**Military College of Signals**

**IS-842 Applied Cryptography**

**MSIS-11 (Fall 2012)**

**Quizz #1**

Maximum Time: 15 Minutes

Maximum Marks: 10

Instructor: Brig (R) Dr. Ashraf Masood

Note: Attempt ALL questions. For full credits, justify your answers with appropriate reasons wherever required.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Question #1**

If we update Feistel network as shown in following diagram

Li

Ri

Ri+1

Li+1

Ki+1

Where . Explain how to decrypt in this case. [5 Marks]

**Question #2**

Let (*E*,*D*) be a (one-time) semantically secure cipher where the message and ciphertext space is {0,1}*n*. Which of the following encryption schemes are semantically secure?

1. *E*′(*k*,*m*)=reverse(*E*(*k*,*m*))
2. *E*′(*k*,*m*)=*E*(*k*,*m*)∥LSB(*m*)
3. *E*′(*k*,*m*)=*E*(0*n*,*m*)
4. *E*′(*k*,*m*)=compute *c*←*E*(*k*,*m*) and output  *c*∥*c* (i.e., output *c* twice)
5. *E*′( (*k*,*k*′), *m*)=*E*(*k*,*m*)∥*E*(*k*′,*m*)

[5 marks]

**Question #3 [Bonus Question]**

Suppose that using commodity hardware it is possible to build a computer for about $200 that can brute force about 1 billion AES keys per second. Suppose an organization wants to run an exhaustive search for a single 128-bit AES key and was willing to spend 4 trillion dollars to buy these machines (this is more than the annual US federal budget). How long would it take the organization to brute force this single 128-bit AES key with these machines? Ignore additional costs such as power and maintenance.

More than a month but less than a year

More than a million years but less than a billion (109) years

More than a day but less than a week

More than a billion (109) years

More than a 100 years but less than a million years

[2 marks]