VII Semester

CRYPTOGRAPHY AND NETWORK SECURITY			
Course Code	21IS71	CIE Marks	50
Teaching Hours/Week (L:T:P: S)	3:0:0:0	SEE Marks	50
Total Hours of Pedagogy	40	Total Marks	100
Credits	03	Exam Hours	03

Course Learning Objectives:

CLO 1. To understand Cryptography, Network Security and its principles
CLO 2. To Analyse different Cryptography algorithms
CLO 3. To Illustrate Public and Private key cryptography
CLO 4. To Explain Key management, distribution and certification
CLO 5. To understand necessary Approaches and Techniques to build protection mechanisms in order to secure computer networks.

Teaching-Learning Process (General Instructions)

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

1. Lecturer method (L) needs not to be only 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 analyse information rather than simply recall it.
6. Introduce Topics in manifold representations.
7. Show the different ways to solve the same problem with different encryption techniques 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.

Module-1

Classical Encryption Techniques: Symmetric Cipher Model, Cryptography, Cryptanalysis and Brute-Force Attack, Substitution Techniques, Caesar Cipher, Monoalphabetic Cipher, Playfair Cipher, Hill Cipher, Polyalphabetic Cipher, One Time Pad.

Block Ciphers and the Data Encryption Standard: Traditional block Cipher structure, Stream Ciphers and Block Ciphers, Motivation for the Feistel Cipher structure, the Feistel Cipher, The data encryption standard, DES encryption, DES decryption, A DES example, results, the avalanche effect, the strength of DES, the use of 56-Bit Keys, the nature of the DES algorithm, timing attacks, Block cipher design principles, number of rounds, design of function F, key schedule algorithm

Textbook 1: Chapter 2, 3

Teaching-Learning Process	Chalk and board, Active Learning, Problem based learning

Module-2

Public-Key Cryptography and RSA: Principles of public-key cryptosystems. Public-key cryptosystems. Applications for public-key cryptosystems, requirements for public-key cryptosystems. public-key cryptanalysis. The RSA algorithm, description of the algorithm, computational aspects, the security of RSA.

Other Public-Key Cryptosystems: Diffie-Hellman key exchange, The algorithm, key exchange protocols, man in the middle attack, Elgamal Cryptographic systems.

Textbook 1: Chapter 9, 10

Teaching-Learning Process	Chalk and board, Active Learning, Demonstration

Module-3

Key Management and Distribution: Symmetric key distribution using Symmetric encryption, A key distribution scenario, Hierarchical key control, session key lifetime, a transparent key control scheme, Decentralized key control, controlling key usage, Symmetric key distribution using asymmetric encryption, simple secret key distribution, secret key distribution with confidentiality and authentication, A hybrid scheme, distribution of public keys, public announcement of public keys, publicly available directory, public key authority, public keys certificates.

Textbook 1: Chapter 14.1 – 14.3

Teaching-Learning Process	Chalk and board, Problem based learning, Demonstration

Module-4

X-509 certificates. Certificates, X-509 version 3

Public key infrastructure.

User Authentication: Remote user Authentication principles, Mutual Authentication, one-way authentication, remote user Authentication using Symmetric encryption, Mutual Authentication, one-way Authentication,

Kerberos, Motivation, Kerberos version 4, Kerberos version 5, Remote user Authentication using Asymmetric encryption, Mutual Authentication, one-way Authentication.

Textbook 1: Chapter 14.4 – 15.4

Teaching-Learning Process	Chalk& board, Problem based learning

Module-5

Electronic Mail Security: Pretty good privacy, S/MIME,

IP Security: IP Security overview, IP Security policy, Encapsulating Security payload, Combining security associations, Internet key exchange.

Textbook 1: Chapter 19.1, 19.2, 20.1 – 20.5

Teaching-Learning Process	Chalk and board, Problem based learning

Course Outcomes

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

CO 1. Understand Cryptography, Network Security theories, algorithms and systems
CO 2. Apply different Cryptography and Network Security operations on different applications
CO 3. Analyse different methods for authentication and access control
CO 4. Evaluate Public and Private key, Key management, distribution and certification
CO 5. Design necessary techniques to build protection mechanisms to secure computer networks

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). A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures not less than 35% (18 Marks out of 50) in the semester-end examination (SEE), and 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:

Three Unit Tests each of **20 Marks (duration 01 hour**)

1. First test at the end of 5th week of the semester
2. Second test at the end of the 10th week of the semester
3. Third test at the end of the 15th week of the semester

Two assignments each of **10 Marks**

4. First assignment at the end of 4th week of the semester
5. Second assignment at the end of 9th week of the semester

Group discussion/Seminar/quiz any one of three suitably planned to attain the COs and POs for **20 Marks** (**duration 01 hours**)

6. At the end of the 13th week of the semester

The sum of three tests, two assignments, and quiz/seminar/group discussion will be out of 100 marks and will be **scaled down to 50 marks**

(to have less stressed CIE, the portion of the syllabus should not be common /repeated for any of the methods of the CIE. Each method of CIE should have a different syllabus portion of the course).

CIE methods /question paper has to be 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 subject (**duration 03 hours)**

1. The question paper will have ten questions. Each question is set for 20 marks. Marks scored shall be proportionally reduced to 50 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.

The students have to answer 5 full questions, selecting one full question from each module

Suggested Learning Resources:

Textbooks

1. William Stallings: Cryptography and Network Security, Pearson 6th edition.

Reference:

1. V. K Pachghare: Cryptography and Information Security, PHI 2nd Edition
2. BehrouzA.Foruzan, Cryptography and Network Security, Tata McGraw Hill 2007.

Web links and Video Lectures (e-Resources):

- https://nptel.ac.in/courses/106105031
- https://onlinecourses.nptel.ac.in/noc21_cs16
- https://www.digimat.in/nptel/courses/video/106105031
- https://www.youtube.com/watch?v=DEqjC0G5KwU
- https://www.youtube.com/watch?v=FqQ7TWvOaus
- https://www.youtube.com/watch?v=PHsa_Ddgx6w

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

Project based learning:

- Implement classical, symmetric and asymmetric algorithms in any preferred language
- Evaluate network security protocol using any simulator available
- Conduct a comprehensive literature survey on the protocols and algorithms
- Identify the security threats and models of security threats
- Implement factorization algorithms and evaluate their complexity, identify a technologies to factorize a large prime number.