KONKAN GYANPEETH

KARJAT COLLEGE OF ARTS, SCIENCE AND COMMERCE

Network Security

B.Sc. (IT) Sem. V

EVALUATION SYSTEM

	Time	Marks
Theory Exam	3 Hrs.	100
TW / Tutorial	–	50

SYLLABUS

1. **Cryptography:**
   Introduction. Some Simple Cryptosystems, The Shift Cipher, The Substitution Cipher, The Affine Cipher, The Vigenere Cipher, The Hill Cipher, The Permutation Cipher, Stream Ciphers, Cryptanalysis, Cryptanalysis of the Affine Cipher, Cryptanalysis of the Substitution Cipher, Cryptanalysis of the Vigenere Cipher, Cryptanalysis of the LFSR-based Stream Cipher. Shannon's Theory, Perfect Secrecy, Entropy, Huffman Encodings and Entropy, Properties of Entropy, Spurious Keys and Unicity Distance.

   The Data Encryption Standard, Description of DES, An Example of DES Encryption, The DES Controversy, DES in Practice, DES Modes of Operation, A Time-memory Trade-off, Differential Cryptanalysis, An Attack on a 3-round DES, An Attack on a 6-round DES.

   Introduction to Public-key Cryptography, More Number Theory, The Euclidean Algorithm, The Chinese Remainder Theorem, Other Useful Facts, The RSA Cryptosystem, Implementing RSA, Probabilistic Primality Testing, Attacks On RSA, The Decryption Exponent, Partial Information Concerning Plaintext Bits, The Rabin Cryptosystem, Factoring Algorithms, The p - 1 Method, Dixon's Algorithm and the Quadratic Sieve, Factoring Algorithms in Practice

2. **Signature Schemes**
   Introduction, The ElGamal Signature Scheme, The Digital Signature Standard, One-time Signatures, Undeniable Signatures, Fail-stop Signatures

   Hash Functions
   Signatures and Hash Functions, Collision-free Hash Functions, The Birthday Attack, A Discrete Log Hash Function, Extending Hash Functions, Hash Functions from Cryptosystems, The MD4 Hash Function, Timestamping.

   Key Distribution and Key Agreement
   Introduction, Key Predistribution , Blom's Scheme, Diffie-Hellman Key Predistribution, Kerberos, Diffie-Hellman Key Exchange, The Station-to-station Protocol, MTI Key Agreement Protocols, Key Agreement Using Self-certifying Keys.

3. Security Trends, The OSI Security Architecture Security Attacks, Security services, Security Mechanisms, A Model for Network Security.

4. **Authentication Applications**
   Kerberos, X.509 Authentication Service, Public-Key Infrastructure, Recommended Reading and Web Sites, Key Terms, Review Questions and Problems, A Kerberos Encryption Techniques, Electronic Mail Security, Pretty Good Privacy, S/MIME, Key Terms, Review Questions, and Problems, A Data Compression Using Zip, Radix-64 Conversion, PGP Random Number Generation

5. **IP Security**
   IP Security Overview, IP Security Architecture, Authentication Header, Encapsulating Security Payload, Combining Security Associations, Key Management, Recommended Reading and Web Site, Key Terms, Review Questions, and Problems

Web Security
Web Security Considerations, Secure Socket Layer and Transport Layer, Security, Secure Electronic Transaction, Recommended Reading and Web Sites

5. Intruders
Intrusion Detection, Password Management, Recommended Reading and Web Sites.

Malicious Software
Viruses and Related Threats, Virus Countermeasures, Distributed Denial of Service Attacks, Recommended Reading and Web Sites.

Firewalls
Firewall Design Principles, Trusted Systems, Common Criteria for Information Technology Security Evaluation, Recommended Reading and Web Sites.

Reference :
1. Cryptography : Theory and Practice (Douglas Stinson) CRC Press, CRC Press LLC
2. Cryptography and Network Security Principles and Practices (William Stallings) PHI (Pearson)