| | | | | |
|---|---|---|---|---|
| | CRYPTOGRAPHY & NETWORK SECURITY | | Semester | 7 |
| | Course Code | BCS703 | CIE Marks | 50 |
| | Teaching Hours/Week S) | | SEE Marks | 50 |
| | Total Hours of Pedagogy | 50 | Total Marks | 100 |
| | Credits | 04 | Exam Hours | 3 |
| | Examination type (SEE) | Theory | | |

Course objectives:

1. Understand the basics of Cryptography concepts, Security and its principle
2. To analyse different Cryptographic Algorithms
3. To illustrate public and private key cryptography
4. To understand the key distribution scenario and certification
5. To understand approaches and techniques to build protection mechanism in order to secure computer networks

Teaching-Learning Process

These are sample Strategies, which teachers can use to accelerate the attainment of the various course outcomes.

l. Lecturer method (L) needs not to be only a traditional lecture method, but alternative effective teaching methods could be adopted to attain the outcomes.

2. Use Of Video/Animation to explain functioning of various concepts.
3. Encourage collaborative (Group Learning) Learning in the class.
4. Ask at least three HOT (Higher order Thinking) questions in the class, which promotes critical thinking
5. Adopt Problem Based Learning (PBL), which fosters students' Analytical skills, develop design thinking skills such as the ability to design, evaluate, generalize, and analyze information rather than simply recall it.
6. Introduce Topics in manifold representations.
7. Show the different ways to solve the same problem with different circuits/logic and encourage the students to come up with their own creative ways to solve them.
8. Discuss how every concept can be applied to the real world - and when that's possible, it helps improve the students' understanding
9. Use any Of these methods: Chalk and board, Active Learning, Case Studies

Module-I 10 hours

| | |
|---|---|
| | A model for Network Security, Classical encryption techniques: Symmetric cipher model, Substitution ciphers-Caesar Cipher, Monoalphabetic Cipher, Playfair Cipher, Hill Cipher, Polyalphabetic Ciphers, One time pad, Steganography.<br>Block Ciphers and Data Encryption Standards: Traditional Block Cipher structures, data Encryption Standard (DES), A DES Example, The strength of DES, Block cipher design principles.<br><br>Cha ter 1: 1.8 Cha 3: 3.1, 3.2, 3.5 Cha ter4: 4.1, 4.2, 4.3, 4.4, 4.5 |
| | Module-2 10 hours |

Il 2

| | |
|---|---|
| | Pseudorandom number Generators: Linear Congruential Generators, Blum Blum Shub Generator.<br>Public key cryptography and RSA: Principles of public key cryptosystems-Public key cryptosystems, Applications for public key cryptosystems, Requirements for public key cryptography, Public key Cryptanalysis, The RSA algorithm: Description of the Algorithm, Computational aspects, The Security of RSA.<br>Diffie-Hellman key exchange: The Algorithm, Key exchange Protocols, Man-in-the-middle Attack, Elliptic Curve Cryptography: Analog of Diffie-Hellman key Exchange, Elliptic Curve Encryption/Decryption, Security of Elliptic Curve Cryptography.<br><br>Chapter 8: 8.2 Chapter 9: 9.1, 9.2 Chapter 10: 10.1, 10.4 |
| | Module-3 10 hours |
| | Applications of Cryptographic Hash functions, Two simple Hash functions, Key management and distribution: Symmetric key distribution using symmetric encryption, Symmetric key distribution using asymmetric encryption, Distribution of public keys, X.509 Certificates, Public Key Infrastructures<br><br>Cha ter 11: 11.1, 11.2 Cha ter 14: 14.1, 14.2, 14.3, 14.4, 14.5 |
| | Module-4 10 hours |
| | User Authentication: Remote user authentication principles, Kerberos, Remote user authentication using asymmetric encryption.<br>Web security consideration, Transport layer security.<br>Email Threats and comprehensive email security, S/MIME, Pretty Good Privacy.<br>Chapter 15: 15.1, 15.3, 15.4 Chapter 17: 17.1, 17.2 Chapter 19: 19.3, 19.4, 19.5 |
| | Module-5 10 hours |
| | Domainkeys Identified Mail.<br>IP Security: IP Security overview, IP Security Policy, Encapsulating Security Payload, Combining security associations, Internet key exchange. Cha ter 19: 19.9 Cha ter20: 20.1, 20.2, 20.3, 20.4, 20.5 |

Course outcome

At the end of the course, the student will be able to :

COI: Explain the basic concepts of Cryptography and Security aspects

C02: Apply different Cryptographic Algorithms for different applications

C03: Analyze different methods for authentication and access control.

C04: Describe key management, key distribution and Certificates.

C05: Explain about Electronic mail and IP Security.

2

Il 3

Assessment Details (both CIE and SEE)

The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 40% of the maximum marks (20 marks out of 50) and for the SEE minimum passing mark is 35% of the maximum marks (18 out of 50 marks). A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures a minimum of 40% (40 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together.

Continuous Internal Evaluation:

For the Assignment component of the CIE, there are 25 marks and for the Internal Assessment Test component, there are 25 marks.

The first test will be administered after 40-50% of the syllabus has been covered, and the second test will be administered after 85-90% of the syllabus has been covered

Any two assignment methods mentioned in the 220B2.4, if an assignment is project-based then only one assignment for the course shall be planned. The teacher should not conduct two assignments at the end of the semester if two assignments are planned.

• For the course, CIE marks will be based on a scaled-down sum of two tests and other methods of assessment.

Internal Assessment Test question paper is designed to attain the different levels of Bloom's taxonomy as per the outcome defined for the course.

Semester-End Examination:

Theory SEE will be conducted by University as per the scheduled timetable, with common question papers for the course (duration 03 hours).

1. The question paper will have ten questions. Each question is set for 20 marks.
2. There will be 2 questions from each module. Each of the two questions under a module (with a maximum of 3 sub-questions), should have a mix of topics under that module.
3. The students have to answer 5 full questions, selecting one full question from each module.
4. Marks scored shall be proportionally reduced to 50 marks

Books

Text Books:

William stallings, 'Cryptography and Network Security", Pearson Publication, Seventh Edition.

References:

l. Keith M Martin, "Everyday Cryptography", Oxford University Press

2. V.K Pachghare,"Cryptography and Network Security", PHI, 2nd Edition

Activity Based Learning (Suggested Activities in Class)/ Practical Based learning

• Group assignment (TWO) to implement Cryptographic Algorithms (15 + 10 marks)