Semester - 1
Paper 104: Cryptography

Marks: 100 **Lectures 60**

Objective: After infrastructure and software, the communication in between multiple devices using applications and securing them become most important, cryptography is the mechanism using which we hide the information in public eye site from anybody and is something which is used very popularly almost anything across the internet. So we start with fundamentals of what is cryptography and how cryptography algorithms work and then come to real world scenarios on how currently our data processed on the internet is secured from the eyes of an intruder. Further, the paper enables the students to use cryptography in the most extensive and elaborate manner.

Unit I: - Classical Ciphers

Ceaser Cipher, Vegnere Cipher, Rail-fence Cipher, Row Transposition Cipher.
Requirement and Basic Properties, Main Challenges, Confidentiality, Integrity, Availability, Non-Repudiation,

Unit II: Secret Key Cryptography

Data Encryption Standard-Symmetric Ciphers (Stream Cipher &Block cipher) Advanced Encryption Standard (AES)-Triple DES-Blowfish, RC4, RC5/RC6 family.

Unit III: Public Key Cryptography and Bitcoins

Principles of public key cryptosystems-The RSA algorithm-Key management -Diffie Hellman Key exchange, Elgamal Algorithm, Polynomial Arithmetic, Elliptic curve arithmetic-Elliptic curve cryptography, cryptanalysis.
Bitcoin introduction, working, blockchain crucial to bitcoin, block chain operation with bitcoins, bitcoin glossary, bitcoin wallets, setup for bitcoin payments, bitcoin mining.

Unit IV: Message authentication code and Hash Functions

Message authentication code Authentication functions, Hash functions-Hash Algorithms (MD5, Secure Hash Algorithm), Digital signatures (Authentication protocols, Digital signature Standard). Digital Certificate and Public Key Infrastructure.

Suggested Readings:

1. Delfs, H. & Knebl, H. (2001). *Introduction to Cryptography: Principles and Applications*. Springer-Verlag Berlin and Heidelberg GmbH & Co.

2. Stallings, W. (2010). *Cryptography and network security: Principles and practice* (5th ed.) Boston: Prentice Hall.

3. Menezes, A.J., Oorschot, P. Van & Vanstone, S.A. (1997). *The Handbook of Applied Cryptography*. CRC Press.

4. Schneier, B. (1995). *Applied cryptography, Protocols, algorithms and source code in C* (2nd ed.). New York: John Wiley & Sons.

Latest research papers from refereed journals discussed by the faculty may also be referred.