SARVAJANIK UNIVERSITY
Sarvajanik College of Engineering and Technology
Bachelor of Technology

Year: B. Tech III (Semester V)

Subject Name: Cryptography and Network Security **Subject Code:**BTIT13502
Type of course: Professional Core Course
Prerequisite: Discrete Mathematics

Rationale: The subject covers various important topics concerning information security like symmetric and asymmetric cryptography, hashing, message and user authentication, digital signatures, key distribution and overview of the malware technologies.

Teaching and Examination Scheme:

Teaching Scheme				Theory Marks			Practical Marks		Total
L	T	P	C	TEE	CA1	CA2	TEP	CA3	
3	0	2	4	60	25	15	30	20	150

CA1: Continuous Assessment (assignments / projects / open book tests / closed book tests) CA2: Sincerity in attending classes / class tests / timely submissions of assignments / self-learning attitude / solving advanced problems TEE: Term End Examination TEP: Term End Practical Exam (Performance and viva on practical skills learned in course) CA3: Regular submission of Lab work / Quality of work submitted / Active participation in lab sessions / viva on practical skills learned in course.

Contents:

Sr. No.	Contents	Total Hrs
1.	**Introduction :** Computer Security Concepts, Security attacks, security services, security mechanisms, A Model for Network Security	02
2.	**Classical Encryption Techniques :** Symmetric Cipher Model – Cryptography Cryptanalysis and Brute-Force Attack, Substitution Techniques - Caesar Cipher, Monoalphabetic Ciphers, Playfair Cipher, Hill Cipher, Polyalphabetic Ciphers, One-Time Pad, Transposition Techniques, Rotor Machines, Steganography	07
3.	**Number Theory and Finite Fields :** Divisibility and the Division Algorithm, The Euclidean Algorithm, Modular Arithmetic, Prime Numbers, Fermat's and Euler's Theorems, Testing for Primality, The Chinese Remainder Theorem, Discrete Logarithms. Groups, Rings, Fields, Finite Fields of the Form GF(p), Polynomial Arithmetic, Finite Fields of the Form GF(2n)	07
4.	**Block Ciphers and the Data Encryption Standard :** Traditional Block Cipher Structure, The Data Encryption Standard, strength of DES, Multiple encryption and triple DES, Design principles of block cipher	04

5.	**Advanced Encryption Standard :** Finite Field Arithmetic, AES Structure, AES Transformation Functions, AES Key Expansion, An AES Example	**04**
6.	**Block Cipher Operation :** Electronic Codebook, Cipher Block Chaining Mode, Cipher Feedback Mode, Output Feedback Mode, Counter Mode	**02**
7.	**Public-Key Cryptography and RSA:** Principles of Public-Key Cryptosystems, The RSA Algorithm, Diffie-Hellman Key Exchange, Elgamal Cryptographic System, Man-in-Middle attack	**05**
8.	**Cryptographic Hash Functions :** Applications of Cryptographic Hash Functions, Two Simple Hash Functions, Requirements and Security, Hash Functions Based on Cipher Block Chaining, Secure Hash Algorithm (SHA)	**03**
9.	**Message Authentication Codes :** Message Authentication Requirements, Message Authentication Functions, Requirements for Message Authentication Codes, Security of MACs, MACs Based on Hash Functions: HMAC, MACs Based on Block Ciphers: DAA and CMAC	**03**
10.	**Digital Signatures :** Elgamal Digital Signature Scheme, Schnorr Digital Signature Scheme, NIST Digital Signature Algorithm	**03**
11.	**Key Management, Distribution and User Authentication :** Symmetric Key Distribution Using Symmetric Encryption, Symmetric Key Distribution Using Asymmetric Encryption, Distribution of Public Keys, X.509 Certificates, Kerberos	**03**
12.	**Web Security:** Web Security Considerations, Transport Layer Security, HTTPS, Secure Shell (SSH)	**02**

Suggested Specification table with Marks (Theory): (For B. Tech only)

Distribution of Theory Marks					
R Level	**U Level**	**A Level**	**N Level**	**E Level**	**C Level**
15	25	10	10	-	-

Legends: R: Remembrance; U: Understanding; A: Application, N: Analyze and E: Evaluate C: Create (Revised Bloom's Taxonomy)

Reference Books:

Sr no	Title of book /article	Author(s)	Publisher and details like ISBN
1	Cryptography and Network Security: Principles and Practice	Stallings, William	Pearson
2	Cryptography: theory and practice	Stinson, Douglas R.	Chapman and Hall/CRC
3	Cryptography & network security	Forouzan, Behrouz A.	McGraw-Hill
4	Applied cryptography: protocols, algorithms, and source code in C	Schneier, Bruce	John wiley & sons
5	Information Security Principles and Practice	Mark Stamp	Willy India Edition
6	Security in Computing	Pfleeger and Pfleeger	PHI

Note: Students should refer to the latest editions of books

Course Outcomes (CO):

Sr. No.	CO statements	Marks % weightage
1.	Understand the concepts related to security attacks, security services, security mechanisms.	5%
2.	Explainthe concepts of Number theory and Finite fields and apply them in appropriate scenario.	15%
3.	Analyse the security schemes of Symmetric Key Cryptography and Asymmetric Key Cryptography for their use in different application scenarios.	45%
4.	Describe and discuss hashing algorithms, Message Authentication Code (MAC), Digital Signature Algorithms, key generation and key managementand Web Security considerations.	35%

List of Open learning website:

- Cryptography and Network Security available at - https://onlinecourses.nptel.ac.in/noc20_cs21/preview
- http://www.cryptix.org/
- http://www.cryptocd.org/
- http://www.cryptopp.com/

List of Experiments:

1 Implement Ceasar and Hill cipher. Both are substitution cipher. Analyze the strength of the cipher in terms of brute force attack and cryptanalysis attack. Suggest one way to improve and strengthen the cipher and analyze with respect to cryptanalysis attack.
Ceasar cipher -
Your plaintext is Hello, Welcome. The key used is 3. How Ceaser cipher will work?
Test case :
A B C
D E F
Hill Cipher -

$$\text{Key K} = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$$

Plaintext = pay
Ciphertext = RRL

2 Implement rail Fence and transposition cipher. Both are permutation cipher. Analyze the strength of the cipher in terms of cryptanalysis.
Rail fence.
Test case : Meetme
Ciphertext : MEMETE
Transposition
Key : 4312567
Plaintext: attackpostponeduntiltwoam
Ciphertext: TTNAAPTMTSUOAODWCOIXKNLYPETZ

3 Implement Playfair Cipher. The plaintext is paired in two characters. Discuss the advantage of polyalphabetic cipher over monoalphabetic cipher.
Key = MONARCHY
Plaintext = ar mu hsea Ciphertext = RM CM BP IM

4 Write a program to implement Vigenere Cipher.

5 Write a program to implement Vernam Cipher.

6 Implement Euclid algorithm to find GCD.
GCD(16,12) = 4
GCD(12,4) = 0
Then 4 is the GCD(16,12)

7 Implement Euler's totientfunction $\phi(n)$. It is defined as the number of positive integers less than n and relatively prime to n. Find $\phi(35)$

and $\phi(37)$. Observe the value and analyze the behavior of totient function.

8 Implement extended Euclidean Algorithm for finding inverse.

9 Implement encryption and decryption using Simplified-DES scheme.

10 Implement encryption and decryption using AES scheme.

11 Implement RSA algorithm.
Take two prime numbers p, q and find n=p x q
Initially take encryption key such that it is relatively prime with ϕ(n).
Find out decryption key.
Take plaintext message M, Ciphertext C=Me mod n.
To get plaintect from ciphertext M=Cd mod n.
Test case :
Two prime numbers 17,11
Encryption key = 7, Decryption key = 23, M=88, C=11

12 Implement Diffie-Hellman Key Exchange algorithm.

13 Write a program to implement Digital Signature Algorithms: DSA.

14 Write a program to implement Digital Signature Algorithms: Elgamal.