COSC 2536/2537

Online Final Test (Mock Questions)

Question-1:

Decrypt the following ciphertext using the double transposition cipher using a matrix of 3 rows and 4 columns.

Y M T O E M H O E M C O

Hint: The first two letters in the plaintext are "C" and "O".

Select the correct answer:

a) Comeatmyhome
b) Cometomyhome
c) Comeonmyhome

Question-2:

In a RSA crypto system, which one of the following is correct for public key parameters ***e*** and ϕ(n) if p=677 and q=971 ,where n=pXq?

Select the correct answer:

a) e = 5, ϕ(n) = 655720
b) e = 7, ϕ(n) = 655720
c) e = 10, ϕ(n) = 655720
d) none of the above

Question-3:

In the case of One-time pad the size of the key is _____ to/than the size of the plain text.

Select the correct answer:

a) less
b) greater
c) equal
d) independent

Question-4:

In Paillier crypto system, what is the value of λ if the two primes are p and q, respectively?

Select the correct answer:

a) GCD(p-1,q-1)
b) LCM(p-1,q-1)
c) GCD(p,n)
d) None of the above

Question-5:

Assume you have two ciphertexts C1= 416 and C2=127 of two different messages m1 and m2 respectively, generated using Paillier homomorphic encryptions. You want to homomorphically add these two numbers. After performing all of the required computations, what is the plaintext result you should get using parameters: $\lambda = 12$, $n = 35$ and $\mu = 23$?

Select the correct answer:

a) 60
b) 50
c) 10
d) 5

Question-6:

Suppose, Bob wants to sign a message and for this he generates the private and public key parameters (d,e) which are (7477,29) using RSA encryption algorithm. If his two prime numbers are 113 and 89, what would be the value of his signature 'S' for the message 500?

Select the correct answer:

a) 8235
b) 8065
c) 8574
d) none of the above

Question-7:

What happens to the distributed ledger in a Blockchain if any one or two nodes fail in the network?

Select the correct answer:

a) it has no impact on the ledger
b) it corrupts the entire ledger
c) it generates a entire new ledger
d) none of the above