**National University of Sciences & Technology**

**Military College of Signals**

**IS-842 Applied Cryptography**

**MSIS-11 (Fall 2012)**

**One-Hour-Test #2**

Maximum Time: 1 Hour

Maximum Marks: 30

Instructor: Brig (R) Dr. Ashraf Masood

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

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

**Question #1**

1. Answer following questions briefly:
   1. What is the difference between diffusion and confusion in cryptographic constructions?
   2. What is the significance of the key schedule in modern block ciphers? (i.e., can't these ciphers be designed without a key schedule?)
   3. What is Davies-Meyer compression function? What is its significance with respect to collision resistance.
   4. Which order of encryption and authentication is preferred in authenticated encryption.
   5. What is difference between SHA-1 and SHA-3 in terms of size of input and output blocks; and number of rounds/sub-rounds.

(8 marks)

**Question #2**

1. Compare AES to DES. For each of the following elements of DES, indicate the comparable element in AES or explain why it is not needed in AES.
   1. XOR of subkey material with the input to the f function
   2. XOR of the f function output with the left half of the block
   3. The f function
   4. Permutation P
   5. Swapping of halves of the block (5 marks)

**Question #3**

1. Answer following questions with justification:
   1. Let *m* be a message consisting of ℓ AES blocks (say ℓ=100). Alice encrypts *m* using CBC mode and transmits the resulting ciphertext to Bob. Due to a network error, ciphertext block number ℓ/2 is corrupted during transmission. All other ciphertext blocks are transmitted and received correctly. Once Bob decrypts the received ciphertext, how many plaintext blocks will be corrupted?
   2. Consider the encrypted CBC MAC built from AES. Suppose we compute the tag for a long message *m* comprising of *n* AES blocks. Let *m*′ be the *n*-block message obtained from *m* by flipping the last bit of *m* (i.e. if the last bit of *m* is *b* then the last bit of *m*′ is *b*⊕1). How many calls to AES would it take to compute the tag for *m*′ from the tag for *m* and the MAC key? (in this question please ignore message padding and simply assume that the message length is always a multiple of the AES block size) Justify your answer with brief explanation.

(5 marks)

**Question #4**

1. Answer following question by show your working.
   1. Solve the equation 3*x*+2=7 in Z19.
   2. How many elements are there in Z\*35?
   3. How much is 210001mod11?

Hint: use Fermat's theorem. (you should not need a calculator)

* 1. How much is 2245mod35?

Hint: use Euler's theorem (you should not need a calculator)

* 1. What is the order of 2 in Z\*35?
  2. Is 6 a generator of Z\*13? (12 marks)