**CRYPTOGRAPHY AND NETWORK SECURITY**

**UNIT-3 IMPORTANT QUESTIONS**

1. Explain about Chinese remainder theorem with an example.
2. Explain about encryption and authentication processes in asymmetric key cryptography.
3. Compare symmetric and asymmetric key cryptographic schemes.
4. Explain about RSA algorithm with an example?
5. Explain about elgamal cryptography with an example.
6. Discuss in detail about Diffie-Helman Key Exchange Algorithm.
7. Explain about elliptic curve cryptography

**UNIT-4 IMPORTANT QUESTIONS**

1. Explain the working of SHA-512 Hash Algorithm with a neat diagram?
2. Compare HMAC and CMAC?
3. What are the services provided by digital signatures?
4. What are approaches available for implementing digital signature algorithm?
5. Explain about NIST Digitial Signature Algorithm?
6. Explain about PGP and services offered by it.
7. Discuss in detail about S/MIME.
8. What are the five header elements of S/MIME

**UNIT-5 IMPORTANT QUESTIONS**

1. Explain SSL protocol
2. Explain about Transport and tunnel modes for various protocols at network level?
3. Discuss in detail about

i)IPSec ii) ESP iii) AH iv)ISAKMP

4. Discuss in detail about knowledge/Expert based IDS/IPS

5. Discuss in detail about Machine Learning based IDS/IPS

6. Discuss in detail about Signature based IDS/IPS

7. Discuss in detail about Host or Network Based IDS

8. Discuss in detail about various

i) viruses ii)Firewall iii)IDS/IPS