Assignment CS703 CIS

Unit-I

1. What are the types of attacks on encrypted message?

2. What is cryptanalysis and cryptography?

3. Explain with example stream cipher and block cipher with example.

4. Explain with example Substitution and Transposition techniques.

5. What is the advantage and disadvantage of one time pad encryption algorithm?

6. Convert “MEET ME” using Hill cipher with the key matrix

7. Briefly explain the design principles of block cipher. Discuss in detail block cipher modes of operation.

8. Explain with example Chinese Remainder theorem

Unit-II

1 Perform encryption and decryption using RSA Algorithm. for the following. P=7; q=11; e=17; M=8.

2. List four general characteristics of schema for the distribution of the public key.

3. Draw the general structure of DES and explain the encryption decryption process?

4. What primitive operation is used in RC4?

5. (i) Explain the generation sub key and S Box from the given 32-bit key by Blowfish. (ii) In AES, hoe the encryption key is expanded to produce keys for the 10 rounds

Unit-III

1. (i) Briefly explain Deffie Hellman key exchange with an example.

2. (i) Write and explain the digital signature algorithm. (ii) Explain in detail Hash Functions.

3. (i) Compare the Features of SHA-1 and MD5 algorithm. (ii) Discuss about the objectives of HMAC and it security features.

4. Users A and B use the Diffie Hellman key exchange technique, a common prime q=11 and a primitive root alpha=7.

(i) If user A has private key XA=3.What is A’s public key YA?

(ii) If user B has private key XB=6 What is B's public key YB? (iii) What is the shared secret key? Also write the algorithm.

5. (i) Explain in detail EIGamal Public key cryptosystem.

Unit-IV

1. How does PGP provide confidentiality and authentication service for e-mail and file storage applications? Draw the block diagram and explain its components.

2. Write Short notes on S/MIME .

3. Explain the architecture of IP Security

4. (i) Describe the SSL Specific protocol – Handshake action in detail.

(ii) Explain Secure Electronic transaction with neat diagram.

5. (i) What is Kerberos? Explain how it provides authenticated service.

(ii)Explain the format of the X.509 certificate.

Unit-V

1. (i) Explain any two approaches for intrusion detection. (i) Identify a few malicious programs that need a host program for their existence.

2. (i) Explain firewalls and how they prevent intrusions. (ii)List and Brief, the different generation of antivirus software.

3. (i) Define intrusion detection and the different types of detection mechanisms, in detail.

4. (i)Explain the types of Host based intrusion detection. List any two IDS software available.

(ii) What are the positive and negative effects of firewall?

5. Describe packet filtering router in detail.