1. **Fill the spaces with the correct answer (5 marks)**

**Integrity - Hash function- Diffie-Hellman- Cryptographic checksums- Confidentiality-RSA- Cryptography- computer security– Transposition – Substitution**

* 1. …………. …. Preventing the sensitive information from unauthorized user.
  2. …………….... A public function of the message for any length into a fixed-length hash value, which serves as the authenticator.
  3. …………………is a practical method for public exchange of a secret key.
  4. ……………………is the science of writing in-secret code and is an ancient art
  5. ………method: where the letters in plain text is replaced by other letters or numbers or symbols.

1. **Given the following plaintext message : (5 marks)**

“Cryptography and network securityare advanced topics for communication

Engineers" Encrypt the message using **transposition** cipher with **key**: 354216

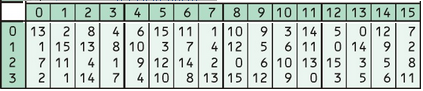
1. **Construct the play fair matrix for the following key: “television” (3 marks)**
2. **What is the difference between: (8 marks)**
   1. stream cipher and block cipher
   2. one-time authentication and mutual authentication
3. **Explain with drawing (3 marks)**

Cipher Block Chaining (CBC) mode :Ci= Ek(Pixor Ci-1), where C0= IV

Cipher Feedback (CFB) mode :Ci= Ek(Ci-1) xor Pi where C0= IV

1. **Given S8 of S-box in DES algorithm (6 marks)**

Solve the following two blocks: **011110** and **100001**



1. **In key generation at DES the used key is 64-bit, Discus in brief how the algorithm use only 56-bit and then generate 16 48-bit keys**  **(4 marks)**
2. **In RSA algorithm (6 marks)**

Let p=5 and q =11. Compute N and Φ(n)?

If e = 13 and D= 37, what is the public and private key?

Write the mathematical equation to encrypt and decrypt a message using the public and private key in RSA algorithm?

1. **What is the authentication? Its type? (5 marks)**
2. **(10 marks)**

**Assuming that Alice and John want to communicate with each other , both of** them has owned key and the corresponding public key stored at a shared server, they also have the server public key, write your own protocol – as you see- to enable Alice and Bob to communicate.

**Note**: illustrate your answer with drawing, illustrate the authentication process and key exchange – choose your own symbols and explain them.

1. **True or false and correct the wrong word (10 marks)**

11.1 Confidentiality can be achieved by encipherment.…………….. ( )

11.2 Digital signature ensures availability…………………………… ( )

11.3 Security service is any action that compromises the security of information owned by an organization. …………………………………………..( )

11.4 SH-1 is a symmetric algorithm …………………………………. ( )

11.5 Kerberos is a computer network authentication protocol ..............( )

1. **Encrypt the following statement using Caesar cipher, let k =10.**

M e e t m e a t t e n o c l o c k t o d a y **(5 marks)**

**13. You are working in information teechnology company, the company decided to build a strong security system. your manager want to disscus with you two important issues in key management which are**

* 1. Key Storage
  2. Key Distribution and Key exchange

Discuss illustrating your ideas. **(6 marks)**