ATME College of Engineering

DEPARTMENT OF CSE-CYBER SECURITY

COURSE MODULE OF THE SUBJECT TAUGHT FOR THE SESSION 2025-26 - (EVEN SEM)

Course Syllabus with CO's

Faculty Name: Mrs. Suhasini			**Academic Year: 2025 - 2026**				
Department: Computer Science & Engineering - Cyber Security							
Course Code	**Course Title**	**Core / Elective**	**Prerequisite**	**Contact Hours**			**Total Hrs/ Sessions**
				L	**T**	**P**	
BCY602	Cryptography and Network Security	Core	Computer Networks, Mathematical Foundations	4	0	0	50T
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.						
Topics Covered as per Syllabus							
Module-1							
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. **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.							
Module-2							
Pseudorandom number Generators Linear Congruential Generators, Blum Blum Shub Generator. **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. **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.							
Module-3							
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.							
Module-4							

User Authentication: Remote user authentication principles**,** Kerberos**,** Remote user authentication using asymmetric encryption.
Web security consideration, Transport layer security.
Email Threats and comprehensive email security, S/MIME, Pretty Good Privacy.

Module-5

Domain keys Identified Mail.
IP Security
IP Security overview, IP Security Policy, Encapsulating Security Payload, Combining security associations, Internet key exchange.

Textbooks:

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

Reference Books

1. Keith M Martin, "Everyday Cryptography", Oxford University Press.
2. V.K Pachghare,"Cryptography and Network Security", PHI, 2nd Edition.

Course outcomes: The students should be able to:

- Understand the basic concepts of Cryptography and Security aspects
- Apply different Cryptographic Algorithms for different applications
- Analyze different methods for authentication and access control.
- Explain key management, key distribution and Certificates.
- Explain Electronic mail and IP Security.

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 22OB2.4, 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.

Subject Code:	BCY602	TITLE: Cryptography and Network Security						Faculty Name:	Ms. Suhasini			
List of Course Outcomes	Program Outcomes											Total
	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	
CO-1	3	2	-	-	-	-	-	-	-	-	-	-	5
CO-2	3	2	3	-	-	-	-	-	-	-	-	-	8
CO-3	-	3	2	-	-	-	-	-	-	-	-	-	5
CO-4	3	2	3	-	-	-	-	-	-	-	-	-	8
CO-5	3	2	2	-	-	-	-	-	-	-	-	-	7
Total	12	11	10	-	-	-	-	-	-	-	-	-	33

Note: 3 = Strong Contribution, 2 = Average Contribution, 1 = Weak Contribution, - = No Contribution

ATME College of Engineering

DEPARTMENT OF CSE-CYBER SECURITY

The Correlation of Course Outcomes (CO's) and Program Specific Outcomes (PSO's)

Subject Code:	BCY602	TITLE: Cryptography and Network Security	Faculty Name:	Ms. Suhasini

List of Course Outcomes	Program Specific Outcomes		Total
	PSO-1	PSO-2	
CO-1	-	-	-
CO-2	-	-	-
CO-3	-	-	-
CO-4	-	-	-
Total	-	-	-