| Q.No. | Question |
|---|---|

## Part – A
**(Each Question carries 2 Marks)**

| | |
|---|---|
| 1. | Define security mechanisms. |
| 2. | Define product cipher. |
| 3. | Tell the GCD of (270, 192). |
| 4. | Explain the avalanche effect. |
| 5. | List the applications of public key cryptosystem. |
| 6. | What is a primitive root of a number? |
| 7. | Identify the security services provided by digital signature. |
| 8. | How digital signatures differ from authentication protocols? |
| 9. | List the three classes of intruders. |
| 10. | Define SET? What are the features of SET? |

## Part – B
**(Answer for each question carries 13 Marks**

| Q.No. | Question |
|---|---|
| 6. | (a) Solve using playfair cipher method. Encrypt the word "Semester Result" with the keyword Examination". Discuss the rules to be followed. |
| | Or |
| | (b) (i) What is steganography? Explain the various techniques used in steganography. (6)<br>(ii) What is monoalphabetic cipher? Examine how it differs from Caesar cipher. (7) |
| 7. | (a) For each of the following elements of DES, indicate the comparable element in AES if available.<br>i) XOR of sub key material with the input to the function (4)<br>ii) f function (3)<br>iii) Permutation p (3)<br>iv) Swapping of halves of the block. (3) |
| | Or |
| | (b) Illustrate structure of AES and describe the steps in AES encryption process with example. |

| | | |
|---|---|---|
| 8. | (a) | With the neat sketch explain the Elliptic curve cryptography with an example. |
| | | Or |
| | (b) | Explain in detail about different ways of distribution of public keys 7. Consider prime field q=19, it has primitive roots {2,3,10,13,14,15}, if suppose α=10. Then write key generation by she choose XA=16. And also sign with hash value m=14 and alice choose secret no K=5. Verify the signature using Elgamal digital Signature Scheme |
| 9. | (a) | Explain briefly about architecture and certification mechanisms in Kerberos and X.509. |
| | | Or |
| | (b) | (i)Where hash functions are used? What characteristics are needed in secure hash function? Explain about the security of hash functions and MACs. (7)<br>(ii) Discuss the classification of authentication function in detail. (6) |
| 0. | (a) | Explain the architecture of IPsec in detail with a neat block diagram. |
| | | Or |
| | (b) | Define intrusion detection and the analyze different types of detection mechanisms in detail. |

**Part – B**

**(Answer for each question carries 16 M**

| | | |
|---|---|---|
| | (a) | Demonstrate the DH key exchange methodology usin following key values: p=11,g=2,XaA=9,XbB=4.<br>In an RSA system, the public key of a given user i e=65,n=2881, what is the private key of this user? |
| | | Or |
| | (b) | Discuss the following in detail.<br>(i) Modular Exponentiation (7)<br>(ii) Finite Fields (6) |