1 |

| | | |
|----------|---|---|
| 2.5 | Browser's Built-in Network Analysis Tools- Lecture 1 | 1 |
| 2.6 | Browser's Built-in Network Analysis Tools- Lecture 2 | 1 |
| 2.7 | Public Records, Brute Forcing Subdomain, Dictionary Attacks | 1 |
| 3 | Module -3 (Web Application Offense) (9 hrs) | |
| 3.1 | Cross-Site Scripting (XSS) | 1 |
| 3.2 | XSS Discovery & Exploitation | 1 |
| 3.3 | Stored XSS | 1 |
| 3.4 | Reflected XSS | 1 |
| 3.5 | Cross- Site Request Forgery- Query Parameter Tampering | 1 |
| 3.6 | XML External Entity (XXE) | 1 |
| 3.7 | Direct XXE, Indirect XXE | 1 |
| 3.8 | Injection- SQL Injection, Code Injection | 1 |
| 3.9 | Denial of Service- Logical DoS Vulnerabilities, Distributed DoS | 1 |
| 4 | Module -4 (Securing and Hardening Web Applications) (11 hrs) | |
| 4.1 | Securing Modern Web Applications | 1 |
| 4.2 | Defensive Software Architecture, Vulnerability Discovery | 1 |
| 4.3 | Vulnerability Analysis, Vulnerability Management | 1 |
| 4.4 | Mitigation Strategies | 1 |

| | | |
|----------|--|---|
| 4.5 | Secure Application Architecture: Authentication and Authorization. | 1 |
| 4.6 | Vulnerability Discovery: Security Automation. | 1 |
| 4.7 | Vulnerability Management: Common Vulnerability Scoring System. | 1 |
| 4.8 | Securing Sessions: Different types of Sessions, | 1 |
| 4.9 | Data Transmission Security: SSL/TLS: Certificate Validation Types and Authorities, Creating Self-Signed Certificate for Testing, | 1 |
| 4.10 | OWASP Top 10 Vulnerabilities | 1 |
| 4.11 | OWASP Top 10 Vulnerabilities and Penetration Testing | 1 |
| 5 | Module –5 (Web Application Development Technologies) (7 hrs) | |
| 5.1 | Basic workflow with a text editor, version control system, and web browser | 1 |
| 5.2 | User interface with HTML, Styles with CSS | 1 |
| 5.3 | JQuery and JavaScript | 1 |
| 5.4 | AJAX, JavaScript objects, and JSON | 1 |
| 5.5 | Server-side programming with Node.js | 1 |
| 5.6 | Storage with Redis and MongoDB | 1 |
| 5.7 | Cloud uploading CloudFoundry | 1 |

| | | | | | | |
|-----------|------------------------|--------------------|---|---|---|--------|
| 221ECS035 | Optimization Technique | CATEGORY | L | T | P | CREDIT |
| | | Program Elective 1 | 3 | 0 | 0 | 3 |

Preamble: The fundamental theories of optimization and various techniques that are used in all engineering specialties are covered. The discussion of linear programming issues and various approaches, algorithms and strategies for reaching solutions are covered. The idea of linear optimization is also covered in this course as a technique of solving transportation and assignment issues. Additionally, the course covers a diversity of non-linear optimization methods.

Course Outcomes: After the completion of the course the student will be able to

| | |
|------|--|
| CO 1 | Generate linear programming problems out of real-world optimization issues, then use the graphical or simplex method to solve them. (Cognitive Knowledge level: Apply) |
| CO 2 | Recognize the linear programming idea of duality and its application. (Cognitive Knowledge level : Apply) |
| CO 3 | Use the ideologies of linear optimization to locate transportation and assignment issues and resolve them. (Cognitive Knowledge level : Apply) |
| CO 4 | Learn how to manage complicated projects using the right strategies, including sequencing and scheduling issues. (Cognitive Knowledge level: Analyze) |
| CO5 | Learn how to recognize and categorize non-linear optimization issues and how to solve them effectively. (Cognitive Knowledge level: Analyze) |

Program Outcomes (PO)

Outcomes are the attributes that are to be demonstrated by a graduate after completing the course.

PO1: An ability to independently carry out research/investigation and development work in engineering and allied streams

PO2: An ability to communicate effectively, write and present technical reports on complex engineering activities by interacting with the engineering fraternity and with society at large.

PO3: An ability to demonstrate a degree of mastery over the area as per the specialization of the program. The mastery should be at a level higher than the requirements in the appropriate bachelor program

PO4: An ability to apply stream knowledge to design or develop solutions for real world problems by following the standards

PO5: An ability to identify, select and apply appropriate techniques, resources and state-of-the-art tool to model, analyse and solve practical engineering problems.

PO6: An ability to engage in life-long learning for the design and development related to the stream related problems taking into consideration sustainability, societal, ethical and environmental aspects

PO7: An ability to develop cognitive load management skills related to project management and finance which focus on Entrepreneurship and Industry relevance.

Mapping of course outcomes with program outcomes

| | PO1 | PO2 | PO3 | PO4 | PO5 | PO6 | PO7 |
|------|-----|-----|-----|-----|-----|-----|-----|
| CO 1 | √ | √ | √ | √ | √ | √ | |
| CO 2 | √ | √ | √ | √ | √ | √ | |
| CO 3 | √ | √ | √ | √ | √ | √ | |
| CO 4 | √ | √ | √ | √ | √ | √ | |
| CO5 | √ | √ | √ | √ | √ | √ | |

Assessment Pattern

| Bloom's Category | End Semester Examination marks |
|------------------|--------------------------------|
| Apply | 70%-80% |
| Analyse | 10% -20% |
| Evaluate | 10% |
| Create | |

Mark Distribution

| Total Marks | CIE Marks | ESE Marks | ESE Duration |
|-------------|-----------|-----------|--------------|
| 100 | 40 | 60 | 2.5 hours |

Continuous Internal Evaluation: 40 marks

Preparing a review article based on peer reviewed

Original publications (minimum 10 publications shall be referred): 15 marks

Course based task/Seminar/Data collection and interpretation: 15 marks

Test paper, 1 number: 10 marks

Test paper shall include minimum 80% of the syllabus.

End Semester Examination: 60 marks

The end semester examination will be conducted by the respective College. There will be two parts; Part A and Part B. Part A will contain 5 numerical/short answer questions with 1 question from each module, having 5 marks for each question (such questions shall be useful in the testing of knowledge, skills, comprehension, application, analysis, synthesis, evaluation and understanding of the students). Students should answer all questions. Part B will contain 7 questions (such questions shall be useful in the testing of overall achievement and maturity

of the students in a course, through long answer questions relating to theoretical/practical knowledge, derivations, problem solving and quantitative evaluation), with minimum one question from each module of which student should answer any five. Each question can carry 7 marks

Syllabus

Module 1

Linear Programming- Linear Programming Problem (LPP), Slack-Surplus Variable, Graphical solution of a LPP, Exceptional cases in Graphical Method, Formulation of LPP, Simplex Method, Artificial variable method, Big-M method, Two-Phase method

Module 2

Duality in Linear Programming- Canonical form of an LPP, Dual of an LPP, Dual Simplex Method, Basics of Sensitivity Analysis.

Module 3

Transportation and Assignment Problem- Transportation Problem, Balanced Transportation Problem, Unbalanced Transportation Problem, North-West Corner Method (NMC), Least Cost Entry Method (LCM), Vogel's Approximation Method (VAM), Degeneracy in Transportation Problems, Assignment Problem, Mathematical Formulation of the Assignment, Hungarian Algorithm to Solve an Assignment Problem.

Module 4

Integer Linear Programming, Travelling Salesman problem and Networking- All Integer ILPP, Gomory's Cutting Plane Method, Mixed Integer Linear Programming Problems, Branch and Bound Techniques, Travelling Salesman Problem, Networking- Critical Path Method (CPM), Program Evaluation and Review Technique (PERT), Optimum Scheduling by CPM.

Module 5

Non-Linear Programming- Quadratic Form, Method of Testing of a Quadratic Form, Conventional Method of Optimization, Convex Functions, Convex Nonlinear Programming Problem (CNLPP), Constraint Qualification (CQ), Quadratic Programming, Separable Programming.

Text Book

1. C.B. Gupta, Optimization Techniques in Operations Research, I.K. International Publishing House Pvt. Ltd., New Delhi, 2008.
2. Frederick S Hillier, Gerald J. Lieberman, Introduction to Operations Research, Seventh Edition, McGraw-Hill Higher Education, 1967. 2. Kanti Swarup, P. K. Gupta, Man Mohan, Operations Research, Sultan Chand & Sons, New Delhi, 2008.

Reference books:

1. Singiresu S Rao, Engineering Optimization: Theory and Practice ,New Age International Publishers, 1996
2. H A Taha, Operations research : An introduction , Macmillon Publishing company,1976
3. B. S. Goel, S. K. Mittal, Operations research, Pragati Prakashan, 1980
4. S.D Sharma, "Operation Research", Kedar Nath and RamNath - Meerut , 2008.
5. Phillips, Solberg Ravindran ,Operations Research: Principles and Practice, Wiley,2007

Course Level Assessment Questions

Course Outcome 1 (CO1):

1) Using Simplex method solve the following LPP:

$$\text{Max } Z = x_1 + x_2 + 3x_3$$

Subject to constrain:

$$3x_1 + 2x_2 + x_3 \leq 3$$

$$2x_1 + x_2 + 2x_3 \leq 2$$

$$x_1, x_2, x_3 \geq 0$$

Course Outcome 2 (CO2):

1) Formulate the dual of the LPP

$$\text{Maximize } Z = 5x_1 + 6x_2$$

Subject to constraints:

$$x_1 + 9x_2 \geq 60$$

$$2x_1 + 3x_2 \leq 45$$

$$x_1, x_2 \geq 0$$

Course Outcome 3 (CO3):

Distinguish transportation problem from assignment problem.

Course Outcome 4 (CO4):

Use Branch and Bound Technique to solve (5 Marks)

$$\text{Minimize } Z = -3x_1 - 4x_2$$

Subject to constraints:

$$3x_1 - x_2 \leq 12$$

$$3x_1 + 11x_2 \leq 66$$

$$x_1, x_2 \geq 0 \text{ and integers}$$

Course Outcome 5 (CO5):

Prove that the set S_f of BFS of a CNLPP is Convex

MODEL QUESTION PAPER:

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY
FIRST SEMESTER M. TECH DEGREE EXAMINATION
221ECS035 Optimization Technique

PART A MULTIPLE CHOICE

Each question carries FIVE marks
60 minutes

- 1) Using Simplex method solve the following LPP: (5 Marks)

$$\text{Max } Z = x_1 + x_2 + 3x_3$$

Subject to constrain:

$$3x_1 + 2x_2 + x_3 \leq 3$$

$$2x_1 + x_2 + 2x_3 \leq 2$$

$$x_1, x_2, x_3 \geq 0$$

- 2) Formulate the dual of the LPP (5 Marks)

$$\text{Maximize } Z = 5x_1 + 6x_2$$

Subject to constraints:

$$x_1 + 9x_2 \geq 60$$

$$2x_1 + 3x_2 \leq 45$$

$$x_1, x_2 \geq 0$$

- 3) Distinguish transportation problem from assignment problem. (5 Marks)

- 4) Use Branch and Bound Technique to solve (5 Marks)

$$\text{Minimize } Z = -3x_1 - 4x_2$$

Subject to constraints:

$$3x_1 - x_2 \leq 12$$

$$3x_1 + 11x_2 \leq 66$$

$$x_1, x_2 \geq 0 \text{ and integers}$$

- 5) Prove that the set S_f of BFS of a CNLPP is Convex. (5 Marks)

PART B- Offline mode

Each question carries SEVEN marks

Answer any FIVE full questions

90 minutes

- 6) Use Big-M method to solve the following LPP (7 marks)

$$\text{Minimize } Z = 3x_1 + 2x_2$$

Subject to constrain:

$$\begin{aligned}x_1 + x_2 &\geq 2 \\x_1 + 3x_2 &\leq 3 \\x_1 - x_2 &= 1 \\x_1, x_2 &\geq 0\end{aligned}$$

7) Prove that: If primal P has an optimal solution, then its Dual D also has an optimal solution. (7 marks)

8) Use dual simplex method to solve the following LPP. (7 marks)

$$\text{Minimize } Z = 4x_1 + 9x_2$$

Subject to constraints:

$$\begin{aligned}x_1 + x_2 &\geq 6 \\2x_1 + 3x_2 &\geq 18 \\x_1, x_2 &\geq 0\end{aligned}$$

9) Solve the following LPP by two-phase method (7 marks)

$$\text{Maximize } Z = 3x_1 - x_2$$

Subject to constraints:

$$\begin{aligned}2x_1 + x_2 &\geq 2 \\x_1 + 3x_2 &\leq 3 \\x_2 &\leq 4 \\x_1, x_2 &\geq 0\end{aligned}$$

10) Outline the algorithm for VAM. (7 marks)

11) Solve the following using Gomory's cutting plane method (7 marks)

$$\text{Minimize } Z = -5x_1 - 7x_2$$

Subject to constraints:

$$\begin{aligned}-x_1 + 3x_2 &\leq 5 \\5x_1 + x_2 &\leq 15 \\x_1, x_2 &\geq 0 \text{ and integers}\end{aligned}$$

12) Prove that $f(X) = C^T X - K$ is a convex function. (7 marks)

| Course Plan | | |
|-------------|--|-----------------|
| No | Topic | No. of Lectures |
| | Linear Programming -Module 1 | 8 |
| 1.1 | Linear Programming Problem (LPP) | 1 |
| 1.2 | Slack-Surplus Variable, Graphical solution of a LPP, | 2 |
| 1.3 | Exceptional cases in Graphical Method, Formulation of LPP, | 1 |
| 1.4 | Simplex Method | 1 |
| 1.5 | Artificial variable method | 1 |
| 1.6 | Big-M method | 1 |
| 1.7 | Two-Phase method | 1 |
| | Duality in Linear Programming -Module 2 | 8 |
| 2.1 | Duality in Linear Programming | 2 |
| 2.2 | Canonical form of an LPP | 1 |
| 2.3 | Dual of an LPP | 2 |
| 2.4 | Dual Simplex Method | 2 |
| 2.5 | Basics of Sensitivity Analysis | 1 |

| | | |
|-----|---|----------|
| | Transportation and Assignment Problem -Module-III | 8 |
| 3.1 | Transportation Problem | 1 |
| 3.2 | Balanced Transportation Problem | 1 |
| 3.3 | Unbalanced Transportation Problem | 1 |
| 3.4 | North-West Corner Method (NMCM), Least Cost Entry Method (LCM) and Vogel's Approximation Method (VAM) | 2 |
| 3.5 | Degeneracy in Transportation Problems | 1 |
| 3.6 | Assignment Problem, Mathematical Formulation of the Assignment | 1 |
| 3.7 | Hungarian Algorithm to Solve an Assignment Problem. | 1 |
| | Integer Linear Programming, Travelling Salesman problem and Networking - Module-IV | 8 |
| 4.1 | All Integer ILPP | 1 |
| 4.2 | Gomory's Cutting Plane Method | 1 |
| 4.3 | Mixed Integer Linear Programming Problems | 1 |
| 4.4 | Branch and Bound Techniques | 1 |
| 4.5 | Travelling Salesman Problem | 1 |
| 4.6 | Critical Path Method (CPM) | 1 |
| 4.7 | Program Evaluation and Review Technique (PERT) | 1 |
| 4.8 | Optimum Scheduling by CPM. | 1 |
| | Non-Linear Programming- Module-V | 8 |
| 5.1 | Quadratic Form | 1 |
| 5.2 | Method of Testing of a Quadratic Form | 1 |
| 5.3 | Conventional Method of Optimization | 1 |

| | | |
|-----|---|---|
| 5.4 | Convex Functions | 1 |
| 5.5 | Convex Nonlinear Programming Problem (CNLPP) | 2 |
| 5.6 | Constraint Qualification (CQ) | 1 |
| 5.7 | Quadratic Programming, Separable Programming. | 1 |



| | | | | | | |
|-----------|--------------------|--------------------|---|---|---|--------|
| 221ECS036 | TOPICS IN NETWORKS | CATEGORY | L | T | P | CREDIT |
| | | PROGRAM ELECTIVE 1 | 3 | 0 | 0 | 3 |

Preamble:

This course enables the learners to get a good grasp of emerging technologies in the field of computer networks. The syllabus dwells at length on wireless networking, as well as solutions for problems faced while efficiently routing data. Newer networking applications and protocols particularly in multimedia are introduced. The learners are given a glimpse of recent trends in networking like software defined networking. The course enables the learners to analyse network protocols and develop network-based applications.

Course Outcomes:

After the completion of the course the student will be able to

| | |
|-------------|---|
| CO 1 | Examine the problem of scalability for routing and also identify the challenges in mobile and multicast routing (Cognitive knowledge: Analyze) |
| CO 2 | Choose the technique that provides the Quality-of-Service needs of a particular application. (Cognitive knowledge: Apply) |
| CO 3 | Survey various wired and wireless networking technologies including wireless cellular technologies. (Cognitive knowledge: Analyze) |
| CO 4 | Classify the multimedia applications in the Internet and compile the various protocols handling these applications. (Cognitive knowledge: Analyze) |
| CO 5 | Describe examples of current networking trends and identify the technological gaps (Cognitive knowledge: Evaluate) |

Program Outcomes (PO)

Outcomes are the attributes that are to be demonstrated by a graduate after completing the course.

- PO1:** An ability to independently carry out research/investigation and development work in engineering and allied streams
- PO2:** An ability to communicate effectively, write and present technical reports on complex engineering activities by interacting with the engineering fraternity and with society at large.
- PO3:** An ability to demonstrate a degree of mastery over the area as per the specialization of the program. The mastery should be at a level higher than the requirements in the appropriate bachelor program
- PO4:** An ability to apply stream knowledge to design or develop solutions for real world problems by following the standards
- PO5:** An ability to identify, select and apply appropriate techniques, resources and state-of-the-art tool to model, analyse and solve practical engineering problems.
- PO6:** An ability to engage in life-long learning for the design and development related to the stream related problems taking into consideration sustainability, societal, ethical and environmental aspects
- PO7:** An ability to develop cognitive load management skills related to project management and finance which focus on Entrepreneurship and Industry relevance.

Mapping of course outcomes with program outcomes

| | PO 1 | PO 2 | PO 3 | PO 4 | PO 5 | PO 6 | PO 7 |
|------|------|------|------|------|------|------|------|
| CO 1 | ☑ | | ☑ | ☑ | ☑ | ☑ | |
| CO 2 | ☑ | | ☑ | ☑ | ☑ | ☑ | |
| CO 3 | ☑ | | ☑ | ☑ | ☑ | ☑ | |
| CO 4 | ☑ | | ☑ | ☑ | ☑ | ☑ | |
| CO 5 | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |

Assessment Pattern

| Bloom's Category | End Semester Examination |
|------------------|--------------------------|
| Apply | 70%-80% |
| Analyse | 30%-40% |
| Evaluate | |
| Create | |

Mark distribution

| Total Marks | CIE | ESE | ESE Duration |
|-------------|-----|-----|--------------|
| 100 | 40 | 60 | 2.5 hours |

Continuous Internal Evaluation Pattern:

Evaluation shall only be based on application, analysis or design-based questions (for both internal and end semester examinations).

Continuous Internal Evaluation: 40 marks

- i. Preparing a review article based on peer reviewed original publications (minimum 10 publications shall be referred) : 15 marks
- ii. Course based task / Seminar/ Data collection and interpretation : 15 marks
- iii. Test paper (1 number) : 10 marks

Test paper shall include minimum 80% of the syllabus.

Course based task/test paper questions shall be useful in the testing of knowledge, skills, comprehension, application, analysis, synthesis, evaluation and understanding of the students.

End Semester Examination Pattern:

The end semester examination will be conducted by the respective College.

There will be two parts; Part A and Part B.

Part A will contain 5 numerical/short answer questions with 1 question from each module, having 5 marks for each question. Students should answer all questions. Part B will contain 7 questions (such questions shall be useful in the testing of overall achievement and maturity of the students in a course, through long answer questions relating to theoretical/practical knowledge, derivations, problem solving and quantitative evaluation), with minimum one question from each module of which student should answer any five. Each question can carry 7 marks

Total duration of the examination will be 150 minutes.

Note: The marks obtained for the ESE for an elective course shall not exceed 20% over the average ESE mark % for the core courses. ESE marks awarded to a student for each elective course shall be normalized accordingly.

For example if the average end semester mark % for a core course is 40, then the maximum eligible mark % for an elective course is $40+20 = 60$ %.

Syllabus

Module 1 (Advanced Internetworking)

The Global Internet, Routing Areas, Interdomain Routing -BGP, IP Version 6, Multicast, Multicast Addresses, Multicast Routing -DVMRP-PIM-MSDP, Routing to a mobile node, Mobile IP, TCP and Mobility, Mobile TCP

Module 2 (Internetwork Quality of Service)

QoS Architectural Framework - Integrated Services Architecture – RSVP - Differentiated Services, Multiprotocol Label Switching- Destination-Based Forwarding - Explicit Routing Virtual Private Networks and Tunnels, Performance issues in networks, Delay Tolerant Networking

Module 3 (Networking Technologies)

Wired: DSL, Cable Networks, SONET, ATM, VLAN, Wireless: Satellite Networks, WiMAX

Cellular Networks: Introduction-Wireless links and Network characteristics -CDMA, Cellular Internet access -An overview of cellular network architecture, 3G cellular data networks, 4G LTE Cellular networks - LTE Protocol Stacks -LTE Radio Access Network -Additional LTE functions, 5G Cellular networks, Managing mobility in cellular networks, Wireless and Mobility-Impact on higher level protocols, Personal Area Networks: Bluetooth, Zigbee

Module 4 (Networking Applications)

Multimedia in the Internet: Streaming stored audio/video, Streaming live audio/video, Real time interactive audio/video, Real time Interactive Protocols: RTP- RTCP-SIP-H.323, SCTP Compression: Audio Compression, Image compression- JPEG, Video Compression- MPEG

Module 5 (Current Topics in Networking)

Overlay Networks: Routing overlays -Resilient overlay networks, Peer-Peer Networks – Bit Torrent-Distributed Hash Tables, Content Distribution networks, Software Defined Networks: Architecture – Control and Data Planes – Open Flow – SDN Controllers, Network Function Virtualization, Data Center Networking

Reference Books

1. Larry Peterson and Bruce Davie, Computer Networks - A Systems Approach, Morgan Kaufmann, 6th edition, 2022
2. James F. Kurose and Keith W. Ross, Computer Networking A Top-Down Approach, Pearson, 8th edition, 2022
3. Jochen Schiller, Mobile Communications, Addison-Wesley, 2nd edition, 2003
4. William Stallings, Data and Computer Communications, Pearson, 5th edition, 2017
5. Andrew Tanenbaum and David Wetherall, Computer Networks, Pearson, 5th edition, 2010
6. Behrouz A Forouzan, Data Communications and Networking, McGraw Hill, 5th edition, 2017
7. Thomas D. Nadeau and Ken Gray, SDN – Software Defined Networks, O'Reilly, 2013

Course Level Assessment Questions

Course Outcome 1 (CO1):

1. Examine how IPV6 deals with the scalability problem in routing.
- 2 Distinguish the various approaches in multicast routing.
3. How is the problem of mobility solved in mobile routing?

Course Outcome 2 (CO2)

1. List the categories of service offered by ISA.
2. Examine the role of MPLS in Internet traffic management.
3. Examine the issues affecting network performance and suggest solutions for the same.

Course Outcome 3(CO3):

1. Choose the network technology that can be used to cover areas that cannot support sufficient infrastructure.
2. Show the evolution of cellular technologies from 3G to 5G.
3. Compare the media access techniques of Bluetooth and Zigbee.

Course Outcome 4 (CO4):

1. Categorize the multimedia applications on the Internet and briefly explain their characteristics.
2. Illustrate how real time protocols support interactive applications like VoIP.
3. Justify the need for compressing audio and video before sending it over the Internet.

Course Outcome 5 (CO5):

1. How do overlay networks introduce new functionality into the Internet?
2. Point out the concept behind software defined networking.
3. A new routing protocol is to be implemented in the SDN control plane. Choose the appropriate layer where it should be implemented giving reasons for the same.

| | |
|--|---------|
| Model Question Paper | |
| QP CODE: | |
| Reg No: _____ | |
| Name: _____ | PAGES : |
| APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY | |

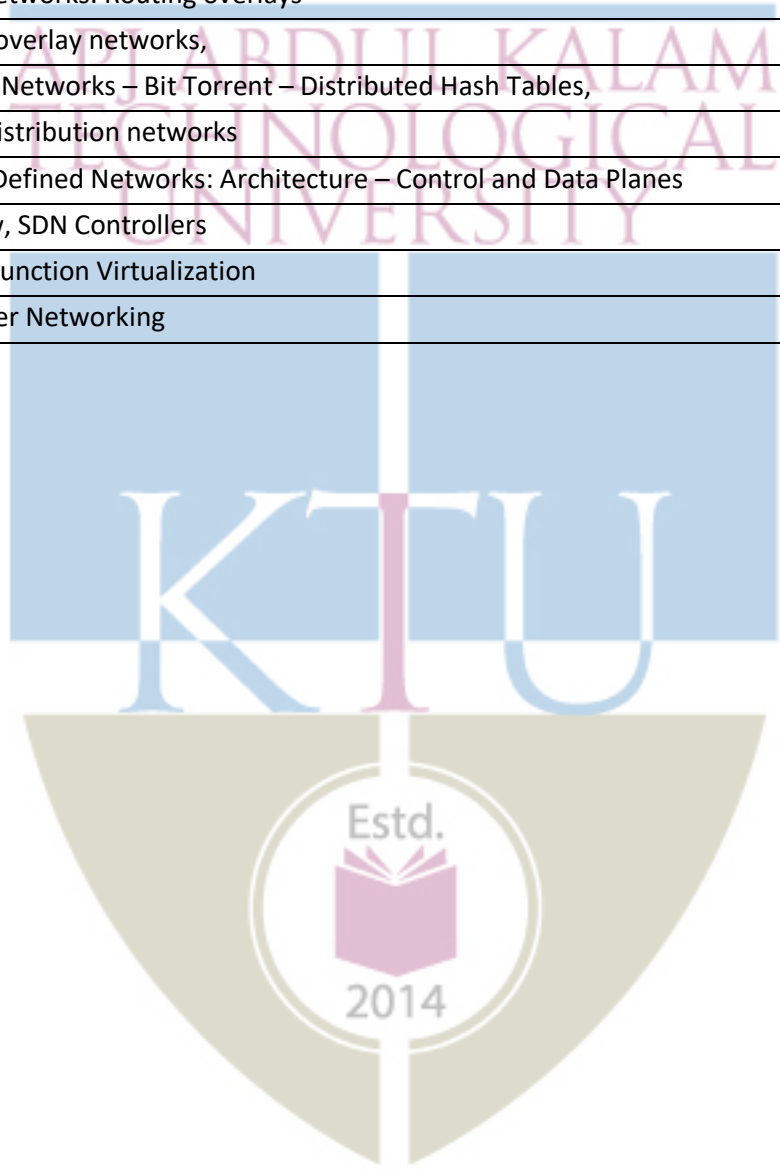
| | |
|---|---|
| FIRST SEMESTER M.TECH DEGREE EXAMINATION, MONTH & YEAR | |
| Course Code: 221ECS036 | |
| Course Name TOPICS IN NETWORKS | |
| Max. Marks : 60 | Duration: 2.5 Hours |
| PART A 4 | |
| Answer All Questions. Each Question Carries 5 Marks | |
| 1. | Illustrate with an example how standard TCP can be enhanced to support mobile users. |
| 2. | Explain the architectural framework for supporting Quality of Service in packet networks. |
| 3. | Examine the role of core network in 3G cellular data network. |
| 4. | There is one sender and eight receivers in a real time multimedia communication system. If the sender is sending multimedia data at 2 Mbps, how many RTP packets can be sent by the sender and each receiver in a second? The system allocates 75 percent of the RTP bandwidth to the receivers and 25 percent to the sender. The average size of each RTP packet is 125 bytes. |

| | | |
|---|--|----------|
| 5. | Define OpenFlow specification used in SDN. | (5x5=25) |
| Part B | | |
| (Answer any five questions. Each question carries 7 marks) | | |
| 6. | (a) X, Y, Z are three ASs. X and Z are connected through Y. X has a peering agreement with Y and Y with Z. Z moves all traffic from Y but does not forward traffic from X. Can Z use BGP to implement this policy? | (4) |
| | (b) How does PIM solve the scalability problem of existing multicast protocols. | (3) |
| 7. | (a) Derive the hexadecimal form of representation of the following link local multicast address: (i) a permanently-assigned multicast group address of 66 (ii) a transient multicast group address of 316 | (4) |
| | (b) A foreign network has a foreign agent. Explain if it is possible for two mobile nodes in the foreign network to use the same care-of address in mobile IP. | (3) |
| 8. | (a) Justify the need for Resource Reservation in multicast transmission. | (4) |
| | (b) How is VPN implemented using MPLS? | (3) |
| 9. | (a) Elaborate on the various elements of 4G LTE network and the interaction between them. | (5) |
| | (b) Calculate the minimum time required to download 2×10^6 bytes using ADSL modem with minimum rate. | (2) |
| 10. | (a) Sketch the superframe format of Zigbee 802.15.4 standard. | (3) |
| | (b) Name some applications which use Zigbee standard and justify its use. | (4) |
| 11. | (a) Describe H323 architectural model for Internet Telephony. | (7) |
| 12. | (a) Comment on the statement "Distributed Hash Tables are said to build structured P2P networks". | (7) |
| | (b) Explain Data Center Networking. | |

Course Plan (For 3 credit courses, the content can be for 40 hrs and for 2 credit courses, the content can be for 26 hrs. The audit course in third semester can have content for 30 hours).

| No | Topic | No. of Lectures (40 hrs) |
|-----|---|---------------------------|
| 1 | Module 1 - (8hrs) | |
| 1.1 | The Global Internet, Routing Areas | 1 hour |
| 1.2 | Interdomain Routing -BGP | 1 hour |
| 1.3 | IP Version 6 | 1 hour |
| 1.4 | Multicast, Multicast Addresses | 1 hour |
| 1.5 | Multicast Routing – DVMRP | 1 hour |
| 1.6 | PIM, MSDP | 1 hour |
| 1.7 | Routing to a mobile node, Mobile IP | 1 hour |
| 1.8 | TCP and Mobility, Mobile TCP | 1 hour |
| 2 | Module 2 - (8hrs) | |
| 2.1 | QoS Architectural Framework | 1 hour |
| 2.2 | Integrated Services Architecture | 1 hour |
| 2.3 | RSVP - Differentiated Services | 1 hour |
| 2.4 | Multiprotocol Label Switching, | 1 hour |
| 2.5 | Virtual Private Networks and Tunnels | |
| 2.6 | Destination-Based Forwarding - Explicit Routing | 1 hour |
| 2.7 | Performance issues in networks | 1 hour |
| 2.8 | Delay Tolerant Networking | 1 hour |
| 3 | Module 3 - (9hrs) | |
| 3.1 | Wired: DSL, Cable Networks, SONET, | 1 hour |
| 3.2 | ATM, VLAN | 1 hour |
| 3.3 | Wireless: Satellite Networks, WiMAX | 1 hour |
| 3.4 | Cellular Networks: Introduction-Wireless links and Network characteristics -CDMA, | 1 hour |
| 3.5 | Cellular Internet access-An overview of cellular network architecture, 3G cellular data networks, | 1 hour |
| 3.5 | 4G LTE Cellular networks - LTE Protocol Stacks -LTE Radio Access Network -Additional LTE functions, | 1 hour |
| 3.6 | 5G Cellular networks | 1 hour |
| 3.7 | Managing mobility in cellular networks, Wireless and Mobility-Impact on higher level protocols | 1 hour |
| 3.8 | Personal Area Networks: Bluetooth, Zigbee | 1 hour |
| 4 | Module 4 - (7hrs) | |
| 4.1 | Multimedia in the Internet: Streaming stored audio/video, Streaming live audio/video, | 1 hour |

| | | |
|-----|---|--------|
| 4.2 | Real time interactive audio/video | 1 hour |
| 4.3 | Real time Interactive Protocols: RTP- RTCP | 1 hour |
| 4.4 | H-323 | 1 hour |
| 4.5 | SIP, SCTP | 1 hour |
| 4.6 | Compression: Audio Compression, Image compression- JPEG, | 1 hour |
| 4.7 | Video Compression- MPEG | 1 hour |
| 5 | Module 5 - (8hrs) | |
| 5.1 | Overlay Networks: Routing overlays | 1 hour |
| 5.2 | -Resilient overlay networks, | 1 hour |
| 5.3 | Peer-Peer Networks – Bit Torrent – Distributed Hash Tables, | 1 hour |
| 5.4 | Content Distribution networks | 1 hour |
| 5.5 | Software Defined Networks: Architecture – Control and Data Planes | 1 hour |
| 5.6 | Open Flow, SDN Controllers | 1 hour |
| 5.7 | Network Function Virtualization | 1 hour |
| 5.8 | Data Center Networking | 1 hour |



| CODE | COURSE NAME | CATEGORY | L | T | P | CREDIT |
|-----------|-----------------------|--------------------|---|---|---|--------|
| 221ECS037 | ADVANCED ARCHITECTURE | Program Elective 1 | 3 | 0 | 0 | 3 |

Preamble:

This purpose of this course is to provide a solid foundation that furnishes the learner with in-depth knowledge of current and emerging trends in computer architectures, focusing on performance and the hardware/software interface. This course covers design and analysis, memory hierarchy, pipelining, operation of multiprocessors, thread level parallelism, and data level parallelism. This course helps the learner with the architectural framework and foundation they need to become influential architects of the future.

Course Outcomes: After the completion of the course the student will be able to

| CO# | CO |
|------|--|
| CO 1 | Solve the advanced issues in design of computer processors, caches and memory(Cognitive Knowledge Level: Apply) |
| CO 2 | Analyze the memory hierarchy design, performance improvement techniques and cache optimization techniques(Cognitive Knowledge Level: Analyze) |
| CO 3 | Analyze the working of pipeline and to understand branching and exception handling in pipelining(Cognitive Knowledge Level: Analyze) |
| CO 4 | State and compare properties of coherence protocol and to understand the operation of multiprocessors and thread level parallelism(Cognitive Knowledge Level: Evaluate) |
| CO 5 | Identify various techniques of data level parallelism including SIMD and GPU processors (Cognitive Knowledge Level: Apply) |

Mapping of course outcomes with program outcomes

| | PO 1 | PO 2 | PO 3 | PO 4 | PO 5 | PO 6 | PO 7 |
|------|------|------|------|------|------|------|------|
| CO 1 | | | | ✓ | | ✓ | |
| CO 2 | | | | ✓ | | ✓ | |
| CO 3 | | | | ✓ | | ✓ | |
| CO 4 | | | | ✓ | | ✓ | |
| CO 5 | ✓ | | | ✓ | | ✓ | |

Assessment Pattern

| Bloom's Category | End Semester Examination |
|------------------|--------------------------|
| Apply | 40 |
| Analyse | 35 |
| Evaluate | 25 |
| Create | |

Mark distribution

| Total Marks | CIE | ESE | ESE Duration |
|-------------|-----|-----|--------------|
| 100 | 40 | 60 | 2.5 hours |

Continuous Internal Evaluation Pattern:

Preparing a review article based on peer reviewed

Original publications (minimum 10 publications shall be referred): 15 marks

Course based task/Seminar/Data collection and interpretation: 15 marks

Test paper, 1 no. : 10 marks

Test paper shall include minimum 80% of the syllabus.

End Semester Examination Pattern:

There will be two parts: Part A and Part B. Part A will contain 5 numerical/short answer questions with 1 question from each module, having 5 marks for each question. Students should answer all questions. Part B will contain 7 questions, with minimum one question from each module of which student should answer any five. Each question can carry 7 marks.

Syllabus

Module 1 (Design and Analysis)

Principles of computer design, Fallacies and Pitfalls, Instruction Set Principles- Classifying instruction set architecture, Memory addressing, Type and size of operands, Operations in the instruction set, Instruction for control flow, encoding an instruction set, Role of compiler.

Module 2 (Memory Hierarchy)

Introduction, Cache performance, Basic cache optimizations, Virtual memory–Techniques for fast address translation, Protection via virtual memory, Fallacies and Pitfalls, Case study of Pentium/Linux memory system-Pentium address translation.

Module 3 (Pipelining)

Introduction, Pipeline hazards, Static branch prediction and dynamic branch prediction, Implementation of MITS, Basic pipeline of MITS, Implementing the control in MITS pipeline,

Dealing with branches in pipeline, Dealing with exceptions, Handling of multi-cycle operations, Maintaining precise exceptions, Case study of MITS R4000 pipeline.

Module 4 (Thread Level Parallelism)

Introduction, Centralized Shared-Memory Architectures, Performance of Symmetric Shared-Memory Multiprocessors, Distributed Shared-Memory and Directory-Based Coherence, Synchronization: The Basics, Models of Memory Consistency: An Introduction, Crosscutting Issues, Case study of Sun T1 Multiprocessor.

Module 5 (Data Level Parallelism)

Vector architecture, SIMD instruction set, Extension for multimedia, Graphic Processing Units, Case study Envida GPU instruction set architecture, GPU memory structure, Innovations in GPU architecture, Comparisons between vector architecture and GPUs, Comparisons between multimedia SIMD computers and GPUs, Loop level parallelism, Finding dependencies, Eliminating dependencies.

Reference Books

1. Hennessy J.L and David A. Patterson “Computer Architecture- A Quantitative Approach” Morgan Kaufmann Publication, Fifth edition, 2002.
2. Randal E Bryant and David O'Hallaron “Computer Systems A programmer's perspective” Pearson Education, 2nd edition 2010 .
3. Kaihwang and Naresh Jotwani, “Advanced Computer Architecture” 2nd edition Tata Mcgraw-Hill, 2010.
4. Sima D, Fountain T and Kacsuk P “Advanced Computer Architecture: A Design Space Approach” Pearson Education, 1st edition 1997.

Course Level Assessment Questions

Course Outcome 1 (CO1):

1. Identify the addressing mode for the high level language statements given below
 - i. `max[1]=arr[J];`
 - ii. `int sum=*a;`
 - iii. `while[*A++];`
 - iv. `int temp++;`
2. Identify the various techniques for instruction encoding. Illustrate with examples.

Course Outcome 2 (CO2) :

1. List and explain basic cache optimization techniques.
2. Consider an in-order execution computer. Assume that the cache miss penalty is 200 clock cycles, and all instructions normally take 1.0 clock cycles. Assume that the average miss rate is 2%, there is an average of 1.5 memory references per instruction, and the average number of cache misses per 1000 instructions is 30. What is the impact on performance when behaviour of the cache is included? Calculate the impact using both misses per instruction & miss rate.

Course Outcome 3(CO3):

1. Consider the execution of following instructions, on our pipelined example processor:
 - `ADD R1, R2, R3`
 - `SUB R4, R1, R5`
 - `AND R6, R1, R7`
 - `OR R8, R1, R9`
 - `XOR R10, R1, R11`

Analyze type of hazards may occur in the above code? If hazard exists, how can we solve it explain?

2. Consider the unpipelined processor in the previous section. Assume that it has a 1ns clock cycle and that it uses 4 cycles for ALU operations and branches and 5 cycles for memory operations. Assume that the relative frequencies of these operations are 40%, 20%, and 40%, respectively. Suppose that due to clock skew and setup, pipelining the processor adds 0.2 ns of overhead to the clock. Ignoring any latency impact, how much speedup in the instruction execution rate will we gain from a pipeline?

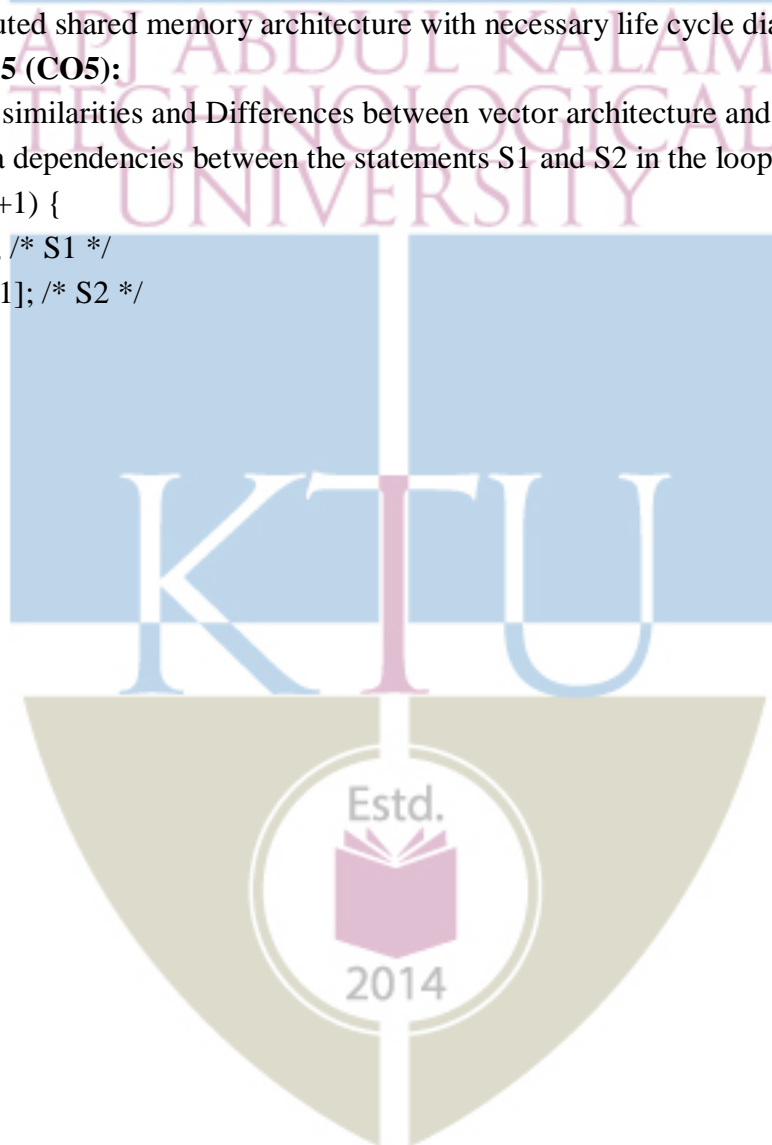
Course Outcome 4 (CO4):

1. Determine the limitations in symmetric shared memory multiprocessors.
2. Explain distributed shared memory architecture with necessary life cycle diagram.

Course Outcome 5 (CO5):

1. Bring about the similarities and Differences between vector architecture and GPUs.
2. Identify the data dependencies between the statements S1 and S2 in the loop.

```
for (i=1; i<=100; i=i+1) {  
A[i+1] = A[i] + C[i]; /* S1 */  
B[i+1] = B[i] + A[i+1]; /* S2 */  
}
```



Model Question paper

QP CODE:

PAGES: 3

Reg No: _____

Name: _____

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

FIRST SEMESTER M.TECH DEGREE EXAMINATION, MONTH & YEAR

Course Code: 221ECS037

Course Name: Advanced Architecture

Max. Marks: 60

Duration: 2.5 Hours

PART A

Answer all Questions. Each question carries 5 Marks

1. Identify the addressing mode for the high-level language statements given below
 - i. `int count = *i++;`
 - ii. `while [*Sum++];`
2. Assume we have a computer where the cycles per instruction (CPI) is 1.0 when all memory accesses hit in the cache. The only data accesses are loads and stores, and these total 50% of the instructions. If the miss penalty is 25 clock cycles and the miss rate is 2%, how much faster would the computer be if all instructions were cache hits?
3. Analyze the type of hazards may occur in the following code.
LW R1, 0(R2)
SUB R4, R1
AND R6, R1, R7
OR R8, R1, R9
4. Suppose we have an application running on a 32-processor multiprocessor, which has a 200ns time to handle reference to a remote memory. For this application, assume that all the references except those involving communication hit in the local memory hierarchy, which is slightly optimistic. Processors are stalled on a remote request, and the processor clock rate is 2GHz. If the base CPI (assuming that all references hit in the cache) is 0.5, evaluate how much faster is the multiprocessor if there is no communication versus if 0.2% of the instructions involve a remote communication reference?
5. Consider the following loops, identify the true dependencies, output dependences and anti-dependences and eliminate the output dependences and anti-dependences.

```
for(i=0;i<100;i++){  
Y[i]=X[i]/C; /*S1*/  
X[i]= X[i]+C; /*S2*/  
Z[i]=Y[i]+C; /*S3*/  
Y[i]=C-Y[i]; /*S4*/
```

(5x3=15 Marks)

PART B

Answer any 5 questions. Each question carries 7 marks

6. A benchmark program is executed on a 40MHz processor. The benchmark program has the following statistics.

| Instruction Type | Instruction Count | Clock Cycle Count |
|------------------|-------------------|-------------------|
| Arithmetic | 1000 | |
| Branch | 1000 | |
| Load/Store | 1000 | |
| Branching Point | 1000 | |

Determine the effective CPI, MIPS rate and execution time of this program.

7. "Fully associative caches do not have conflict misses". Examine the statement.

OR

8. Consider an in-order execution computer. Assume that the cache miss penalty is 200 clock cycles, and all instructions normally take 1.0 clock cycles. Assume that the average miss rate is 2%, there is an average of 1.5 memory references per instruction, and the average number of cache misses per 1000 instructions is 30. What is the impact on performance when behaviour of the cache is included? Calculate the impact using both misses per instruction and miss rate.
9. List the three pipeline hazards. Explain branch pipeline hazard in detail.

OR

10. Distinguish Static and Dynamic branch prediction in pipelining.
11. Explain multiprocessor cache coherence.
12. Analyze the similarities and differences between vector architecture and GPUs.

(5x7=35 Marks)

2014

Course Plan

| No | Topic | No. of Lectures |
|----------|---|-----------------|
| 1 | Design and Analysis | 8 hours |
| 1.1 | Principles of computer design | 1 |
| 1.2 | Fallacies and Pitfalls | 1 |
| 1.3 | Instruction Set Principles- Classifying instruction set architecture | 1 |
| 1.4 | Memory addressing, Type and size of operands | 1 |
| 1.5 | Operations in the instruction set | 1 |
| 1.6 | Instruction for control flow | 1 |
| 1.7 | Encoding an instruction set | 1 |
| 1.8 | Role of compiler | 1 |
| 2 | Memory Hierarchy | 8 hours |
| 2.1 | Introduction | 1 |
| 2.2 | Cache performance | 1 |
| 2.3 | Basic cache optimizations | 1 |
| 2.4 | Virtual memory –Techniques for fast address translation | 1 |
| 2.5 | Protection via virtual memory | 1 |
| 2.6 | Fallacies and Pitfalls | 1 |
| 2.7 | Case study of Pentium/Linux memory system-Pentium address translation | 1 |
| 2.8 | Linux Virtual memory system | 1 |
| 3 | Pipelining | 8 hours |
| 3.1 | Introduction | 1 |
| 3.2 | Pipeline hazards | 1 |
| 3.3 | Static branch prediction and dynamic branch prediction | 1 |
| 3.4 | Implementation of MITS, Basic pipeline of MITS | 1 |
| 3.5 | Implementing the control in MITS pipeline | 1 |
| 3.6 | Dealing with branches in pipeline, Dealing with exceptions | 1 |
| 3.7 | Handling of multi-cycle operations, Maintaining precise exceptions | 1 |
| 3.8 | Case study of MITS R4000 pipeline | 1 |
| 4 | Multiprocessors and Thread level Parallelism | 8 hours |
| 4.1 | Introduction | 1 |
| 4.2 | Centralized Shared-Memory Architectures | 1 |
| 4.3 | Performance of Symmetric Shared-Memory Multiprocessors | 1 |
| 4.4 | Distributed Shared-Memory and Directory-Based Coherence | 1 |
| 4.5 | Synchronization: The Basics | 1 |
| 4.6 | Models of Memory Consistency: An Introduction | 1 |
| 4.7 | Crosscutting Issues | 1 |
| 4.8 | Case study Sun T1 Multiprocessor | 1 |
| 5 | Data Level Parallelism | 8 hours |
| 5.1 | Vector architecture, SIMD instruction set | 1 |
| 5.2 | Extension for multimedia, Graphic Processing Units | 1 |

| | | |
|-----|---|---|
| 5.3 | Case study Envida GPU instruction set architecture | 1 |
| 5.4 | GPU memory structure | 1 |
| 5.5 | Innovations in GPU architecture, Comparisons between vector architecture and GPUs | 1 |
| 5.6 | Comparisons between multimedia SIMD computers and GPUs | 1 |
| 5.7 | Loop level parallelism | 1 |
| 5.8 | Finding dependencies, Eliminating Dependencies | 1 |



| CODE | COURSE NAME | CATEGORY | L | T | P | CREDIT |
|-----------|-------------------------------|--------------------|---|---|---|--------|
| 221ECS038 | FILE SYSTEM FORENSIC ANALYSIS | PROGRAM ELECTIVE 2 | 3 | 0 | 0 | 3 |

Preamble: The objective of the course is to provide the students the knowledge of the organization of files in different Operating Systems. The course is designed to develop intuition in the students to analyze the disk images of various File Systems and identify the data. The course also aims to provide knowledge on specific artifacts valuable to forensic examinations.

Course Outcomes:

After the completion of the course, the student will be able to

| | |
|------|--|
| CO 1 | Demonstrate Volume / Partition (Cognitive Knowledge Level: Analysis) |
| CO 2 | Understand FAT file System structures and analyze the FAT file system. (Cognitive Knowledge Level: Apply) |
| CO 3 | Evaluate and Analyze the NTFS file system. (Cognitive Knowledge Level: Evaluate) |
| CO 4 | Evaluate and Analyze Ext X File systems. (Cognitive Knowledge Level: Evaluate) |
| CO 5 | Illustrate the data organization in Flash Memory architecture, HFS+, and Android Mobile file systems. (Cognitive Knowledge Level: Analysis) |

Program Outcomes (PO)

Outcomes are the attributes that are to be demonstrated by a graduate after completing the course.

PO1: An ability to independently carry out research/investigation and development work in engineering and allied streams

PO2: An ability to communicate effectively, write and present technical reports on complex engineering activities by interacting with the engineering fraternity and with society at large.

PO3: An ability to demonstrate a degree of mastery over the area as per the specialization of the program. The mastery should be at a level higher than the requirements in the appropriate bachelor's program

PO4: An ability to apply stream knowledge to design or develop solutions for real-world problems by following the standards

PO5: An ability to identify, select and apply appropriate techniques, resources and state-of-the-art tool to model, analyze and solve practical engineering problems.

PO6: An ability to engage in life-long learning for the design and development related to the stream-related problems taking into consideration sustainability, societal, ethical, and environmental aspects

PO7: An ability to develop cognitive load management skills related to project management and finance which focus on Entrepreneurship and Industry relevance.

Mapping of course outcomes with program outcomes

| | PO 1 | PO 2 | PO 3 | PO 4 | PO 5 | PO 6 | PO 7 |
|------|------|------|------|------|------|------|------|
| CO 1 | ☑ | | ☑ | ☑ | ☑ | | |
| CO 2 | ☑ | ☑ | ☑ | ☑ | ☑ | | |
| CO 3 | ☑ | ☑ | ☑ | ☑ | ☑ | | |
| CO 4 | ☑ | ☑ | ☑ | ☑ | ☑ | | |
| CO 5 | ☑ | | ☑ | ☑ | ☑ | | |

Assessment Pattern

| Bloom's Category | End Semester Examination |
|------------------|--------------------------|
| Apply | 40% |
| Analyse | 40% |
| Evaluate | 20% |
| Create | |

Mark distribution

| Total Marks | CIE | ESE | ESE Duration |
|-------------|-----|-----|--------------|
| 100 | 40 | 60 | 2.5 hours |

Continuous Internal Evaluation Pattern:

Evaluation shall only be based on application, analysis or design based questions (for both internal and end semester examinations).

Continuous Internal Evaluation: 40 marks

- i. Preparing a review article based on peer-reviewed original publications (minimum 10 publications shall be referred) : 15 marks
- ii. Course based task / Seminar/ Data collection and interpretation : 15 marks
- iii. Test paper (1 number) : 10 marks

Test paper shall include a minimum of 80% of the syllabus.

Course-based task/test paper questions shall be useful in the testing of knowledge, skills, comprehension, application, analysis, synthesis, evaluation, and understanding of the students.

End Semester Examination Pattern:

The end semester examination will be conducted by the respective College.

There will be two parts; Part A and Part B.

Part A will contain 5 numerical/short answer questions with 1 question from each module, having 5 marks for each question. Students should answer all questions. Part B will contain 7 questions (such questions shall be useful in the testing of overall achievement and maturity of the students in a course, through long answer questions relating to theoretical/practical knowledge, derivations, problem-solving and quantitative evaluation), with a minimum one question from each module of which student should answer any five. Each question can carry 7 marks

Total duration of the examination will be 150 minutes.

Note: The marks obtained for the ESE for an elective course shall not exceed 20% over the average ESE mark % for the core courses. ESE marks awarded to a student for each elective course shall be normalized accordingly.

For example, if the average end semester mark % for a core course is 40, then the maximum eligible mark % for an elective course is $40+20 = 60$ %.

Syllabus

Module 1

Digital Investigation Basics and Volume Analysis: Digital Investigations and Evidence, Digital Crime Scene Investigation Process, Data Analysis, Data Organizations, Booting Process, Hard Disk Technology, Hard disk data Acquisition - Reading the source data, Writing the output data, A Case Study. PC based partitions - DOS partitions, Analysis considerations, Apple partitions, Removable media, Server based partitions- GPT partitions, Multiple disk volumes- RAID, Disk Spanning - Linux MD, Linux LVM, Windows LDM

Module 2

FAT File System Analysis: File system, File system category, Content category, Metadata category, File name category, Application category, FAT concepts and analysis- Introduction, File system category, Content category, Metadata category, File name category, File recovery,

determining type, Consistency check, FAT data structure-Boot sector, FAT 32 FS info, directory entries, Long file name directory entries, A Case Study.

Module 3

NTFS File System Analysis: Introduction, MFT concepts, MFT entry attribute concepts, Other attribute concepts, Indexes, NTFS Analysis- File system category, Content category, Metadata category, File name category, File recovery, determining the type, Consistency check, NTFS data structure- Basic concepts, Standard file attributes, Index attributes and data structures, File system metadata files, A Case Study.

Module 4

Ext X File Systems: Ext2 & Ext3 concepts- File system category, Content, Metadata category, File name category, File recovery, determining the type, Consistency check, Ext2 and Ext3 data structures, Ext4 data structures, File Recovery possibility in Ext2, Ext3, Ext4.

Module 5

Android and MAC File Systems: Introduction to Flash Memory , Architecture, NAND and NOR, Android Mobile File Systems - Data Organization, YAFFS2, F2FS, MAC File System - HFS+ - Data Organization.

Text Books

1. Brian Carrier, "File System Forensic Analysis", Addison Wesley, 2005.
2. Andrew Hoog, " Android Forensics Investigation, Analysis and Mobile Security for Google Android ", Syngress, 2011.

Reference Books

1. Casey, Eoghan, "Digital Evidence and Computer Crime", Edition 2, Academic Press, 2004.
2. Dan Farmer & Wietse Venema, "Forensic Discovery", Addison Wesley, 2005.

Course Level Assessment Questions

Course Outcome 1 (CO1):

1. Examine the types of partitions in DOS?
2. Distinguish the areas of GPT disks?

3. Compare the two methods of disk spanning in Linux.

Course Outcome 2 (CO2)

1. Explain the importance of slack space?
2. Examine the relation between Directory Entry structures, clusters, and FAT
3. Illustrate when a file named file1 is created in the FAT file system, within a directory dir. Assume the cluster size to be 1024 bytes and the size of the file is 6000 bytes.

Course Outcome 3(CO3):

1. What is meant by clusters? How do they co-relate with file allocation strategies? Why clusters are referred to logical allocation units?
2. Comment on the sparse compressed attributes in NTFS?
3. Illustrate the method to find all references to a file named "CurriculumVitae.doc" in both allocated and deleted instances of the file.

Course Outcome 4 (CO4):

1. Examine the use of block pointers.
2. Compare the allocation algorithms in ExtX?
3. Compare the possibility of File recovery in ExtX File Systems.

Course Outcome 5 (CO5):

1. Compare the different options available in /mnt/sdcard?
2. What are the important features of YAFFS2?
3. List the constraints on the files stored in the Internal Storage of Android devices?

Model Question Paper

QP CODE:

Reg No: _____

Name: _____

PAGES : 2

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

FIRST SEMESTER M.TECH DEGREE EXAMINATION, MONTH & YEAR

Course Code: 221ECS038

Course Name: File System Forensic Analysis

Max. Marks: 60

Duration: 2.5 Hours

PART A

Answer All Questions. Each Question Carries 5 Marks

- | | | |
|----|--|-----|
| 1. | Compare the different types of Write Blockers present with the help of diagrams. | (5) |
| 2. | How the damaged data units are handled by the FAT file system? | (5) |
| 3. | Examine the Standard Attributes in NTFS. | (5) |
| 4. | What are the different methods to assign names to File / Directory in Ext X | (5) |
| 5. | Explain the methods of Persistent data storage | (5) |

Part B

(Answer any five questions. Each question carries 7 marks)

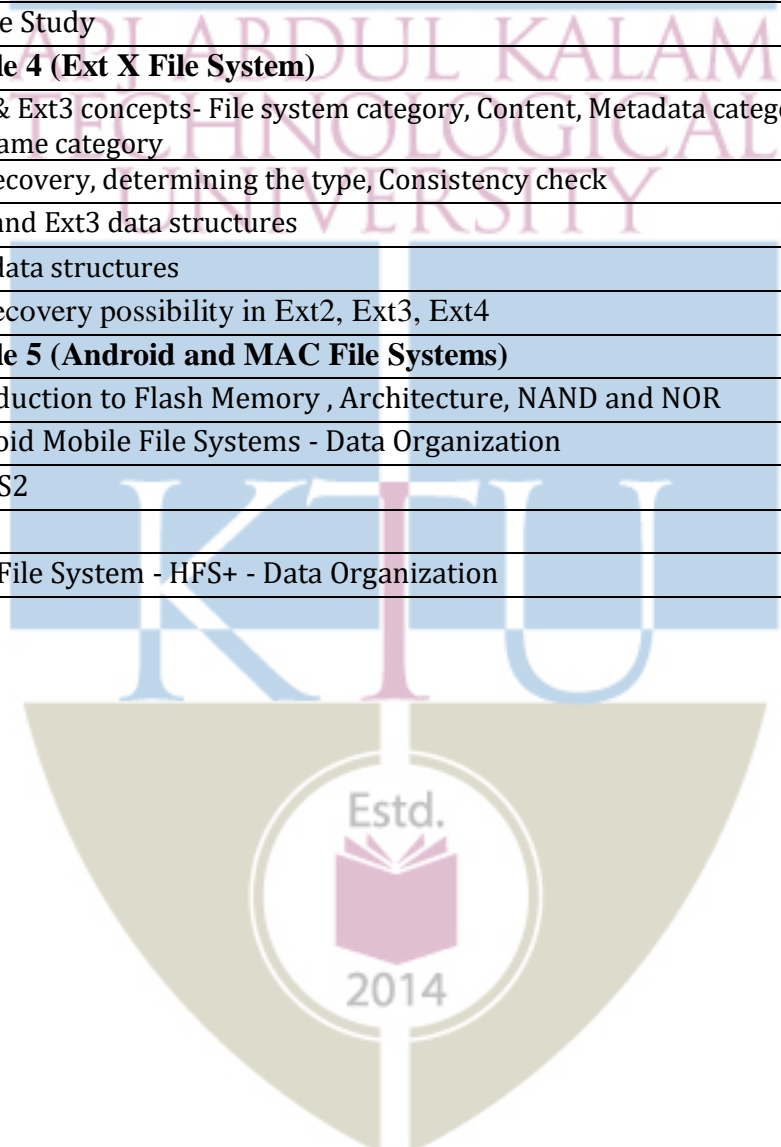
- | | | | |
|----|-----|--|-----|
| 6. | (a) | Examine the acquisition of data. List and explain the commands used. | (4) |
| | (b) | List the various steps involved in the booting process. | (3) |
| 7. | (a) | Distinguish between logical file system searching and data unit viewing | (3) |
| | (b) | How can we find the first cluster in FAT12/16 and FAT32 file system? Give basic steps to calculate the sector address. | (4) |
| 8. | (a) | Justify the importance of MFT in NTFS | (3) |
| | (b) | Explain the analysis techniques for the NTFS file system category. Also, mention the analysis considerations | (4) |
| 9. | (a) | Everything in NTFS is treated as an attribute. Substantiate this statement with relevant facts. | (3) |

| | | | |
|----|-----|--|-----|
| | (b) | What is the importance of the file system? How analysis of the file system helps in the forensic investigation? | (4) |
| 10 | (a) | Make a comparative study on HPA and DCO. Explain their concepts with suitable diagrams. | (4) |
| | (b) | Differentiate live analysis and dead analysis. What is their impact on the digital crime scene in the investigation process? | (3) |
| 11 | (a) | What are the different data structures used to store data in the file system category of Ext X? | (3) |
| | (b) | How file names are assigned using links. | (4) |
| 12 | (a) | What are the different types of memory in Android devices? | (3) |
| | (b) | What details are identified by examining the /proc/yaffs? | (4) |

Course Plan (For 3 credit courses, the content can be for 40 hrs, and for 2 credit courses, the content can be for 26 hrs. The audit course in the third semester can have content for 30 hours).

| No | Topic | No. of Lectures (40) |
|-----|--|----------------------|
| 1 | Module 1 (Digital Investigation Basics and Volume Analysis) | |
| 1.1 | Digital Investigations and Evidence, Digital crime scene investigation process | 1 |
| 1.2 | Data Analysis, Data organizations | 1 |
| 1.3 | Bootting Process, Hard Disk Technology | |
| 1.4 | Hard disk data acquisition - Reading the source data, Writing the output data | 1 |
| 1.5 | A Case Study | |
| 1.6 | PC based partitions- DOS partitions, Analysis considerations | 1 |
| 1.7 | Apple partitions, removable media | 1 |
| 1.8 | Server based partitions- GPT partitions | 1 |
| 1.9 | Multiple disk volumes- RAID, Disk Spanning - Linux MD, Linux LVM, Windows LDM | 2 |
| 2 | Module 2 (FAT File System Analysis) | |
| 2.1 | File system, File system category, Content category, Metadata category, File name category, Application category | 1 |
| 2.2 | FAT concepts and analysis- Introduction, File system category, Content category | 1 |
| 2.3 | Metadata category, File name category | 1 |
| 2.4 | File recovery, determining type, Consistency check | 1 |
| 2.5 | FAT data structure-Boot sector, FAT 32 FS info, directory entries | 2 |
| 2.6 | Long file name directory entries | |
| 2.7 | A Case Study | 2 |

| | | |
|-----|---|---|
| 3 | Module 3 (NTFS File System Analysis) | |
| 3.1 | Introduction, MFT concepts | 1 |
| 3.2 | MFT entry attribute concepts, Other attribute concepts, Indexes | 1 |
| 3.3 | NTFS Analysis- File system category, Content category, Metadata category, File name category | 1 |
| 3.4 | File recovery, determining the type, Consistency check | 1 |
| 3.5 | NTFS data structure- Basic concepts, Standard file attributes, Index attributes and data structures | 2 |
| 3.6 | File system metadata files | |
| 3.7 | A Case Study | 2 |
| 4 | Module 4 (Ext X File System) | |
| 4.1 | Ext2 & Ext3 concepts- File system category, Content, Metadata category, File name category | 2 |
| 4.2 | File recovery, determining the type, Consistency check | 1 |
| 4.3 | Ext2 and Ext3 data structures | 2 |
| 4.4 | Ext4 data structures | 2 |
| 4.5 | File Recovery possibility in Ext2, Ext3, Ext4 | 1 |
| 5 | Module 5 (Android and MAC File Systems) | |
| 5.1 | Introduction to Flash Memory , Architecture, NAND and NOR | 2 |
| 5.2 | Android Mobile File Systems - Data Organization | 2 |
| 5.3 | YAFFS2 | 2 |
| 5.4 | F2FS | |
| 5.5 | MAC File System - HFS+ - Data Organization | 2 |



| | | | | | | |
|-----------|-------------|-----------------------|---|---|---|--------|
| 221ECS039 | BLOCK CHAIN | CATEGORY | L | T | P | CREDIT |
| | | Program Elective 2 | 3 | 0 | 0 | 3 |

Preamble: The objective of this course is to design and develop block chain based decentralized applications. Enables the learners to start from the fundamentals and then cover all the technical and functional aspects needed to build any blockchain solution using the best tools and techniques in the industry. In this course, they will build smart contracts, bitcoin wallets, create transactions, and more.

After the completion of the course the student will be able to

| | |
|------|---|
| CO 1 | State the key differentiators for blockchain from other technology systems. (Cognitive Knowledge level: Apply) |
| CO 2 | Summarize the classification of consensus algorithms. (Cognitive Knowledge Level: Apply) |
| CO 3 | Design, develop, deploy and test smart contract (Cognitive Knowledge level: Evaluate) |
| CO 4 | Design, deploy and test DAPP (Cognitive Knowledge level: Evaluate) |
| CO 5 | Explore on-chain and off-chain data (Cognitive Knowledge level: Apply) |

Program Outcomes (PO)

Outcomes are the attributes that are to be demonstrated by a graduate after completing the course.

- PO1:** An ability to independently carry out research/investigation and development work in engineering and allied streams
- PO2:** An ability to communicate effectively, write and present technical reports on complex engineering activities by interacting with the engineering fraternity and with society at large.
- PO3:** An ability to demonstrate a degree of mastery over the area as per the specialization of the program. The mastery should be at a level higher than the requirements in the appropriate bachelor program
- PO4:** An ability to apply stream knowledge to design or develop solutions for real world problems by following the standards
- PO5:** An ability to identify, select and apply appropriate techniques, resources and state-of-the-art tool to model, analyse and solve practical engineering problems.
- PO6:** An ability to engage in life-long learning for the design and development related to the stream related problems taking into consideration sustainability, societal, ethical and environmental aspects

PO7: An ability to develop cognitive load management skills related to project management and finance which focus on Entrepreneurship and Industry relevance.

Mapping of course outcomes with program outcomes

| | PO 1 | PO 2 | PO 3 | PO 4 | PO 5 | PO 6 | PO 7 |
|------|------|------|------|------|------|------|------|
| CO 1 | ☑ | ☑ | ☑ | | | | |
| CO 2 | ☑ | ☑ | ☑ | | ☑ | | |
| CO 3 | ☑ | ☑ | ☑ | | | | |
| CO 4 | ☑ | ☑ | ☑ | | ☑ | | |
| CO 5 | ☑ | ☑ | ☑ | | | | |

Assessment Pattern

| Bloom's Category | End Semester Examination |
|------------------|--------------------------|
| Apply | 45 |
| Analyse | 30 |
| Evaluate | 25 |
| Create | |

Mark distribution

| Total Marks | CIE | ESE | ESE Duration |
|-------------|-----|-----|--------------|
| 100 | 40 | 60 | 2.5 hours |

Continuous Internal Evaluation Pattern: 40 marks

1. Course based task/Seminar/Data collection and interpretation: 20 marks
2. Test paper, 1 no.: 20 marks

End Semester Examination Pattern:

There will be two parts; Part A and Part B.

1. Part A will be conducted by the University in proctored online mode. The examination will be for 60 minutes and will contain 5 multiple choice/short answer questions with 1 question from each module, having 5 marks for each question
2. Part B will be conducted internally by the respective college. The examination will be for 90 minutes and will contain 7 questions with minimum one question from each module of which student should answer any five. Each question can carry 7 marks.
3. The marks obtained for Part B will be regulated in line with the mark scored in Part A

Syllabus

Module1:

Cryptography basics: Symmetric key cryptography, Asymmetric key cryptography, Introduction to Hashing- Applications of cryptographic hash functions – Merkle trees, Distributed hash tables, Block Chain, Bitcoin to Block Chain, Blockchain programming: Decentralized infrastructure, Disintermediation protocol, Trust enabler Motivating scenarios: Automatic and consistent data collection, Timely information sharing, Auditable actions for provenance, Guidance for governance, Pandemic management

Module2:

Consensus – definition, types, consensus in blockchain. Decentralization – Decentralization using blockchain, Methods of decentralization, Routes to decentralization, Blockchain and full ecosystem decentralization. Consensus Algorithms, Crash fault-tolerance (CFT) algorithms – Paxos, Raft. Byzantine fault tolerance (BFT) algorithms – Practical Byzantine Fault Tolerance (PBFT), Proof of work (PoW), Proof of stake (PoS), Types of PoS.

Module3

The concept of a smart contract: Bitcoin transactions versus smart contract transactions, Design of a smart contract, A use case diagram for the counter, Development of a smart contract code: Solidity language, Smart contract code for Counter, Deploying and testing the smart contract, Introduction to remix IDE, Use case of Decentralized airline system, The relevance of public-key cryptography to blockchain, Transaction signing, Deploying smart contracts on Ropsten, Using the private key in mnemonic form, populating a blockchain wallet, Deploying and transacting on Ropsten.

Module4: From smart contracts to Dapps

Dapp development using Truffle: The development process, Installing Truffle, Building the Dapp stack, Install Ganache test chain, Develop the smart contract, Deploy the smart contract, Develop and configure the web application

Module5: On-chain and off-chain data, Web3 Basics

On-chain data, Blind auction use case, Off-chain data, External data sources ASK airline system use case study, Web3 API: Web3 in Dapp stack, Web3 packages, The channel concept: Micropayment channel, Micropayment channel use case.

Reference Books

1. Bina Ramamurthy, 'Block chain in Action', Manning Publications, First edition,2020
2. Imran Bashir, Mastering Blockchain: A deep dive into distributed ledgers, consensus protocols, smart contracts, DApps, cryptocurrencies, Ethereum, and more, Packt Publishing, Third edition, 2020.

3. Josh Thompson, 'Blockchain: The Blockchain for Beginnings, Guild to Blockchain Technology and Blockchain Programming', Create Space Independent Publishing Platform, 2017.
4. Ritesh Modi, Solidity Programming Essentials: A beginner's guide to build smart contracts for Ethereum and blockchain, Packt Publishing, First edition, 2018.
5. Kumar Saurabh, Ashutosh Saxena, Blockchain Technology: Concepts and Applications, First Edition, Wiley Publications, First edition, 2020.
6. Chandramouli Subramanian, Asha A George, et al, Blockchain Technology, Universities Press (India) Pvt. Ltd, First edition, August 2020.
7. Lorne Lantz, Daniel Cawrey, Mastering Blockchain: Unlocking the Power of Cryptocurrencies, Smart Contracts, and Decentralized Applications, O'Reilly Media, First edition, 2020.
8. Andreas M. Antonopoulos, Gavin Wood, Mastering Ethereum: Building Smart Contracts and DApps, O'Reilly Media, First edition, 2018.

Course Level Assessment Questions

Course Outcome 1 (CO1):

1. Discuss the role of secure hash functions in blockchain
2. Describe the various industries that can benefit from block chain technology

Course Outcome 1 (CO2):

1. If your blockchain network has 5 Byzantine nodes, what is the minimum number of nodes that are required to ensure Byzantine fault tolerance using PBFT protocol
2. Explain and illustrate how Paxos protocol can be used to achieve consensus

Course Outcome 1 (CO3):

1. Explain how smart contracts can be used for enforcing agreements between parties in the form of business logic
2. Show how Practical Byzantine Fault Tolerance can achieve consensus in the presence of Byzantine faults

Course Outcome 1 (CO4):

1. Explain how hash functions are used to build Merkle trees in blockchain.
2. How will you setup a meta mask wallet

Course Outcome 1 (CO5):

1. Explain the steps in building Dapp stack
2. Explain the role of web3.0 in block chain-based Dapp stack

Model Question paper

Reg. No.....

Name:.....

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY FIRST SEMESTER

FIRST SEMESTER M. TECH DEGREE EXAMINATION

BLOCK CHAIN

COURSE CODE :221ECS039

Max. Marks : 25+ 35

Duration: 1+ 1.5 Hours

PART A

Each question carries FIVE marks 60 minutes

1. Discuss the role of secure hash functions in blockchain.
2. If your blockchain network has 5 Byzantine nodes, what is the minimum number of nodes that are required to ensure Byzantine fault tolerance using PBFT protocol
3. Explain how smart contracts can be used for enforcing agreements between parties in the form of business logic.
4. Explain how hash functions are used to build Merkle trees in blockchain
5. Explain the steps in building Dapp stack

PART B-Offline mode

Answer any FIVE full questions

90 minutes

6. a. Describe the various industries that can benefit from block chain technology (4 marks)
b. Write short note on hashing technique (3 marks)
7. Explain and illustrate how Paxos protocol can be used to achieve consensus. (7 marks)
8. a. What is smart contract (2 marks)
b. Design a smart contract for Air Line Reservation System (5 marks)
9. Show how Practical Byzantine Fault Tolerance can achieve consensus in the presence of Byzantine faults (7 marks)

- 10 a. Explain consensus mechanisms used in blockchain. (5 marks)
- b. How will you setup a meta mask wallet (2 marks)
11. a. Write short note on on-chain and off- chain data (4 marks)
- b. What is web3.0 and list any 5 features of web 3.0 (3 marks)
12. a. Explain the role of web3.0 in block chain-based Dapp stack (3 marks)
- b. Write not on web3 packages (4 marks)

Course Plan (For 3 credit courses, the content can be for 40 hrs and for 2 credit courses, the content can be for 26 hrs. The audit course in third semester can have content for 30 hours).

| No | Topic | No. of Lectures |
|-----|--|-----------------|
| 1 | Module 1 | (7 hrs) |
| 1.1 | Cryptography basics: Symmetric key cryptography, Asymmetric key cryptography | 1 |
| 1.2 | Introduction to Hashing | 1 |
| 1.3 | Applications of cryptographic hash functions – Merkle trees, Distributed hash tables | 1 |
| 1.4 | Block Chain, Bitcoin to Block Chain | 1 |
| 1.5 | Blockchain programming: Decentralized infrastructure | 1 |
| 1.6 | Disintermediation protocol, Trust enabler | 1 |
| 1.7 | Motivating scenarios: Automatic and consistent data collection, Timely information sharing, Auditable actions for provenance, Guidance for governance, Attribution of actions, Pandemic management | 1 |
| 2 | Module 2 | (6 hrs) |
| 2.1 | Consensus – definition, types, consensus in blockchain | 1 |
| 2.2 | Decentralization using blockchain, Methods of decentralization | 1 |
| 2.3 | Routes to decentralization, Blockchain and full ecosystem decentralization. | 1 |
| 2.4 | Consensus Algorithms, Crash fault-tolerance (CFT) algorithms – Paxos, Raft | 1 |
| 2.5 | Byzantine fault tolerance (BFT) algorithms – Practical Byzantine Fault Tolerance (PBFT) | 1 |
| 2.6 | Proof of work (PoW), Proof of stake (PoS), Types of PoS. | 1 |

| | | |
|------|--|-----------------|
| 3 | Module 3 | (12 hrs) |
| 3.1 | The concept of a smart contract: Bitcoin transactions versus smart contract transactions | 1 |
| 3.2 | Design of a smart contract | 1 |
| 3.3 | A use case diagram for the counter | 1 |
| 3.4 | Development of a smart contract code: Solidity language | 1 |
| 3.5 | Smart contract code for Counter | 1 |
| 3.6 | Deploying and testing the smart contract | 1 |
| 3.7 | Introduction to remix IDE | 1 |
| 3.8 | Use case of Decentralized airline system | 1 |
| 3.9 | The relevance of public-key cryptography to blockchain | 1 |
| 3.10 | Generating Ethereum addresses | 1 |
| 3.11 | Transaction signing, Deploying smart contracts on Ropsten | 1 |
| 3.12 | Using the private key in mnemonic form, populating a blockchain wallet, Deploying and transacting on Ropsten | 1 |
| 4 | Module 4 | (8 hrs) |
| 4.1 | Dapp development using Truffle: The development process | 1 |
| 4.2 | Installing Truffle | 1 |
| 4.3 | Building the Dapp stack | 1 |
| 4.4 | Install Ganache test chain | 1 |
| 4.5 | Familiarizing Ganache test chain | 1 |
| 4.6 | Develop the smart contract | 1 |
| 4.7 | Deploy the smart contract | 1 |
| 4.8 | Develop and configure the web application | 1 |
| 5 | Module 5 | (7 hrs) |
| 5.1 | On-chain data | 1 |
| 5.2 | Blind auction use case | 1 |
| 5.3 | Off-chain data | 1 |
| 5.4 | External data sources ASK airline system use case study | 1 |

| | | |
|-----|--|---|
| 5.5 | Web3 API: Web3 in Dapp stack | 1 |
| 5.6 | Web3 packages | 1 |
| 5.7 | The channel concept: Micropayment channel, Micropayment channel use case | 1 |



| | | | | | | |
|-----------|---------------|--------------------|---|---|---|--------|
| 221ECS040 | SECURE CODING | CATEGORY | L | T | P | CREDIT |
| | | Program Elective 2 | 3 | 0 | 0 | 3 |

Preamble:

This course aims to provide a knowledge to analyse various security attacks and to recognize and remove common coding errors that lead to vulnerabilities. It provides techniques for developing a secure application.

Prerequisites: Nil

Course Outcomes:

After the completion of the course the student will be able to

| | |
|------|---|
| CO 1 | Implement security as a culture and show mistakes that make applications vulnerable to attacks. (Cognitive Knowledge Level: Understand) |
| CO 2 | Compare various attacks like DoS, buffer overflow, web specific, database specific, web-spoofing attacks. (Cognitive Knowledge Level: Analyze) |
| CO 3 | Synthesize alternative designs and implementations that incorporate mitigations for observed vulnerabilities. (Cognitive Knowledge Level: Evaluate) |
| CO 4 | Use knowledge of information management and computer networking and communications while performing software-security assessments and designing and implementing secure code. (Cognitive Knowledge Level: Apply) |
| CO 5 | Properly handle application faults, implement secure authentication, authorization and data validation controls used to prevent common vulnerabilities. (Cognitive Knowledge Level: Analyze) |

Program Outcomes (PO)

Outcomes are the attributes that are to be demonstrated by a graduate after completing the course.

PO1: An ability to independently carry out research/investigation and development work in engineering and allied streams

PO2: An ability to communicate effectively, write and present technical reports on complex engineering activities by interacting with the engineering fraternity and with society at large.

PO3: An ability to demonstrate a degree of mastery over the area as per the specialization of the program. The mastery should be at a level higher than the requirements in the appropriate bachelor program

PO4: An ability to apply stream knowledge to design or develop solutions for real world problems by following the standards

PO5: An ability to identify, select and apply appropriate techniques, resources and state-of-the-art tool to model, analyse and solve practical engineering problems.

PO6: An ability to engage in life-long learning for the design and development related to the stream related problems taking into consideration sustainability, societal, ethical and environmental aspects

PO7: An ability to develop cognitive load management skills related to project management and finance which focus on Entrepreneurship and Industry relevance.

Mapping of course outcomes with program outcomes

| | PO 1 | PO 2 | PO 3 | PO 4 | PO 5 | PO 6 | PO 7 |
|------|------|------|------|------|------|------|------|
| CO 1 | ✓ | | ✓ | ✓ | | ✓ | |
| CO 2 | ✓ | | ✓ | ✓ | ✓ | ✓ | |
| CO 3 | ✓ | | ✓ | ✓ | ✓ | ✓ | |
| CO 4 | ✓ | | ✓ | ✓ | ✓ | ✓ | |
| CO 5 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

Assessment Pattern

| Bloom's Category | End Semester Examination marks |
|------------------|--------------------------------|
| Apply | 40 |
| Analyse | 35 |
| Evaluate | 25 |
| Create | |

Mark distribution

| Total Marks | CIE | ESE | ESE Duration |
|-------------|-----|-----|--------------|
| 100 | 40 | 60 | 2.5 hours |

Continuous Internal Evaluation Pattern: 40 marks

1. Developing a review article based on peer reviewed original publications: 15 marks
2. Course based task/Seminar/Data collection and interpretation: 15 marks
3. Test paper, 1 no.: 10 marks

End Semester Examination Pattern: 60 marks

There will be two parts; Part A and Part B.

1. Part A will be conducted by the University in proctored online mode. The examination will be for 60 minutes and will contain 5 multiple choice/short answer questions with 1 question from each module, having 5 marks for each question
2. Part B will be conducted internally by the respective college. The examination will be for 90 minutes and will contain 7 questions with minimum one question from each module of which student should answer any five. Each question can carry 7 marks.
3. The marks obtained for Part B will be regulated in line with the mark scored in Part A.

Course Level Assessment Questions

Course Outcome 1 (CO1):

1. Provide a code vulnerable to heap overrun with an appropriate example to illustrate how a user can misuse it.
2. With the help of a code snippet discuss how as a programmer you can prevent buffer overflows.

Course Outcome 2 (CO2):

1. You have installed a game which requires to modify your registry entry. What are the access rights the game will demand? Is it necessary that you will play the game as an administrator?
2. Comment on the following issues: RPC security setting level and DoS application failure attacks.

Course Outcome 3 (CO3):

1. Discuss SQL injection attacks. How can they be prevented in our applications?
2. With a suitable code illustrate the issues of string handling and type conversion in C language.

Course Outcome 4 (CO4):

1. Consider a web application which allows a user to enter their profile name which is displayed on their profile page. The same name is viewed by every other user of this web application when they want to migrate to each other's page. How can a malicious user misuse this application?
2. Discuss XSS scripting attacks. Can we bypass XSS filters?

Course Outcome 5 (CO5):

1. Illustrate the role of software tester.
2. With a suitable example demonstrate the process of testing file-based applications.

Model Question paper

Reg. No.....

Name:.....

**APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY
FIRST SEMESTER M. TECH DEGREE EXAMINATION**

SECURE CODING

COURSE CODE: 221ECS040

Max. Marks: 25+ 35

Duration: 1+ 1.5 Hours

PART A
MULTIPLE CHOICE -online mode
Each question carries FIVE marks 60 minutes

1

How are authorized users and confidential data managed?

2

Illustrate how threats are modelled using DREAD.

3

Which of the following script is an example of Quick detection in the SQL injection attack? Justify your answer.

- a) `SELECT loginame FROM master..sysprocesses WHERE spid = @@SPID`
- b) For integer inputs : `convert(int, @@version)`
- c) IF condition true-part ELSE false-part (S)
- d) `SELECT header, txt FROM news UNION ALL SELECT name, pass FROM members`

4

Identify the attack where the extra data that holds some specific instructions in the memory for actions is projected by a cyber-criminal or penetration tester to crack the system.

5

Let suppose a search box of an application can take at most 200 words, and you've inserted more than that and pressed the search button; the system crashes. Identify the cause and justify your answer with proper arguments.

PART B -Offline mode
Answer any FIVE full questions
90 minutes

- 6 (a) With the help of a code snippet discuss how as a programmer you can prevent buffer overflows. (3 Marks)
- (b) Provide a code vulnerable to heap overrun with an appropriate example to illustrate how a user can misuse it. (4 Marks)
- 7 (a) You have installed a game which requires to modify your registry entry. What are the access right the game will demand. Is it necessary that you will play the game as an administrator? (3 Marks)
- (b) Comment on the following issues: RPC security setting level and DoS application failure attacks. (4 Marks)
- 8 (a) Illustrate risk mitigation techniques. (3 Marks)
- (b) Illustrate ARP spoofing and discuss its countermeasures. (4 Marks)
- 9 (a) With a suitable code illustrate the issues of string handling and type conversion in C language. (3 Marks)
- (b) Discuss SQL injection attacks. How can they be prevented in our applications? (4 Marks)
- 10 (a) Discuss XSS scripting attacks? Can we bypass XSS filters? (3 Marks)
- (b) Consider a web application which allows a user to enter their profile name which is displayed on their profile page. The same name is viewed by every other user of this web application when they want to migrate to each other's page. How can a malicious user misuse this application? (4 Marks)
- 11 (a) Illustrate the role of software tester. (3 Marks)
- (b) With a suitable example demonstrate the process of testing file-based applications. (4 Marks)

Syllabus

Module I: Introduction to Security Goals and various threats and attacks.

Introduction: Security, CIA Triad, Viruses, Trojans, and Worms In a Nutshell, Security Concepts. Malware Terminology: Active and Passive Security Attacks. IP Spoofing, Tear drop, DoS, DDoS, XSS, SQL injection, Smurf, Man in middle, Format String attack. Types of Security Vulnerabilities- buffer overflows, Invalidated input, race conditions, access control problems, weaknesses in authentication, authorization, or cryptographic practices.

Module II: Security development process and threat modelling.

Secure Software Development Cycle (S-SDLC), Security issues while writing SRS, Design phase security, Development Phase, Test Phase, Maintenance Phase, Writing Secure Code – Best Practices SD3 (Secure by design, default and deployment), Security principles and Secure Product Development Timeline. Threat modelling process and its benefits:

Module III: Secure Coding Techniques.

Secure Coding Techniques: Protection against DoS attacks, Application Failure Attacks, CPU Starvation Attacks, Insecure Coding Practices In Java Technology. ARP Spoofing and its countermeasures. Buffer Overrun- Security Issues in C Language: Avoiding Server Hijacking, Securing RPC, ActiveX and DCOM

Module IV: Database and Web specific issues

Database and Web-specific issues: SQL Injection Techniques and Remedies, Race conditions, Time of Check Versus Time of Use and its protection mechanisms. Validating Input and Inter-process Communication, Securing Signal Handlers and File Operations. XSS scripting attack and its types

Module V: Testing secure applications.

Testing Secure Applications: Security code overview, secure software installation. The Role of the Security Tester, Building the Security Test Plan. Testing HTTP-Based Applications, Testing File-Based Applications, Testing Clients with Rogue Servers

Reference Books

1. Michael Howard and David LeBlanc, “Writing Secure Code”, Microsoft Press US , (2004)
2. Vitaly Osipov, “Buffer Overflow Attacks: Detect, Exploit, Prevent” Syngress, (2005)
3. Frank Swiderski and Window Snyder, “Threat Modelling”, Microsoft Professional,First Edition (2004)
4. Mark G. Graff and Kenneth R. van Wyk, “Secure Coding – Principles & Practices”, O’Reilly (2003).

5. Robert C. Seacord, “Secure Coding in C and C++ (Sei Series in Software Engineering)”, Pearson Addison-Wesley Professional (2013)

COURSE PLAN

| No | Topic – | No. of Lectures |
|-----|---|-----------------|
| 1 | Module I: | <u>8</u> |
| 1.1 | Introduction by discussing Security, CIA Triad, Viruses, Trojans, and Worms In a Nutshell, Security Concepts- exploit, threat, vulnerability, risk, attack. | 1 |
| 1.2 | Malware Terminology: Rootkits, Trapdoors, Botnets, Key loggers, Honeypots | 1 |
| 1.3 | Active and Passive Security Attacks. IP Spoofing, Tear drop, DoS, DDoS | 1 |
| 1.4 | XSS, SQL injection, Smurf, Man in middle, Format String attack. | 1 |
| 1.5 | Types of Security Vulnerabilities- buffer overflows, Invalidated input | 1 |
| 1.6 | race conditions, access control problems | 1 |
| 1.7 | weaknesses in authentication, authorization, or cryptographic practices. | 1 |
| 1.8 | Security in software requirements | 1 |
| 2 | Module II | <u>8</u> |
| 2.1 | Secure Software Development Cycle (S-SDLC), Security issues while writing SRS. | 1 |
| 2.2 | Design phase security, Development Phase, Test Phase, Maintenance Phase, | 1 |
| 2.3 | Writing Secure Code – Best Practices SD3 (Secure by design, default and deployment), | 1 |
| 2.4 | Secure Product Development Timeline | 1 |
| 2.5 | Security principles and. Threat modelling process and its benefits: Identifying the Threats by Using Attack Trees and rating threats using DREAD | 1 |
| 2.6 | Risk Mitigation Techniques and Security Best Practices | 1 |
| 2.7 | Security techniques, authentication, authorization. | 1 |
| 2.8 | Defence in Depth and Principle of Least Privilege. | |
| 3 | Module III | <u>8</u> |
| 3.1 | Secure Coding Techniques: Protection against DoS attacks, ., and, | 1 |
| 3.2 | Application Failure Attacks, CPU Starvation Attacks | 1 |
| 3.3 | Insecure Coding Practices In Java Technology | 1 |
| 3.4 | ARP Spoofing and its countermeasures. | 1 |
| 3.5 | Buffer Overrun- Stack overrun, Heap Overrun, Array Indexing Errors, Format String Bugs. | 1 |
| 3.6 | Security Issues in C Language: String Handling, Avoiding Integer Overflows and Underflows | 1 |
| 3.7 | Type Conversion Issues- Memory Management Issues, Code Injection Attacks | 1 |

| | | |
|-----|--|-----------------|
| 3.8 | Canary based countermeasures using Stack Guard and Propolice. Socket Security, Avoiding Server Hijacking, Securing RPC, ActiveX and DCOM | |
| 4 | Module IV | <u>8</u> |
| 4.1 | SQL injection – attack scenario : SQL Injection Techniques and Remedies, | 1 |
| 4.2 | Solutions – blacklisting, whitelisting, escaping, Second order SQL injection. | 1 |
| 4.3 | Prepared statements and bind variables, mitigating the impact of SQL injection attacks. | 1 |
| 4.4 | Race conditions, Time of Check Versus Time of Use and its protection mechanisms | 1 |
| 4.5 | Validating Input and Inter-process Communication, Securing Signal Handlers and File Operations. | 1 |
| 4.6 | XSS scripting attack and its types | 1 |
| 4.7 | Persistent and Non persistent attack XSS Countermeasures | 1 |
| 4.8 | Bypassing the XSS Filters. | |
| 5 | Module V | <u>8</u> |
| 5.1 | Security code overview. | 1 |
| 5.2 | secure software installation | 1 |
| 5.3 | The Role of the Security Tester | 1 |
| 5.4 | Building the Security Test Plan | 1 |
| 5.5 | Testing HTTP-Based Applications | 1 |
| 5.6 | Testing File-Based Applications – Part 1 | 1 |
| 5.7 | Testing File-Based Applications – Part 2 | 1 |
| 5.8 | Testing Clients with Rogue Servers | 1 |

| | | | | | | |
|-----------|------------------------------|--------------------|---|---|---|--------|
| 221ECS041 | CLOUD COMPUTING AND SECURITY | CATEGORY | L | T | P | CREDIT |
| | | Program Elective 2 | 3 | 0 | 0 | 3 |

Preamble:

This purpose of this course is to provide a basic concepts of security systems and cryptographic protocols, which are widely used in the design of cloud security. The issues related multi tenancy operation, virtualized infrastructure security and methods to improve virtualization security are also dealt with in this course.

Course Prerequisites:

Basic course in distributed computing, computer networks and cryptography at PG/UG level.

Course Outcomes: After the completion of the course the student will be able to

| CO# | CO |
|------|---|
| CO 1 | Examine the various cloud computing models and services. (Cognitive Knowledge Level: Apply) |
| CO 2 | Experiment the implementing virtualization techniques. (Cognitive Knowledge Level: Apply) |
| CO 3 | Use appropriate cloud programming methods to solve big data problems. (Cognitive Knowledge Level: Apply) |
| CO 4 | Examine the need for security mechanisms in cloud (Cognitive Knowledge Level: Analyse) |
| CO 5 | Compare the different popular cloud computing platforms (Cognitive Knowledge Level: Analyse) |

Mapping of course outcomes with program outcomes

| | PO 1 | PO 2 | PO 3 | PO 4 | PO 5 | PO 6 | PO 7 |
|------|------|------|------|------|------|------|------|
| CO 1 | | | | ✓ | | ✓ | |
| CO 2 | | | | ✓ | | ✓ | |
| CO 3 | | | | ✓ | | ✓ | |
| CO 4 | | | | ✓ | ✓ | ✓ | |
| CO 5 | | | | ✓ | ✓ | ✓ | |

Assessment Pattern

| Bloom's Category | End Semester Examination |
|------------------|--------------------------|
| Apply | 40 |
| Analyse | 25 |
| Evaluate | 35 |
| Create | |

Mark distribution

| Total Marks | CIE | ESE | ESE Duration |
|-------------|-----|-----|--------------|
| 100 | 40 | 60 | 2.5 hours |

Continuous Internal Evaluation Pattern:

Preparing a review article based on peer reviewed original publications (minimum 10 publications shall be referred): 15 marks

Course based task/Seminar/Data collection and interpretation: 15 marks

Test paper: 10 marks

Test paper shall include minimum 80% of the syllabus.

End Semester Examination Pattern:

There will be two parts: Part A and Part B. Part A will contain 5 numerical/short answer questions with 1 question from each module, having 5 marks for each question. Students should answer all questions. Part B will contain 7 questions, with minimum one question from each module of which student should answer any five. Each question can carry 7 marks.

Syllabus

Module 1(Cloud Computing Fundamental)

Overview of Computing Paradigms-Grid Computing, Cluster Computing, Distributed Computing, Utility Computing, Cloud Computing. NIST reference Model-Basic terminology and concepts. Cloud characteristics, benefits and challenges, Roles and Boundaries. Cloud delivery (service) models-Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS),

Software-as-a-Service (SaaS), XaaS (Anything-as-a-service)-Cloud deployment models- Public cloud, Community cloud, Private cloud, Hybrid cloud.

Module 2(Virtualization)

Introduction to component virtualization Basics of Virtualization - Types of Virtualizations - Implementation Levels of Virtualization - Virtualization of CPU, Memory, I/O Devices - Desktop Virtualization – Server Virtualization Storage Virtualization – Network Virtualization.

Module 3 (Architectural Design of Compute and Storage Clouds)

Layered Cloud Architecture Development – Design Challenges - Inter Cloud Resource Management – Resource Provisioning and Platform Deployment – Global Exchange of Cloud Resources.

(Cloud Programming) Parallel Computing and Programming Paradigms. Map Reduce – Hadoop Library from Apache, HDFS, Pig Latin High Level Languages, Apache Spark.

Module 4(Fundamental Cloud Security)

Basic terms and concepts in security-- Cloud Security Challenges Software-as-a-Service Security – Security Governance - Threat agents, Cloud security threats/risks, Trust. Operating system security-Virtual machine security- Security of virtualization- Security Risks Posed by Shared Images, Security Risks Posed by Management OS. Infrastructure security Network Level Security, Host Level Security, Data Security, Application-level security, Security of the Physical Systems- Virtual Machine Security Identity & Access Management- Access Control.

Module 5 (Popular Cloud Platforms) Amazon Web Services (AWS):- AWS ecosystem- Computing services, Amazon machine images, Elastic Compute Cloud (EC2), Advanced compute services. Storage services-Simple Storage System (Amazon S3), Elastic Block Store (Amazon EBS), Database Services, Amazon CDN Services and Communication services.

(Google Cloud Platform) IaaS Offerings: Compute Engine (GCE), Cloud Storage, PaaS Offerings: Google App Engine (GAE), Storage services, Application services, Compute services, Database Services, SaaS Offerings: Gmail, Docs, Google Drive.

(Microsoft Azure) Azure Platform Architecture, Hyper-V, Azure Virtual Machine, Compute services, Storage services.

Reference Books

1. Kai Hwang, Geoffrey C Fox, Jack G Dongarra, “Distributed and Cloud Computing, From Parallel Processing to the Internet of Things”, Morgan Kaufmann Publishers, 2012.
2. John W.Rittinghouse and James F.Ransome, “Cloud Computing: Implementation, Management, and Security”, CRC Press, 2010.
3. Toby Velte, Anthony Velte, Robert Elsenpeter, “Cloud Computing, A Practical Approach”, TMH, 2009.
4. George Reese, “Cloud Application Architectures: Building Applications and Infrastructure in the Cloud” O'Reilly, 2009.
5. Anthony T. Velte, Toby Velte, Robert Elsenpeter, Computing, A Practical Approach, McGraw-HillOsborne
6. Dimitris N. Chorafas, Cloud Computing Strategies, CRC Press
7. Tim Mather, SubraKumaraswamy, ShahedLatif, Cloud Security and Privacy: An EnterprisePerspective on Risks and Compliance, O'Reilly Media
8. Ronald L. Krutz, Cloud Security: A Comprehensive Guide to Secure Cloud Computing, John Wiley& Sons
9. Buyya, R., Vecchiola, C., & Selvi, S. T. “Mastering cloud computing: foundations and applications programming”, (2017 Edition), Morgan Kaufmann.
10. Bhowmik, S., “Cloud computing”, (2017 Edition). Cambridge University Press.

Course Level Assessment Questions

Course Outcome 1 (CO1):

1. “A hybrid cloud is a combination of two or more other cloud deployment models”. Justify the statement with an example.
2. Examine the main characteristics of a Platform-as-a-Service solution?
3. “Cloud computing help to reduce the time to market for applications and to cut down capital expenses “! Conclude?

Course Outcome 2 (CO2):

1. Discuss virtualization. What is the role of VMM in virtualization?
2. Compare various implementation levels of Virtualization.
3. State the differences between a traditional computer and a virtual machine.

Course Outcome 3(CO3):

1. Compare on-premise and cloud-based internetworking.

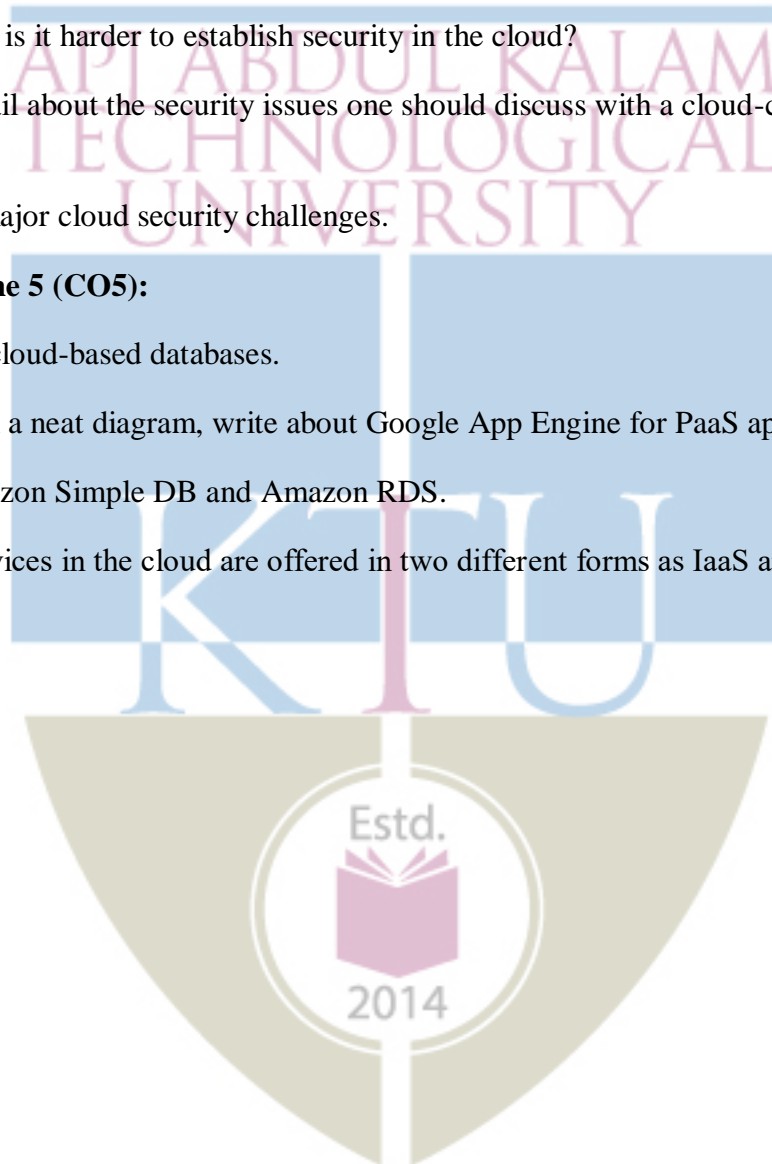
2. Determine how virtualization be implemented at the hardware level?
3. Design a Hadoop Map Reduce program that counts the number of occurrences of each character in a file.
4. Illustrate a Hadoop Map Reduce program to find the maximum temperature in the weather dataset.

Course Outcome 4 (CO4):

1. Estimate why is it harder to establish security in the cloud?
2. Justify in detail about the security issues one should discuss with a cloud-computing vendor.
3. List out the major cloud security challenges.

Course Outcome 5 (CO5):

1. Interpret the cloud-based databases.
2. Illustrate with a neat diagram, write about Google App Engine for PaaS applications.
3. Compare amazon Simple DB and Amazon RDS.
4. “Storage services in the cloud are offered in two different forms as IaaS and as SaaS”. Explain.



Model Question paper

QP CODE:

PAGES: 3

Reg No: _____

Name: _____

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

FIRST SEMESTER M. TECH DEGREE EXAMINATION, MONTH & YEAR

Course Code: 221ECS041

Course Name: CLOUD COMPUTING AND SECURITY

Max. Marks: 60

Duration: 2.5 Hours

PART A

Answer all Questions. Each question carries 5 Marks

1. Is the IT outsourcing model of traditional computing similar to cloud computing? Justify.
2. Can I Virtualize all my servers or should some servers or applications not be virtualized?
3. Design a Hadoop Map Reduce program that counts the number of occurrences of each character in a file.
4. Discuss any two identity management techniques used in cloud computing.
5. If clients want to configure the azure file storage, what is your approach do that?

(5x5=25 Marks)

PART B

Answer any 5 questions. Each question carries 7 marks

6. Examine on-demand functionality? how it is provided in cloud computing? (3)
Justify it why grid computing considered as the predecessor of cloud computing? (4)
7. Discover why a hyper visor is also called a virtual machine monitor? (3)
Explain Xen? Discuss its elements for virtualization. (4)
8. Illustrate with a neat diagram and explain Generic Cloud architecture and components. (4)

List out the major functions of the Map Reduce framework? Explain the logical data flow of Map Reduce function using a suitable example. (3)

9. Discover common threats and vulnerabilities in cloud-based environments with suitable examples (4)

Compare data security, application security virtual machine security? (3)

10. Build the architecture of Windows Azure (4)

Discuss some examples of large cloud provider and databases? (3)

11. Classify the basic components of an IaaS-based solution for cloud computing? Also provide some examples of IaaS implementations. (4)

List out the characteristics and challenges of cloud computing (3)

12. Compare full virtualization and Para virtualization. (3)

Storage services in the cloud are offered in two different forms as IaaS and as SaaS". Explain. (4)

(5x7=35Marks)

Course Plan

| No | Contents | No. of Lecture Hours (40 hrs) |
|---|---|----------------------------------|
| Module 1 (Fundamental Cloud Computing) (6 hours) | | |
| 1.1 | Traditional computing: Limitations. | 1 |
| 1.2 | Overview of Computing Paradigms: Grid Computing, Cluster Computing, Distributed Computing, Utility Computing, Cloud Computing. | 1 |
| 1.3 | NIST reference Model Basic terminology and concepts | 1 |
| 1.4 | Cloud characteristics and benefit s, challenges. Roles and Boundaries. | 1 |
| 1.5 | Cloud delivery (service) models: Infrastructure-as-a-Service (IaaS), Platform-asa-Service (PaaS), Software-as-a-Service (SaaS), XaaS (Anything-as-a-service). | 1 |
| 1.6 | Cloud deployment models: Public cloud, Community cloud, Private cloud, Hybrid | 1 |

| | | |
|---|---|---|
| | cloud. | |
| Module 2(Virtualization)(8 Hours) | | |
| 2.1 | Introduction to virtualization, Virtualizing physical computing resources Virtual Machines (Machine virtualization):- non-virtualized v/s virtualized machine environments. | 1 |
| 2.2 | Types of VMs: process VM v/s system VM, Emulation, interpretation and binary translation. | 1 |
| 2.3 | Hardware-level virtualization: Hypervisors/VMM, Types of Hypervisors. | 1 |
| 2.4 | Full Virtualization, Para-Virtualization, Hardware-assisted virtualization, OS level virtualization. | 1 |
| 2.5 | Basics of Network Virtualization | 1 |
| 2.6 | Storage Virtualization and Desktop Virtualization, Pros and cons of virtualization. | 1 |
| 2.7 | Case Study: Xen: Para-virtualization. | 1 |
| 2.8 | Case Study: VMware: full virtualization. | 1 |
| Module 3 (Architectural Design of Compute and Storage Clouds, Cloud Programming) (8 Hours) | | |
| 3.1 | Architectural Design of Compute and Storage Clouds | 1 |
| 3.2 | Layered Cloud Architecture Development – Design Challenges | 1 |
| 3.3 | Inter Cloud Resource Management – Resource Provisioning and Platform Deployment | 1 |
| 3.4 | Global Exchange of Cloud Resources. | 1 |
| 3.5 | Cloud Programming: Parallel Computing and Programming Paradigms. | 1 |
| 3.6 | Map Reduce. | 1 |
| 3.7 | Hadoop Library from Apache, HDFS. | 1 |
| 3.8 | Pig Latin High Level Languages, Apache | 1 |

| | | |
|--|---|---|
| | Spark. | |
| Module 4 (Fundamental Cloud Security) (8 Hours) | | |
| 4.1 | Basic terms and concepts in security | 1 |
| 4.2 | Cloud Security Challenges Software-as-a-Service Security, Security Governance | 1 |
| 4.3 | Threat agents, Cloud security threats/risks, Trust. | 1 |
| 4.4 | Operating system security-Virtual machine security- | 1 |
| 4.5 | Security of virtualization- Security Risks Posed by Shared Images, Security Risks Posed by Management OS. | 1 |
| 4.6 | Infrastructure security Network Level Security, Host Level Security, Data Security , Application level security, | 1 |
| 4.7 | Security of the Physical Systems- Virtual Machine Security. | 1 |
| 4.8 | Identity & Access Management- Access Control. | 1 |
| Module 5 (Popular Cloud Platforms) (9 Hours) | | |
| 5.1 | Amazon Web Services (AWS):- AWS ecosystem, Computing services: Amazon machine images, Elastic Compute Cloud (EC2). | 1 |
| 5.2 | Advanced computing services, Storage services: Simple Storage System (Amazon S3), Elastic Block Store (Amazon EBS). | 1 |
| 5.3 | Database Services, Amazon CDN Services and Communication services. | 1 |
| 5.4 | Google Cloud Platform:- IaaS Offerings: Compute Engine (GCE), Cloud Storage | 1 |
| 5.5 | PaaS Offerings: Google App Engine (GAE), Storage services, Application services, Compute services. | 2 |
| 5.6 | Database Services, SaaS Offerings: Gmail, Docs, Google Drive. | 1 |

| | | |
|-----|---|---|
| 5.7 | Microsoft Azure: Azure Platform Architecture, Hyper-V, Azure Virtual Machine. | 1 |
| 5.8 | Azure Compute services, Storage services. | 1 |



| | | | | | | |
|-----------|----------------------------|--------------------|---|---|---|--------|
| 221ECS042 | FORMAL METHODS IN SECURITY | CATEGORY | L | T | P | CREDIT |
| | | Program Elective 2 | 3 | 0 | 0 | 3 |

Preamble:

The purpose of this course is to provide the formal methods of logic and program verification. This course understands the temporal logic and model checking for detecting security vulnerabilities. The student gains fundamental knowledge in formal aspects of secure computing and is able to formally verify and analyse the protocols.

Course Outcomes: After the completion of the course the student will be able to

| CO# | Course Outcome |
|------|--|
| CO 1 | Demonstrate Formal Methods- Logic and Program Verification (Cognitive Knowledge Level: Apply) |
| CO 2 | Use Temporal Logic and Model Checking for program verifications (Cognitive Knowledge Level: Analyze) |
| CO 3 | Verify concurrent and reactive programs/systems using model-checking and propositional temporal logic. (Cognitive Knowledge Level: Analyze) |
| CO 4 | Use static and dynamic program analysis and model-checking for detecting common security vulnerabilities in programs and communication protocols (Cognitive Knowledge Level: Analyze) |
| CO 5 | Familiarize SPIN, PVS, TAMARIN, Frama-C and Isabelle tools (Cognitive Knowledge Level: Understand) |

Mapping of course outcomes with program outcomes

| | PO 1 | PO 2 | PO 3 | PO 4 | PO 5 | PO 6 | PO 7 |
|------|------|------|------|------|------|------|------|
| CO 1 | | | ✓ | ✓ | | ✓ | |
| CO 2 | | ✓ | | ✓ | | ✓ | |
| CO 3 | | | | ✓ | ✓ | ✓ | |
| CO 4 | | ✓ | | ✓ | | ✓ | |
| CO 5 | ✓ | | | ✓ | ✓ | ✓ | |

Assessment Pattern

| Bloom's Category | End Semester Examination |
|------------------|--------------------------|
| Apply | 40 |
| Analyse | 35 |
| Evaluate | 25 |
| Create | |

Mark distribution

| Total Marks | CIE | ESE | ESE Duration |
|-------------|-----|-----|--------------|
| 100 | 40 | 60 | 2.5 hours |

Continuous Internal Evaluation Pattern:

Preparing a review article based on peer reviewed

Original publications (minimum 10 publications shall be referred): 15 marks

Course based task/Seminar/Data collection and interpretation: 15 marks

Test paper, 1 no. : 10 marks

Test paper shall include minimum 80% of the syllabus.

End Semester Examination Pattern:

There will be two parts: Part A and Part B. Part A will contain 5 numerical/short answer questions with 1 question from each module, having 5 marks for each question. Students should answer all questions. Part B will contain 7 questions, with minimum one question from each module of which student should answer any five. Each question can carry 7 marks.

Syllabus

Module 1

Formal Methods – Propositional and Predicate logic, and theorem-proving, Fixed-points and their role in program analysis and model-checking, Formal methods in secure computing- Clark Wilson model and Chinese wall model.

Module 2

Verification of sequential programs using weakest preconditions and inductive methods, and verification of concurrent and reactive programs/systems using model-checking and propositional temporal logic (CTL and LTL). Modelling security protocol, trustworthy processes, data types for models, modelling an intruder.

Module 3

Application of static and dynamic program analysis and model-checking for detecting common security vulnerabilities in programs and communication protocols. Protocol goals- Yahalom protocol, secrecy, External threat authentication.

Module 4

Information flow and taint analysis for the security of web applications, pi-calculus for formal modelling of mobile systems and their security. Non -repudiation Zhou-Gollmann protocol, anonymity and Dining cryptographers' analysis.

Module 5

SPIN, PVS, TAMARIN, Frama-C and Isabelle tools familiarization. Introduction of secure computing protocol model-Dolev Yao model, BAN logic and derivatives.

TEXT BOOKS:

1. Edmund M. Clarke, Orna Grumberg and Doron Peled, Model Checking, MIT Press, 1999.
2. Lloyd, J.W., Logic and Learning: Knowledge Representation, Computation and Learning in Higher-order Logic, Springer Berlin Heidelberg, 2003.
3. M. Ruth and M. Ryan, Logic in Computer Science - Modelling and Reasoning about Systems, Cambridge University Press, 2004 .
4. G. Bella, Formal Correctness of Security Protocols, Springer, 2009. 5. Datta A, Jha S, Li N, Melski D and Reps T, Analysis Techniques for Information Security, Synthesis Lectures on Information Security, Privacy, and Trust, 2010.

REFERENCES

1. Peter Ryan, Steve Schneider, M. H. Goldsmith, "Modelling and Analysis of Security Protocols", Pearson Education, 2010.
2. Theo Dimitrakos, Fabio Martinelli, "Formal Aspects In Security And Trust: Ifip TN Wg1.7", Workshop on Formal Aspects in Security, Springer, 2005.
3. W. Mao, "Modern Cryptography: Theory & Practice", Pearson Education, 2004.
4. Giampaolo Bella, "Formal Verification of Security Protocols", Springer, 2007.
5. Colin Boyd, Anish Mathuria, "Protocols for Authentication and Key Establishment", Springer, 2003.
6. Giampaolo Bella, "Formal Correctness of Security Protocols (Information Security and Cryptography)", Springer, 1e, 2007.

Course Level Assessment Questions

Course Outcome 1 (CO1):

1. Demonstrate fixed points in program analysis.
2. Describe the Chinese wall model.

Course Outcome 2 (CO2) :

1. Illustrate with an example Verification using model-checking.
2. Design the modelling of security protocol citing a real world scenario.

Course Outcome 3(CO3):

1. Illustrate the model checking process for communication protocol.
2. Discuss Yahalom protocol in formal secure computing.

Course Outcome 4 (CO4):

1. Demonstrate the pi-calculus formal modelling for system security.
2. Give the taint analysis for the security of web applications.

Course Outcome 5 (CO5):

1. Explain PVS familiarization in detail.
2. Explain BAN logic and its derivatives

Model Question paper

QP CODE:

PAGES: 3

Reg No: _____

Name: _____

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

FIRST SEMESTER M. TECH DEGREE EXAMINATION, MONTH & YEAR

Course Code: 221ECS042

Course Name: Formal methods in Security

Max. Marks: 60

Duration: 2.5 Hours

PART A

Answer all Questions. Each question carries 5 Marks

1. What is a formal method in security?
2. Explain the propositional temporal logic of CTL and LTL.
3. Explain the model checking process for security vulnerabilities.
4. What is information flow in relation to formal methods in security?
5. Discuss the concept behind modelling an intruder.

(5x3=15 Marks)

PART B

Answer any 5 questions. Each question carries 7 marks

6. Differentiate propositional and predicate logic.
7. Explain the Theorem proving logic in detail.
8. Explain the verification using inductive methods.
9. Explain the application of static vs dynamic program analysis.
10. Explain Isabelle tools in detail.
11. Explain the process of concurrent and reactive programs.

(5x7=35 Marks)

Course Plan

| No | Topic | No. of Lectures |
|----------|---|-----------------|
| 1 | Formal methods | 8 hours |
| 1.1 | Formal Methods in security | 1 |
| 1.2 | Propositional and Predicate logic | 1 |
| 1.3 | Theorem-proving logic | 1 |
| 1.4 | Fixed-points | 1 |
| 1.5 | Fixed points in program analysis | 1 |
| 1.6 | Fixed points in model checking | 1 |
| 1.7 | Formal methods in secure computing | 1 |
| 1.8 | Clark Wilson model and Chinese wall model | 1 |
| 2 | Verification | 8 hours |
| 2.1 | Introduction in Verification | 1 |
| 2.2 | Verification of sequential programs using weakest preconditions | 1 |
| 2.3 | Verification using inductive methods | 1 |
| 2.4 | Verification of concurrent and reactive programs | 1 |
| 2.5 | Verification using model-checking | 1 |
| 2.6 | Propositional temporal logic (CTL and LTL) | 1 |
| 2.7 | Modelling security protocol | 1 |
| 2.8 | Modelling an intruder | 1 |
| 3 | Formal methods applications | 8 hours |
| 3.1 | Application of static and dynamic program analysis | 2 |
| 3.2 | Model-checking for detecting common security vulnerabilities | 2 |
| 3.3 | communication protocols model checking | 2 |
| 3.4 | Protocol goals- Yahalom protocol, secrecy | 1 |
| 3.5 | External threat authentication | 1 |
| 4 | Formal modelling 8 hours | |
| 4.1 | Information flow | 1 |
| 4.2 | Taint analysis for the security of web applications | 2 |
| 4.3 | pi-calculus for formal modelling of mobile systems | 2 |
| 4.4 | pi-calculus for formal modelling of mobile system security | 2 |
| 4.5 | Zhou Gollmann and Dining cryptographers' analysis-anonymity | 1 |
| 5 | Familiarization | 8 hours |
| 5.1 | SPIN familiarization | 2 |
| 5.2 | PVS familiarization | 1 |
| 5.3 | TAMARIN familiarization | 1 |
| 5.4 | Frama-C familiarization | 1 |
| 5.5 | Isabelle tools familiarization | 1 |
| 5.6 | Dolev Yao model | 1 |
| 5.7 | BAN logic and derivatives | 1 |

| | | | | | | |
|-----------|-------------------------------|-----------------------|---|---|---|--------|
| 221ECS043 | COURSE NAME LINEAR ALGEBRA | CATEGORY | L | T | P | CREDIT |
| | | Program Elective 2 | 3 | 0 | 0 | 3 |

Preamble: This course introduces the tools and methods of linear algebra that are important in many areas of computer science, such as graphics, image processing, cryptography, machine learning, computer vision, optimization, information retrieval, and web search. Vector space provides an abstract framework for studying linear operations involving a variety of mathematical objects such as n-tuples, polynomials, matrices, and functions. The concepts of basis and linear transformations provide the necessary tools for operating within and between vector spaces, and matrix algorithms aid in the practical implementation of these ideas. The concept of inner product is useful for doing approximations and orthogonal projections in vector spaces.

Course Outcomes: The COs shown are only indicative. For each course, there can be 4 to 6 COs.

After the completion of the course the student will be able to

| | |
|-------------|--|
| CO 1 | Recognize familiar mathematical objects as vector spaces and identify their subspaces, bases and dimension. (Cognitive Knowledge level:Apply) |
| CO 2 | Apply principles of matrix algebra to build and operate linear transformations. (Cognitive Knowledge level:Apply) |
| CO 3 | Utilize the concept of orthogonality to construct approximations and projections. (Cognitive Knowledge level:Apply) |
| CO 4 | Compute eigen values and eigen vectors and use them to simplify operations involving large matrices (Cognitive Knowledge level:Analyze) |
| CO 5 | Apply the tools of linear algebra in the representation and manipulation of data (Cognitive Knowledge level:Evaluate) |

Program Outcomes - POs

- PO1** An ability to carry out research/investigation and development work in engineering and allied streams.
- PO2** An ability to communicate effectively, write and present technical reports on complex engineering activities by interacting with the engineering fraternity and with society at large.
- PO3** An ability to demonstrate a degree of mastery over the area as per the specialization of the program. The mastery should be at a level higher than the requirements in the appropriate bachelor program.
- PO4** An ability to apply stream knowledge to design or develop solutions for real world problems by following the standards.

PO5 An ability to identify, select and apply appropriate techniques, resources and state-of-the-art tool to model, analyse and solve practical engineering problems.

PO6 An ability to engage in life-long learning for the design and development related to the stream related problems taking into consideration sustainability, societal, ethical and environmental aspects.

PO7 An ability to develop cognitive load management skills related to project management and finance which focus on Entrepreneurship and Industry relevance.

Mapping of course outcomes with program outcomes

| | PO 1 | PO 2 | PO 3 | PO 4 | PO 5 | PO 6 | PO 7 |
|------|------|------|------|------|------|------|------|
| CO 1 | ✓ | ✓ | ✓ | | ✓ | | |
| CO 2 | ✓ | ✓ | ✓ | | ✓ | | |
| CO 3 | ✓ | ✓ | ✓ | | ✓ | | |
| CO 4 | ✓ | ✓ | ✓ | | ✓ | | |
| CO 5 | ✓ | ✓ | ✓ | | ✓ | | |

Assessment Pattern

| Bloom's Category | End Semester Examination |
|------------------|--------------------------|
| Apply | 70-80% |
| Analyse | 20-30% |
| Evaluate | |
| Create | |

Mark distribution

| Total Marks | CIE | ESE | ESE Duration |
|-------------|-----|-----|--------------|
| 100 | 40 | 60 | 2.5 hours |

Continuous Internal Evaluation : 40 marks

Evaluation shall only be based on application, analysis or design-based questions (for both internal and end semester examinations).

1. Preparing a review article based on peer reviewed original publications (minimum 10 publications shall be referred) : 15 marks
2. Course based task / Seminar/ Data collection and interpretation: 15 marks

15 marks

3. Test paper (1 number) :

10 marks

Test paper shall include minimum 80% of the syllabus.

Course based task/test paper questions shall be useful in the testing of knowledge, skills, comprehension, application, analysis, synthesis, evaluation and understanding of the students.

End Semester Examination Pattern:

There will be two parts; Part A and Part B. Part A contains 5 questions with 1 question from each module, having 4 marks for each question. Students should answer all questions. Part B contains 2 questions from each module of which a student should answer any one. Each question can have maximum 2 sub-divisions

The end semester examination will be conducted by the respective College.

There will be two parts; Part A and Part B. Part A will contain 5 numerical/short answer questions with 1 question from each module, having 5 marks for each question. Students should answer all questions. Part B will contain 7 questions (such questions shall be useful in the testing of overall achievement and maturity of the students in a course, through long answer questions relating to theoretical/practical knowledge, derivations, problem solving and quantitative evaluation), with minimum one question from each module of which student should answer any five. Each question can carry 7 marks

Total duration of the examination will be 150 minutes.

Note: The marks obtained for the ESE for an elective course shall not exceed 20% over the average ESE mark % for the core courses. ESE marks awarded to a student for each elective course shall be normalized accordingly.

For example, if the average end semester mark % for a core course is 40, then the maximum eligible mark % for an elective course is $40+20 = 60\%$.

Course level assessment questions.

Course outcome 1

1. In each of the following check whether R^2 is a vector space with respect to the given definitions of addition and scalar multiplication

a) $(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2), \quad c(x, y) = (cx, y)$

b) $(x_1, y_1) + (x_2, y_2) = (x_1, 0), \quad c(x, y) = (cx, cy)$

c) $(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2), \quad c(x, y) = (\sqrt{cx}, \sqrt{cy})$

2. Find the coordinate vector of $u = 5x^2 + x + 9$ with respect to the basis

$$B = \{x^2 - x + 1, 3x^2 - 1, 2x^2 + x + 2\} \text{ Of } P_2.$$

Course outcome 2

1. Show that the mapping $T: P_2 \rightarrow P_3$ defined by $T[p(x)] = (x + 1)p(x - 2)$ is a linear transformation. What is the matrix of T with respect to the standard bases of P_2 and P_3 ?
2. Find the matrix representing the linear transformation $T: R^2 \rightarrow R^2$ which rotates the plane by 45 degrees counterclockwise and then reflects across the horizontal X- axis.

Course outcome 3

1. A is a 3×3 matrix with eigen values $-1, 0$ and 1 , with corresponding eigen vectors $\begin{pmatrix} 1 \\ 0 \\ 2 \end{pmatrix}, \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix}$ and $\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$ respectively. Find the matrix A and compute A^{20} . State all the results you use to arrive at the answer.
2. Show that the reflection of the plane R^2 in the line $y = -x$ is a diagonalizable transformation and find the diagonal matrix representation of it and the basis for this representation

Course outcome 4

1. Find the orthogonal complement of the subspace of R^4 spanned by the vectors $(1,2,2,1)$ and $(3,4,2,3)$
2. Does there exist an inner product in R^2 , in which the vectors $(1,3)$ and $(-1,2)$ are orthogonal? If yes, construct it. If no, why?

Course outcome 5

1. Find a QR-decomposition of the matrix $\begin{bmatrix} 1 & -1 \\ 0 & 0 \\ 2 & 1 \end{bmatrix}$
2. Use power method to find the dominant eigen value and the corresponding eigen vector of the matrix $\begin{bmatrix} 5 & 4 & 2 \\ 4 & 5 & 2 \\ 2 & 2 & 2 \end{bmatrix}$

Reg. No.

Name:

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

FIRST SEMESTER M. TECH DEGREE EXAMINATION

221ECS043-LINEAR ALGEBRA

Max. Marks: 60

Duration: 2.5 hours

PART A

(answer all questions. Each question carries 5 marks)

1. Check whether the polynomials $x^2 + 1$, $3x - 1$, $-4x + 1$ are linearly independent in P_2 , the vector space of polynomials of degree 2 or less.
2. A linear transformation $T: R^2 \rightarrow R^3$ is given by $T(a, b) = (a + b, a - b, 2b)$. Find the matrix of T with respect to the standard bases of R^2 and R^3 .
3. Compute the eigen values of the linear transformation $T: R^2 \rightarrow R^2$ defined by $T(a, b) = (2a - b, a + 4b)$
4. Find any orthonormal basis of the vector space M_2 of all real matrices of order 2×2 with the usual operations and standard inner product.
5. Find the LU decomposition of the matrix $\begin{bmatrix} 2 & 2 \\ 4 & 9 \end{bmatrix}$.

PART B

(Answer any 5 questions. Each question carries 7 marks)

6. Show that the set V of points lying on the plane $2x - y + z = 0$ is a subspace of R^3 . Find a basis and dimension of V .
7. Given the two bases $B = \{(1,2), (3, -1)\}$ and $C = \{(3,1), (5,2)\}$ of R^2 , find the basis change transition matrices from B to C and C to B . If the vector u has coordinates $(2,3)$ in the basis B find its coordinates in the basis C .
8. Check whether the map $T: P_2 \rightarrow P_2$ defined by $T(p) = p(2x + 1)$ is diagonalizable
9. Use Gram Schmidt orthogonalization process to construct an orthonormal basis for the set of vectors $(x, y, z) \in R^3$, lying in the plane $P = \{(x, y, z): 2x - y + 3z = 0\}$
10. Compute the projection of the vector $(3, -1, 2)$ on the plane $x + y + z = 0$ in R^3 under the standard inner product.
11. Find a singular value decomposition of the matrix $\begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 0 \end{bmatrix}$.

12. Find the least square solution to the following inconsistent system of equations

$$\begin{aligned}x + 2y + z &= 1 \\3x - y &= 2 \\2x + y - z &= 2 \\x + 2y + 2z &= 1\end{aligned}$$

Syllabus

Module 1

Vector Spaces-Definition and Examples. Subspaces, Spanning sets and linear independence. Basis and dimension, Co-ordinates with respect to a given basis. Row space, Column space and null space of a matrix

Module 2

Linear transformations between vector spaces and their properties, Kernel and range of linear transformations, Rank Nullity theorem, matrix representation of linear transformation, invertible transformations and their matrix representation, co-ordinates and linear transformations under change of basis, similar matrices. Isomorphism between n-space and finite dimensional vector spaces

Module 3

Eigen values, eigenvectors and eigen spaces of matrices and linear transformation, Properties of eigen values and eigen vectors, Diagonalization of matrices, orthogonal diagonalization of real symmetric matrices, representation of linear transformation by diagonal matrix,

Module 4

Real Inner Product spaces, properties of inner product, length and distance, Cauchy-Schwarz inequality, Orthogonality, Orthonormal basis, Gram Schmidt orthogonalization process. Orthogonal subspaces, Orthogonal projection. orthogonal complement and direct sum representation.

Module 5

LU-decomposition of matrices, QR-decomposition, Singular value decomposition, Least squares solution of inconsistent linear systems, curve-fitting by least square method. Power method for finding dominant eigen value,

Text Books

1. Richard Bronson, Gabriel B. Costa, Linear Algebra-an introduction, 2nd edition, Academic press, 2007
2. Gareth Williams, Linear Algebra with Applications, Jones and Bartlett Publishers, eighth edition, 2014

References

1. Gilbert Strang, Linear Algebra and It's Applications, 4th edition, Cengage Learning, 2006
2. Seymour Lipschutz, Marc Lipson, Schaum's outline of linear algebra, 3rd Ed., Mc Graw Hill Edn.2017
3. David C Lay, Linear algebra and its applications,3rd edition, Pearson
4. Stephen Boyd, Lieven Vandenberghe, Introduction to Applied Linear Algebra: Vectors, Matrices,and Least Squares, Cambridge University Press, 2018
5. W. Keith Nicholson, Linear Algebra with applications, 4th edition, McGraw-Hill, 2002

Course Plan

| No | Module 1 | 8 hours | No. of Lectures |
|-----|--|------------------|-----------------|
| 1 | Vector spaces | | |
| 1.1 | Defining of vector spaces , example | | 1 |
| 1.2 | Subspaces | | 1 |
| 1.3 | Linear dependence, Basis , dimension | | 3 |
| 1.4 | Row space, column space, rank of a matrix | | 2 |
| 1.5 | Co ordinate representation | | 1 |
| 2 | Module 2 | 8 hours | |
| 2.1 | General linear transformation, Matrix of transformation. | | 2 |
| 2.2 | Kernel and range of a linear mapping | | 1 |
| 2.3 | Properties of linear transformations, | | 1 |
| 2.4 | Rank Nullity theorem. | | 1 |
| 2.5 | Change of basis . | | 2 |
| 2.6 | isomorphism | | 1 |
| 3 | Module 3 | (8 hours) | |
| 3.1 | Eigen values and Eigen vectors of a linear transformation and matrix | | 2 |
| 3.2 | Properties of Eigen values and Eigen vectors | | 1 |
| 3.3 | Diagonalization., orthogonal diagonalization | | 3 |
| 3.4 | Diagonalizable linear transformation | | 2 |
| 4 | Module 4 | (8 hours) | |
| 4.1 | Inner Product: Real and complex inner product spaces, | | 2 |
| 4.2 | Properties of inner product, length and distance | | 1 |

| | | |
|-----|---|---|
| 4.3 | Triangular inequality, Cauchy-Schwarz inequality | 1 |
| 4.4 | Orthogonality, Orthogonal complement, Orthonormal bases, | 2 |
| 4.5 | Gram Schmidt orthogonalization process, orthogonal projection | 2 |
| 4.6 | Direct sum representation | 1 |
| 5 | Module 5 (8 hours) | |
| 5.1 | LU decomposition, QR Decomposition | 2 |
| 5.2 | Singular value decomposition | 2 |
| 5.3 | Least square solution | 2 |
| 5.4 | Curve fitting | 1 |
| 5.5 | Power method | 1 |



| | | | | | | |
|-----------|-----------------|----------|---|---|---|--------|
| 221LCS100 | COMPUTING LAB I | CATEGORY | L | T | P | CREDIT |
| | | LAB 1 | 0 | 0 | 2 | 1 |

Preamble: The course is designed to provide students practical knowledge of computer networking, network programming and familiarize them with the cryptographic algorithms. This course aims to provide a foundational platform for Security Aspirants by providing Security Awareness and Training that heighten the chances of catching a scam or attack before it is fully enacted, minimizing damage to the resources and ensuring the protection of information technology assets.

Course Outcomes:

After the completion of the course the student will be able to

| | |
|-------------|--|
| CO 1 | Implement cyber security solutions and use of cyber security, information assurance, and cyber/computer forensics software/tools. (Cognitive Knowledge level : Apply). |
| CO 2 | Demonstrate skills needed to deal with common programming errors that lead to most security problems and to learn how to develop secure applications. (Cognitive Knowledge level : Apply) |
| CO 3 | Identify the nature of the threats to software and incorporate secure coding practices throughout the planning and development of the product. (Cognitive Knowledge level : Analyse) |
| CO 4 | Able to properly handle application faults, implement secure authentication, authorization and data validation controls used to prevent common vulnerabilities. (Cognitive Knowledge level : Apply) |
| CO 5 | Practice with an expertise in academics to design and implement security solutions. (Cognitive Knowledge level : Evaluate) |

Program Outcomes (PO)

Outcomes are the attributes that are to be demonstrated by a graduate after completing the course.

PO1: An ability to independently carry out research/investigation and development work in engineering and allied streams

PO2: An ability to communicate effectively, write and present technical reports on complex engineering activities by interacting with the engineering fraternity and with society at large.

PO3: An ability to demonstrate a degree of mastery over the area as per the specialization of the program. The mastery should be at a level higher than the requirements in the appropriate bachelor program

PO4: An ability to apply stream knowledge to design or develop solutions for real world problems by following the standards

PO5: An ability to identify, select and apply appropriate techniques, resources and state-of-the-art tool to model, analyse and solve practical engineering problems.

PO6: An ability to engage in life-long learning for the design and development related to the stream related problems taking into consideration sustainability, societal, ethical and environmental aspects

PO7: An ability to develop cognitive load management skills related to project management and finance which focus on Entrepreneurship and Industry relevance.

Mapping of course outcomes with program outcomes

| | PO 1 | PO 2 | PO 3 | PO 4 | PO 5 | PO 6 | PO 7 |
|------|------|------|------|------|------|------|------|
| CO 1 | ☑ | | ☑ | ☑ | ☑ | ☑ | |
| CO 2 | ☑ | | ☑ | ☑ | ☑ | ☑ | |
| CO 3 | ☑ | | ☑ | ☑ | ☑ | ☑ | ☑ |
| CO 4 | ☑ | | ☑ | ☑ | ☑ | ☑ | ☑ |
| CO 5 | ☑ | | ☑ | | ☑ | ☑ | ☑ |

Assessment Pattern

| Bloom's Category | End Semester Examination |
|------------------|--------------------------|
| Apply | 60 |
| Analyse | 20 |
| Evaluate | 20 |

| | |
|--------|--|
| Create | |
|--------|--|

Mark distribution

| Total Marks | CIE | ESE | ESE Duration |
|-------------|-----|-----|--------------|
| 100 | 100 | - | 3hours |

LABORATORY COURSES

The laboratory courses will be having only Continuous Internal Evaluation and carries 100 marks. Final assessment shall be done by two examiners; one examiner will be a senior faculty from the same department.

LAB REPORT:

All the students attending the Lab should have a Fair Report. The report should contain details of the experiment such as Objective, Algorithm/Design, Description, Implementation, Analysis, Results, and Outcome. The report should contain a printout of the respective code with inputs addressing all the aspects of the algorithm described and corresponding outputs. All the experiments noted in the fair report should be verified by the faculty regularly. The fair report, properly certified by the faculty, should be produced during the time of the final assessment.

SYLLABUS

Hash Value Generation and verification, Forensic Acquisition using Software acquisition tool, Analysis of forensic image file. Addressing Data Hiding Techniques using Hex Workshop/Win hex. Extraction and Examination of Registry files. Acquisition and Analysis of Live Data.

Familiarization with CRYPTOOL, Familiarization with Open SSL. AES algorithm for 128-bit key, RSA algorithm. Secure hash algorithm, Digital signature algorithm, Diffie-Hellman key exchange. Elliptic curve cryptography algorithm. Secure mail using PGP. Familiarization with Wireshark, Familiarization with Backtrack (Kali Linux).

References

- 1) Nelson, Phillips Enfinger, Steuart, Guide to Computer Forensics and Investigations ,Sixth Edition CENGAGE Learning.
- 2) Harlan Carvey ,Windows Forensic Analysis DVD Toolkit, Edition 2, Syngress Inc. ,2009

3) Harlan Carvey ,Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry .

4) Wale Soyinka, Linux Administration: A Beginner's Guide, 6th Edition, McGraw-Hill Education

5) W. Richard Stevens, UNIX Network Programming Volume I, Pearson Education

6) D.E. Comer, Internetworking with TCP/IP Volume III, Pearson Education

7) Jason Weiss, Java Cryptography Extensions: Practical Guide for Programmers (The Practical Guides), Morgan Kaufmann Publishers.

Sample List of Exercises/Experiments:

A student is requested to do a set of 6 to 10 experiments minimum

| SLNO | Experiment Details | No of hours |
|------|--|-------------|
| 1 | Generate and Validate Hash Values of Office Files, PDFs , multimedia files using Hasher tool. | 2 |
| 2 | Forensic Image Acquisition using TrueBack and Encase Imager. | 2 |
| 3 | Analyze an Image file using Cyber Check tool and FTK/ProDiscover, Familiarisation of Report Module in above tools. | 4 |
| 4 | Try out Data Hiding Techniques using Hex Workshop/Win hex tool | 2 |
| 5 | To Analyse Windows Registry Files using FRAN /Prodiscover. | 2 |
| 6 | Acquisition and Analysis of Live Data Using WinLift tool and Familiarization of volatility Framework and PS Tools | 4 |
| 7 | Familiarization with CRYPTOOL, Familiarization with Open SSL. | 2 |
| 8 | AES algorithm for 128-bit key, RSA algorithm. Secure hash algorithm | 4 |
| 9 | Digital signature algorithm, Diffie-Hellman key exchange. | 2 |
| 10 | Elliptic curve cryptography algorithm | 2 |
| 11 | Secure mail using PGP. S/MIME standard | 2 |

| | | |
|----|--|---|
| 12 | Familiarization with Wireshark, Familiarization with Backtrack (Kali Linux). | 4 |
| 13 | Implement program to send an encrypted string via Bluetooth from a PC as client to a mobile as server. | 2 |
| 14 | Program for distributed Denial of service | 2 |
| 15 | SQL Injection | 2 |

APJ ABDUL KALAM
TECHNOLOGICAL
UNIVERSITY

