BE Semester-__VI__ (Computer Engineering) Question Bank

(Cryptography and network security)

All questions carry equal marks(10 marks)

Q.1	Give differences 1. Monoalphabetic cipher and polyalphabetic cipher. 2. Unconditionally secure and computationally secure 3. Block cipher and stream cipher 4. Cryptanalytic attack and brute force attack.
Q.2	Explain with example playfair and ceaser cipher.
Q.3	Explain with example hill cipher.
Q.4	Explain DES algorithm.
Q.5	Explain any two methods for random number generation.
Q.6	How key can be distributed in cryptography? What are the issues?
Q.7	Explain RSA algorithm and give example of generation of public and private keys and generation of ciphertext through RSA.
Q.8	Explain elliptic curve cryptography.
Q.9	Explain how Diffie Hellman key exchange works?
Q.10	Write Euclid’s algorithm and give suitable example.
Q.11	Explain blowfish.
Q.12	What is encryption and decryption? What is active and passive attacks?
Q.13	Write Blowfish algorithm.
Q.14	Define categories of security services.
Q.15	Define categories of security mechanisms.
Q.16	Explain the five ingredients of symmetric encryption scheme.
Q.17	Write the three dimensions of cryptographic systems.
Q.18	List the various types of attacks on encrypted system.
Q.19	Explain the Fiestel cipher.
Q.20	Write the principles of public key cryptography.
Q.21	Explain RC5 and RC2 schemes.
Q.22	Explain MD5 algorithm.
Q.23	Explain SHA1 algorithm.
Q.24	What types of attacks are addressed by message authentication?
Q.25	Describe the basic uses of message encryption.
Q.26	Describe the basic uses of message authentication code.
Q.27	Describe the basic uses of hash function.
Q.28	Write the requirements of hash functions.
Q.29	What are the properties a digital signature should have?
Q.30	Give examples of replay attack.
Q.31	Write the digital signature standard algorithm.
Q.32	Explain pretty good privacy
Q.33	What fields are there in authentication header?
Q.34	Write the firewall design principals.
Q.35	Explain transport layer security
Q.36	Explain secure socket layer.
Q.37	Write about kerberose and x.509 authentication services.
Q.38	What are web security requirement?

Q.39	Explain the concept of trusted systems.
Q.40	Explain modular arithmetic.