SARVAJANIK UNIVERSITY
Sarvajanik College of Engineering and Technology
Bachelor of Technology

B. Tech. Semester VI

Subject Name: **Cryptography and Network Security** **Subject Code: BTEC14617**
Type of course: PEC
Prerequisite: Computer Networking, Mathematical concepts: Random numbers, Number theory
Rationale: Cryptography and Network Security covers various important topics related to information security like symmetric and asymmetric cryptography, hashing, digital signatures, key distribution and overview of the malware technologies. It also covers the Network security aspects like user authentication, network access control, web and wireless security.

Teaching and Examination Scheme:

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

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

Content:

Sr. no.	Topics	Teaching Hrs.	Module Weightage
1.	**Cryptography and Network Security Concepts** Cryptography basics: Ciphering and it's types Security concepts: Security attacks, Security services, Security mechanism, Security design principals	3	5
2.	**Symmetric Ciphers** Symmetric cipher model, Substitution and Transposition technique DES-Data Encryption Standards, DES avalanche effect, DES strength AES-Advanced Encryption Standards, AES structure, AES key expansion Block cipher Block cipher design principles and operation, Multiple encryption and triple DES, Electronic Code Book, Cipher Block Chaining Mode, Cipher Feedback mode, Output Feedback mode, Counter mode	15	35
3.	**Asymmetric Ciphers** Principles of public key cryptosystems, RSA algorithm, Diffie-Hallman key exchange, Elgamal Cryptographic systems, Pseudorandom number generation based on asymmetric cipher	7	15
4.	**Cryptographic Data Integrity Algorithms**	10	20

	Hash function, Two simple hash function, Hash functions based on cipher block chaining, SHA-Secure Hash Algorithm, MAC-Message Authentication Code-it's requirement-function-security, MCAs based on hash function, MCAs based block ciphers-DAA and CMAC, Digital signature, Elgamal and Schnorr digital signature schemes		
5.	**User Authentication** Principles, Remote user authentication with symmetric and asymmetric encryption, Kerberos	2	5
6.	**Network Security** Network access control, Extensible authentication protocol, Web security consideration, Transport layer security, HTTPS, SSH-Secure shell, Wireless security, IP security-IPsec, IPsec applications, IPsec services, Transport and tunnel model	8	20

Suggested Specification table with Marks (Theory/Practical):

% Distribution of Marks					
R Level	**U Level**	**A Level**	**N Level**	**E Level**	**C Level**
5	40	20	20	5	10

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

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.

Reference Text Books:

Sr. No.	Title of book /article	Author(s)	Publisher and details like ISBN	Year of publication	Publication Edition
1.	Cryptography And Network Security, Principles And Practice	William Stallings	Pearson	2018	Latest
2.	Information Security Principles and Practice	Mark Stamp	Willy India Edition	2018	Latest
3.	Cryptography & Network Security	Forouzan, Mukhopadhyay	McGrawHill	2018	Latest
4.	Cryptography and Network Security	Atul Kahate	TMH	2018	Latest

5.	Cryptography and Security	C K Shyamala, N Harini, T R Padmanabhan	Wiley-India	2018	Latest

Course Outcome:

Sr. No.	CO Statement After learning this subject students will be able to,	Marks % weightage
CO-1	Compare, contrast and use the principles of various cryptography algorithms.	10
CO-2	Select and compile various symmetric key and asymmetric key algorithms.	30
CO-3	Detect integrity of messages using various cryptographic data integrity algorithms.	30
CO-4	Select various user authentication mechanisms.	10
CO-5	Apply and Integrate the concepts of Information security for network security.	20

Mapping with POs:

	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO 2	PSO 3
CO-1	3	2	3	1	3	2	1	2	2	3	2	3	-	-	-
CO-2	3	2	3	1	3	-	-	-	-	2	1	3	-	3	-
CO-3	3	3	3	3	3	3	2	3	3	3	1	3	-	2	3
CO-4	3	2	2	3	3	3	-	3	3	3	3	3	-	-	-
CO-5	3	3	2	3	2	3	2	2	2	3	2	3	-	3	-

List of practical:

1 Write a program to implement Caesar cipher.
2 Write a program to implement a Monoalphabetic cipher.
3 Write a program to implement Hill Cipher.
4 Write a program to implement the Columnar transposition cipher.
5 Write a program to implement the Vigenere Cipher.
6 Write a program to implement Vernam cipher.
7 Write a program to implement DES Cipher.
8 Write a program to implement the RSA Cryptosystem.
9 Write a program to implement a Diffie-Hellman key exchange algorithm.
10 Write a program that creates a shortcut of a file. (Virus program)
11 Write a program that increases file size by 10.

List of Open Source/learning websites:

- http://www.cryptix.org/
- http://www.cryptocd.org/
- http://www.cryptopp.com/

List of Open Source software:

- Cryptool (www.cryptool.org)