Gyanmanjari Innovative University

Course Syllabus
Gyanmanjari Institute of Technology
Semester-6 (B.Tech.)

Subject: Cryptography and Network Security-BETIT16326

Type of course: Professional Core

Prerequisite: Basic knowledge of computer science, programming, and computer networks.

Rationale:

Cryptography and Network Security (CNS) is essential for understanding how to protect data and communication across networks. This subject covers the principles, algorithms, and protocols used to ensure confidentiality, integrity, authentication, and availability of information. Proficiency in CNS is vital for designing secure systems, defending against cyber threats, and implementing effective security measures in modern computing and networking environments.

Teaching and Examination Scheme:

Teaching Scheme			Credits	Examination Marks					Total Marks
				Theory Marks		Practical Marks		CA	
CI	T	P	C	ESE	MSE	V	P	ALA	
4	0	2	5	60	30	10	20	30	150

Legends: CI-Classroom Instructions; T – Tutorial; P - Practical; C – Credit; ESE - End Semester Examination; MSE- Mid Semester Examination; V – Viva; CA - Continuous Assessment; ALA- Active Learning Activities.

Course Content:

Sr. No	Course content	Hrs.	% Weightage
1	**Introduction to Cryptography and Security Fundamentals:** Introduction to Cryptography, Need for Cryptography in Modern System, Uses of Cryptography, Security Goals, Types of Attacks: Passive Attacks and Active Attacks, Future Goals of Cryptography, Classical Cryptography: Substitution Techniques & Transposition Techniques Cipher.	12	20%
2	**Foundations of Symmetric Cryptography:** Greatest Common Divisor (GCD), Types of Cryptographic algorithms: Symmetric and Asymmetric, 1.Symmetric Key Cryptography: Principles of Symmetric Key Cryptography, Block Cipher, Stream Cipher, Data Encryption Standard(DES) and Triple DES, Advance Encryption Standard (AES), Block Cipher Mode: (ECB,CBC,CFB,OFB,CTR).	12	20%
3	**Foundations of Asymmetric Key Cryptography:** Concept of Public-Key Cryptography, RSA Algorithm: Working, Key Generation, and Applications, Diffie-Hellman Key Exchange Protocol, Elliptic Curve Cryptography (ECC) and Its Advantages, Key Management and Distribution.	12	20%
4	**Classic Digital Signature Schemes:** Digital Signature Fundamentals and Security Requirements, The Role of Hash Function and Non-repudiation, The Elgamal Digital Signature Scheme, The Schnorr Digital Signature Scheme, The NIST Digital Signature Algorithm (DSA), Digital Signature Schemes: Comparative Analysis and Security.	12	20%
5	**Modern Security: Hashing, MACs, and Cyber Defense:** Cryptography Hash Functions, Their Application, Simple Hash Function, Its Requirements and Security, Hash Function Based on Cipher Block Chaining, Secure Hash Algorithm (SHA), Message Authentication Codes, Its Requirements and Security, MACs Based on Hash Functions, Macs based on Block Cipher, Network Security Fundamentals, Types of Cyber Attacks, Firewalls and Intrusion Detection Systems (IDP/IPS), Secure Communication Protocols, Cybersecurity Principles and Risk Management, Secure Communication Protocols, Cybersecurity Principles and Risk Management, Case Studies of Security Breaches.	12	20%

Continuous Assessment:

Sr. No	Active Learning Activities	Marks
1	**Digital Signature Verifier:** In this activity, each student will implement a Digital Signature System using Python or Java to understand the working of public-key cryptography. They will generate a key pair, sign a message using the private key, and verify the signature using the public key. The implementation must include hashing (e.g., SHA-256) to ensure message integrity. Students will submit the source code and a screenshot showing successful signing and upload it on GMIU portal.	10
2	**SHA Integrity Analyzer:** In this activity, each student will write a program to implement and compare different Secure Hash Algorithms (SHA-1, SHA-256, and SHA-512). They will demonstrate how even a small change in input causes a large change in the hash output (avalanche effect). Students will document their observations, explain the importance of hashing in digital signatures, and upload their source code and upload it on GMIU portal.	10
3	**MAC-Based Message Authentication:** In this activity, each student will design and simulate a Message Authentication Code (MAC) mechanism using HMAC in Python. They will create sender and receiver scripts where the sender generates a MAC for a message and the receiver verifies it using a shared secret key. Students will demonstrate how MAC ensures data integrity and authentication. The final report with source code, execution screenshots, and analysis and upload it on GMIU portal.	10
	Total	30

Suggested Specification table with Marks (Theory):60

Distribution of Theory Marks (Revised Bloom's Taxonomy)						
Level	**Remembrance (R)**	**Understanding (U)**	**Application (A)**	**Analyze (N)**	**Evaluate (E)**	**Create (C)**
Weightage %	20%	30%	15%	15%	10%	10%

Note: This specification table shall he treated as a general guideline for students and teachers. The actual distribution of marks in the question paper may vary slighily from above table.

Course Outcome:

After learning the course, the students should be able to:	
CO1	Understand cryptography basics, security goals, attacks, and classical ciphers.
CO2	Apply symmetric encryption algorithms and block cipher modes.
CO3	Use asymmetric key techniques like RSA, Diffie–Hellman, and ECC.
CO4	Analyze various digital signature schemes and their security.
CO5	Evaluate hash functions, MACs, and core network security mechanisms.

List of Practical:

Sr. No	Description	Unit No	Hrs.
1	Write a program and perform Caesar Cipher algorithm in Crypt Tool.	01	01
2	Write a program and perform Mono alphabetic Cipher Algorithm in Crypt Tool.	01	02
3	Write a program and perform Poly alphabetic Cipher Algorithm in Crypt Tool.	01	02
4	Write a program and perform Play Fair algorithm in Crypt Tool.	01	02
5	Write a program and perform Hill Cipher algorithm in Crypt Tool.	01	02
6	Write a program and perform Rail Fence algorithm in Crypt Tool.	01	01
7	Write a program and perform One Time Pad algorithm in Crypt Tool.	01	01
8	Write a program and perform Data Encryption Standard (DES) algorithm in Crypt Tool.	02	02
9	Write a program and perform Advance Encryption Standard (AES) algorithm in Crypt Tool.	02	02
10	Write a program and perform Triple - Data Encryption Standard (3-DES) algorithm in Crypt Tool.	02	02
11	Write a program and perform RSA algorithm in Crypt Tool.	03	01
12	Write a program and perform SHA - 1 algorithm in Crypt Tool.	05	02
13	Write a program and perform SHA - 256 algorithm in Crypt Tool.	05	02
14	Write a program and perform SHA - 512 algorithm in Crypt Tool.	05	02
15	Write a program and perform MD5 algorithm in Crypt Tool.	05	02
16	Write a program and perform MAC algorithm in Crypt Tool.	05	02
17	Write a program and perform HMAC algorithm in Crypt Tool.	05	02
		Total	30

Instructional Method:

The course delivery method will depend upon the requirement of content and need of students. The teacher in addition to conventional teaching method by black board, may also use any of tools such as demonstration, role play, Quiz, brainstorming, MOOCs etc.

From the content 10% topics are suggested for flipped mode instruction.

Students will use supplementary resources such as online videos, NPTEL/SWAYAM videos, e-courses, Virtual Laboratory.

The internal evaluation will be done on the basis of Active Learning Assignment.

Practical/Viva examination will be conducted at the end of semester for evaluation of performance of students in laboratory.

Reference Books:

[1] William Stallings – Cryptography and Network Security: Principles and Practice – Pearson, 7th Edition, 2017.
[2] Mark Stamp – Information Security: Principles and Practice – Wiley India Edition, 3rd Edition, 2019.
[3] Behrouz A. Forouzan, Debdeep Mukhopadhyay – Cryptography & Network Security – McGraw Hill, 3rd Edition, 2015.
[4] Atul Kahate – Cryptography and Network Security – Tata McGraw-Hill (TMH), 3rd Edition, 2013.
[5] Charles J. Brooks – Cybersecurity Essentials – Pearson, 1st Edition, 2018.