CRYPTOGRAPHY

UNIT 1

1. State Fermat’s theorem ?
2. Categorize Passive and Active attack.
3. Explain the OSI security architecture along with the services available?
4. Using playfair cipher algorithm, encrypt the message using the key "MONARCHY"and explain ?
5. State Chinese remainder theorem and find X for the given set of congruent equations using CRT
   X≡2(mod 3)
   X≡3(mod5)
   X≡2(mod7

UNIT II

1. Explain briefly about DES in detail?
2. Explain the RSA algorithm in detail and discuss its merits
3. Explain RSA algorithm ,perform encryption and decryption to system with p=7;q=11;e=17;M=8.
4. Explain Diffie-Hellman key exchange algorithm in detail.
5. What do you mean by AES?.Diagrammatically illustrate the structure of AES and describe the steps in AES encryption process with example?

UNIT III

1. Write algorithm of MD5 and explain
2. Briefly explain Digital Signature Algorithm.
3. With a neat diagram,explain the steps involved in SHA algorithm for encrypting a message with maximum length of less than 2 128 bits and produce as output of 512-bit message digest?
4. Explain about secure hash algorithm(SHA) in detail?
5. Differentiate MAC and hash function?

UNIT IV

1.Discuss about X.509 authentication service in detail.
2. Discuss about S/MIME in detail.
3. Write about PGP in detail.

4. Explain in detail about SET.
5. Describe about IP security
6. What is kerberos? Explain how it provides authenticated service?

UNIT V

1. Write about virus and related threats in detail?
2. Explain about the malicious software?
3. Explain the architecture of IP security in detail?
4. Write the steps involved in the simplified form of the SSL/TLS protocol
5. What is a firewall ? Define Firewall policy ?