Name: **ID:** ***(Total = 20 Marks)***

1) Complete the sentences: ***6 Marks = 1 point each***
   a) Cryptanalysis is the discipline of …. the cryptographic systems .
   b) Kerckhkoffs Principle main idea stress on making the cryptosystem algorithm … to all
   c) Although hill cipher support diffusion and confusion which are the main properties of good cryptosystem, it is not to be used as common cryptosystem because of its …
   d) Although the Vernam (One time pad) cipher is unconditionally secure which makes it almost impossible to be broken, its problem not to be used practically is …
   e) Elliptic curve crypto system is promising to replace RSA because …
   f) The system clock can be used as … software based random number generators.

---

2) Choose the is best: ***6 Marks = 1/2 point each***
   a) Public key cryptosystem – Asymmetric Key Cryptography
   b) Secret Key cryptography - Symmetric Key Cryptography

DES:	**RSA**:	**AES:**
Merkle-Hellman Knapsack:	**Vigènere Cipher:**	**Enigma Machine:**
ElGamal:	**Wheel Cipher:**	**Caesar Cipher:**
Elliptic Curve cryptography:	**One Time Pad:**	**Transposition:**

---

3) Assume a Public key cryptosystem having the following message encryption output using the public keys: ***8 Marks = 2points each***

User *A*	User *B*
$E_{a\text{-public}}(COE) = (ICS)$	$E_{b\text{-public}}(SWE) = (ICS)$
$E_{a\text{-public}}(ICS) = (SWE)$	$E_{b\text{-public}}(ICS) = (COE)$
$E_{a\text{-public}}(SWE) = (AEE)$	$E_{b\text{-public}}(COE) = (AEE)$
$E_{a\text{-public}}(AEE) = (COE)$	$E_{b\text{-public}}(AEE) = (SWE)$

Assume the public key and private key for both users *A* and *B* are known by each others and they want to communicate. What will be seen on the network assuming the following:

   a) User *A* wants to send to *B* message (ICS) Openly but signed (authenticated):
   b) User *B* wants to send to *A* message (AEE) confidentially but signed (authenticated)::
   c) User *A* wants to send to *B* message (SWE) confidentially but signed (authenticated):
   d) User *B* wants to send to *A* message (COE) confidentially but signed (authenticated):