2CE603/2IT603: INFORMATION SYSTEM SECURITY

2nd Internal Syllabus (December-2019 to May-2020)

SR.NO.	DESCRIPTION
1.	**BASICS OF ENCRYPTION AND DECRYPTION**
	1. Symmetric key and Key Distribution Problem. 2. Key range and Key Size. 3. Diffie-Hellman Key Exchange/Key Agreement Algorithm. 4. Man in the Middle Attack
2.	**SYMMETRIC KEY OPERATION**
	1. Stream Cipher and Block Cipher 2. Claude Shannon's concept of Confusion & Diffusion 3. Algorithm types 4. Algorithm modes: ECB, CBC, CFG, OFB, CTR 5. Feistal Cipher Structure 6. Data Encryption Standards (DES) 7. DES Analysis, Double DES and Triple DES with two and three keys 8. Meet-in-the-middle attack in double DES
3.	**NUMBER THEORY**
	1. Euler's Totient or Phi Function 2. Chinese Remainder Theorem 3. Primality Test: (Fermat's Little Theorem, Square Root Test, Miller-Rabin Test)
4.	**SYMMETRIC AND ASYMMETRIC KEY BOTH TOGETHER**
	1. Digital Envelope 2. Digital Signature, RSA & Digital Signature 3. Message Digest (MD) 4. Message Authentication Code (MAC)
5.	**PUBLIC KEY CRYPTOGRAPHY**
	1. Merkle-Hellman Knapsack Cryptosystem 2. RSA Cryptosystem 3. RSA Attacks (Factorization attack, Chosen Cipher attack) 4. Rabin Cryptosystem
6.	**FIREWALLS**
	1. Types of Firewalls – Packet filters & Application Gateways 2. Network Address Translation (NAT) 3. Demilitarized Zone (DMZ) Networks
7.	**SECURE SOCKET LAYER (SSL)**
	1. How SSL Works? 2. Handshake Protocol, Record Protocol, Alert Protocol

Reference Book: "Cryptography and Network Security" by Atul Kahate
"Cryptography and Network Security" by William stallings
"Cryptography and Network Security" by Forouzan

Prof. Paresh M. Solanki (Computer Engineering)
Prof. Menka N. Patel (Computer Engineering)
Prof. Sweta A. Dargad (Computer Engineering)