IMPORTANT QUESTIONS

Unit-1:

1. Explain different types of attacks being performed by an intruder?
2. Discuss in detail about different security mechansims.
3. Construct a playfair matrix with the key “LARGEST” to encrypt the message:MEET ME AT THE TOGA PARTY.
4. Compare vigenare and vernam ciphers.

Unit-2:

1. With a neat diagram explain fiestel block cipher structure?
2. Explain about DES algorithm?
3. What are the different stages in each round of AES Algorithm?

Unit-3:

1. Explain about Miller-Rabin Primality Algorithm with an example
2. Explain about RSA algorithm with an example?
3. Explain about elgamal cryptography with an example.
4. Discuss in detail about Diffie-Helman Key Exchange Algorithm.
5. Explain about elliptic curve cryptography

Unit-4:

1. Differentiate between Message Integrity and Message Authentication?
2. Explain the working of SHA-512 Hash Algorithm with a neat diagram?
3. Compare HMAC and CMAC?
4. What are the services provided by digital signatures?
5. Explain about Digitial Signature Algorithm?

Unit-5:

1. Compare SSL and TLS.
2. Explain about PGP and services offered by it.
3. Discuss in detail about S/MIME.
4. Discuss in detail about
   i)IPSec ii)ISAKMP

5. Discuss in detail about various

   i) viruses ii)Firewall iii)IDS/IPS