Term 081 Quiz 3 COE 449: Network Security Engineering Dr Adnan Gutub Monday 29th December 2008

Name: **ID:** **(30 Marks = 1 point per question)**

1) The following sentences are wrong, correct them below:

a) Cryptanalysis is the discipline of analyzing and studying the cryptographic systems to benefit in building secure communications over non-secure channels

b) Kerckhkoffs Principle main idea stress on security through obscurity

c) Since advance substitution replaces every letter with a randomly chosen other letter making its brute force attack need 26! tests, the system cannot be broken easily.

d) The main problem of hill cipher not to be used as common cryptosystem is that it does not support diffusion and confusion which are the main properties of good cryptosystem.

e) The main problem of not using the Vernam (One time pad) cipher is that its unconditionally secure which makes it almost impossible to be broken.

f) Elliptic curve crypto system is promising to replace RSA because of political reasons.

g) The system clock, the mouse movement, and the temperature measurements, can be used as strong hardware based random number generators.

2) Choose from the sentences what is best matching the crypto systems (some may be used more than once and some may not be needed)
   a) Integer Factorization
   b) Algebraic coding theory (decoding a linear code)
   c) Discrete logarithm problem for finite fields
   d) Elliptic curve discrete logarithm problem
   e) Non of the above

DES:	**RSA**:	**AES:**
Merkle-Hellman Knapsack:	**Vigènere Cipher:**	**McEliece:**
Enigma Machine:	**ElGamal**:	**Wheel Cipher:**
Chor-Rivest:	**Monoalphabetic Substitution:**	**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:

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 (COE) openly:

b. User *B* wants to send to *A* message (SWE) confidentially:

c. User *A* wants to send to *B* message (ICS) Openly but signed (authenticated):

d. User *B* wants to send to *A* message (AEE) confidentially but signed (authenticated)::

e. User *A* wants to send to *B* message (ICS) confidentially:

f. User *B* wants to send to *A* message (ICS) confidentially and signed (authenticated):

g. User *A* wants to send to *B* message (SWE) confidentially but signed (authenticated):

h. User *B* wants to send to *A* message (COE) confidentially but signed (authenticated):