CVM UNIVERSITY
Aegis: Charutar Vidya Mandal (Estd.1945)

FACULTY OF ENGINEERING & TECHNOLOGY

Effective from Academic Batch: 2020-21

Programme: **Bachelor of Engineering (Information Technology)**

Semester: **VI**

Course Code: **102046708**

Course Title: **Information and Network Security**

Course Group: **Professional Core Course**

Course Objectives: The objective of this course is to teach the concepts of securing computer networks, with emphasize on principles and practices of information and network security. The subject covers various important topics concerning information security like symmetric and asymmetric cryptography, hashing, message and user authentication, digital signatures, key distribution with the overview of the network security.

Teaching & Examination Scheme:

Contact hours per week			Course Credits	Examination Marks (Maximum / Passing)				
				Theory		J/V/P*		Total
Lecture	Tutorial	Practical		Internal	External	Internal	External	
3	0	2	4	40 / 14	60 / 21	20 / 7	30 / 10	150 / 52

* **J**: Jury; **V**: Viva; **P**: Practical

Detailed Syllabus:

Sr.	Contents	Hours
1	Need of Security, Computer Security Concepts, Security Attacks, Security Services, Security Mechanisms, A Model for Network Security, Symmetric Cipher Model, Substitution Techniques, Transposition Techniques.	05
2	Block Cipher Principles, The Data Encryption Standard (DES), A DES Example, The Strength of DES, Block Cipher Design Principles, Stream Ciphers, RC4, Advanced Encryption Standard (AES) with Structure, Transformation Functions, Key Expansion, Example, and Implementation, Block Cipher Modes of Operation, Key Management and Distribution for Symmetric Encryption.	12
3	Introduction to Number Theory, Principles of Public-Key Cryptosystems, RSA Algorithm, it's computational aspects and security, Diffie-Hellman Key Exchange, Man-in-Middle attack, Key Management and Distribution for Asymmetric Encryption.	07

4	Authentication Requirements, Application of Cryptographic Hash Function, Requirements and Security of Hash Function, Secure Hash Algorithm (SHA), Message Authentication Codes, Message Authentication Functions, Requirements and Security of MACs, MACs based on Hash Functions.	**06**
5	Digital Signature, Its Properties, Requirements and Security, Various Digital Signature Schemes (ElGamal and Schnorr), Remote User-Authentication Principles, Remote User-Authentication with Symmetric and Asymmetric Encryption	**05**
6	Web Security Threats and Approaches, SSL Architecture and Protocol, Transport Layer Security, HTTPS and SSH.	**05**
	Total	**40**

List of Practicals / Tutorials:

1	To implement Caesar cipher encryption-decryption.
2	To implement Monoalphabetic cipher encryption-decryption.
3	To implement Playfair cipher encryption-decryption.
4	To implement Polyalphabetic cipher encryption-decryption.
5	To implement Hill cipher encryption-decryption.
6	To implement Rail Fence and Columnar transposition cipher encryption-decryption.
7	To implement Simplified Data Encryption Standard.
8	To implement Diffi-Hellman Key Exchange method.
9	To implement RSA encryption-decryption algorithm.
10	Demonstrate and perform various encryption-decryption techniques with cryptool.
11	Study and use open-source packet analyzer-Wireshark to understand security mechanism of various network protocols.
12	Detail Case study: Real world implementation of Network Security Algorithm/Concept.

Reference Books:

1	William Stallings, "Cryptography and Network Security, Principles and Practice", Pearson Education, India
2	Atul Kahate, "Cryptography and Network Security", Tata Mc Grawhill, India
3	Forouzan, "Cryptography & Network Security", PHI
4	Mark Stamp, "Information Security Principles and Practice", Willy India Edition
5	N Harini, T R Padmanabhan, C K Shyamala, "Cryptography and Security", Wiley-India

Supplementary learning material:	
1	NPTEL Videos and PDF - "Cryptography and Network Security by Debdeep Mukhopadhyay, IIT Kharagpur"- https://nptel.ac.in/courses/106105031/
2	Videos - "Computer Systems Security by Nickolai Zeldovich & James Mickens, MIT" – https://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-858-computer-systems-security-fall-2014/index.htm
3	"Network and Computer Security by Prof Ronald Rivest, MIT" - https://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-857-network-and-computer-security-spring-2014/index.htm
4	Vlabs, "Cryptography Lab" - http://cse29-iiith.vlabs.ac.in/

5	Cryptool - https://www.cryptool.org/en/
6	Wireshark - https://www.wireshark.org/download.html

Pedagogy:

- Direct classroom teaching
- Audio Visual presentations/demonstrations
- Assignments/Quiz
- Continuous assessment
- Interactive methods
- Seminar/Poster Presentation
- Industrial/ Field visits
- Course Projects

Suggested Specification table with Marks (Theory) (Revised Bloom's Taxonomy):

Distribution of Theory Marks in %						**R**: Remembering; **U**: Understanding; **A**: Applying; **N**: Analyzing; **E**: Evaluating; **C**: Creating
R	**U**	**A**	**N**	**E**	**C**	
20%	25%	25%	10%	10%	10%	

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

Course Outcomes (CO):

Sr.	Course Outcome Statements	%weightage
CO-1	Develop concept of security needed in communication of data through computers and networks along with various possible attacks.	**20**
CO-2	Understand various encryption mechanisms for secure transmission of data and management of key required for encryption.	**40**
CO-3	Understand authentication requirements and study various authentication mechanisms.	**25**
CO-4	Understand network security concepts and study different web security mechanisms.	**15**

Curriculum Revision:	
Version:	1.0
Drafted on (Month-Year):	June-2020
Last Reviewed on (Month-Year):	-
Next Review on (Month-Year):	June-2025