BVM ENGINEERING COLLEGE [AN AUTONOMOUS INSTITUTION]

5CP48: CRYPTOGRAPHY AND INFORMATION SECURITY
CREDITS – 4 (LTP:3,0,1)

Course Objective:
To impart knowledge of mathematics behind cryptography, various algorithms, cyber security, malwares-viruses and quantum cryptography.

Teaching and Evaluation Scheme:

Teaching Scheme (Hours per week)			Credits	Assessment Scheme				Total Marks
				Theory Marks		Practical Marks		
L	T	P	C	ESE	CE	ESE	CE	
3	0	2	4	60	40	20	30	150

Course Contents:

Unit No.	Topics	Teaching Hours
1	**Mathematical Foundation:** Modular Arithmetic; Matrices; Linear Congruence; Prime Numbers; Fermat's and Euler's theorem; Primality test; factorization; Chinese reminder; Discrete Logarithms; Quadratic Congruence; Congruence Calculus or Modular Arithmetic; Basic Arithmetic Operations for Large Integers (Addition, subtraction, Multiplication, Division, Powers, Integral root, Generating a random integer); Factorization of Integers; Modular Square Root	06
2	**Cryptography:** Introduction; Symmetric Key Cipher; Classical Encryption Techniques (Substitution, Transposition, Steganography); Block Ciphers and Its principals; DES; AES; RC4; Asymmetric key Ciphers; Principles of Asymmetric ciphers; RSA; Key Management; Introduction of Hash and MAC.	12
3	**Transferring Secret Information :** Sharing Secrets; Shamir's Secret Sharing Scheme; Oblivious Data Transfer; Zero-Knowledge Proofs; Enforcing honest behavior using Zero Knowledge Proofs; Proofs of knowledge; Multi-party computation.	08
4	**Malware and Virology:** Description of the System; Users; Trust and Trusted Systems; Buffer Overflow and Malicious Software; Malware; spyware; adware; key-loggers; Metamorphic malwares; Hunting for metamorphic; Computer Virus-Antivirus Coevolution; Tracking Botnets, Honeynet; Software security and obfuscation	08
5	**Cyber Security:** Cyber Security Fundamentals; Cyber Security Risk and Threat Management; How to measure cybersecurity? Metric in practice; Cyber Security Laws; Regulations and Ethics; Cyber Laws and Cyber Acts (IT Act 2000)	05

Unit No.	Topics	Teaching Hours
6	**Quantum Cryptography:** Lattice in Cryptography; Quantum Bit; Quantum Registers and Quantum Algorithms; Shor's Algorithm; Grover's Search Algorithm; No-Cloning Theorem; Quantum Key-Exchange	07
	Total	45

List of References:

1. Behrouz A. Forouzan , "*Cryptography & Network Security*", McGraw-Hill
2. William Stalling , "*Cryptography and Network Security: Principles and Practice*", Pearson Education
3. Deven Shah, "*Mark Stamp's Information Security: Principles and Practice*", Wiley India
4. Pfleeger and Pfleeger, "*Security in Computing*" , Prentice Hall