IT9122 APPLIED CRYPTOGRAPHY 3 0 0 3

UNIT I **9**

Classical Cryptography-The Shift Cipher,The Substitution Cipher,The Affine Cipher Cryptanalysis-Cryptanalysis of the Affine Cipher,Cryptanalysis of the Substitution Cipher,Cryptanalysis of the Vigenere Cipher,Shannon's Theory.

UNIT II **9**

Block Cipher and the Advanced Encryption Standard-Substitution -Permutation Netrworks, Linear Cryptanalysis, Differential Cryptoanalysis , The Data Encryption Standard, The Advanced Encryption Standard, Modes of Operation ,Cryptography Hash Function- Hash Function and Data Integrity,Security of Hash Function ,Iterated Hash Functions, Message Authentication Codes.

UNIT III **9**

The RSA Cryptosystem and Factorin Integer- Intoduction to Public –key Cryptography, Number theory,The RSA Cryptosystem ,Other Attacks on RSA,The ELGamal Cryptosystem,Shanks' Algorithm,Finit Fields,Elliptic Curves over the Reals, Elliptical Curves Modulo a Prime,Signature Scheme –Digital Signature Algorithm.

UNIT IV **9**

Identification Scheme and Entity Attenuation-Challenge – and – Response in the Secret-key Setting,Challenge – and – Response in the Public key Setting,The Schnorr Identificataon Scheme,Key distribution-Diffie-Hellman Key, Predustribution,Unconditionaly Secure key Predistribution,Key Agreement Scheme-Diffie-Hellman Key agreement,Public key infrastructure-PKI,Certificates,Trust Models.

UNIT V **9**

Secret Sharing Schemes-The Shamir Threshold Scheme,Access Structure and General Scret key sharing,Informataion Rate and Construction of Effcient Schemes,Multicast Securuty and Copyright production-Multicast Security,Braodcast Encryption ,Multicast Re-keying,Copyright Protection ,Tracing Illegally Redistribution keys.

TOTAL : 45

TEXT BOOK

Douglas R. Stinson ,"Cryptography Theory and Practice ", Third Edition, Chapman & Hall/CRC,2006

REFERENCES

1. Menges A. J , Oorschot P, Vanstone S.A,"Handbollk of Appliled Cryptography" CRC Press,1997.

2. William Stallings, "Cryptography and Network Security: Principles and Practices", Third Edition, Pearson Education,2006.

3. Wenbo Mao, "Modern Cryptography – Theory and Practice", Pearson Education, First Edition, 2006.
4. Charles B. Pfleeger, Shari Lawrence Pfleeger, "Security in Computing", Fourth Edition, Pearson Education, 2007.
5. Wade Trappe and Lawrence C. Washington, "Intrduction to Cryptography with Coding Theory" Second Edition, Pearson Education, 2007.