**Military College of Signals**

**IS-842 Applied Cryptography**

**MSIS-11 (Fall 2012)**

**One-Hour-Test #1**

Maximum Time: 1 Hour

Maximum Marks: 100

Instructor: Brig (R) Dr. Ashraf Masood

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

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

**Question #1**

Given an Affine Cipher with ***P = C = Z26***and ***K*** = {(a,b) є ***Z26 × Z26***}. Decrypt the ciphertext “YATJ” encrypted with key ***K***=(11, 2). (20 marks)

**Question #2**

Assuming that Vigenere Cipher oracle is available for chosen plaintext attack. As a adversary choose a suitable plaintext such that the keyword can be determined simply by inspection of the ciphertext. (10 marks)

**Question #3**

Have a look at the substitution cipher and recall the Shanon’s definition of perfect secrecy. Prove that the substitution cipher is perfectly secure for the special case of ℓ = 1 (where ℓ is the length of plaintext , ciphertext and key), and that it is not perfectly secure if ℓ ≥ 2. Justify your answer.

(15 marks)

**Question #4**

Let ***M*=*C*=*K***={0,1,2,…,255} and consider the following cipher defined over (***K*,*M*,*C***):   
*E*(*k*,*m*) = *m*+*k* (mod256); *D*(*k*,*c*) = *c*−*k* (mod256) .   
Does this cipher have perfect secrecy? Justify your answer. (15 marks)

**Question #5**

Suppose you are told that the one-time pad (OTP) encryption of the message "attack at dawn" is 6c73d5240a948c86981bc294814d (the plaintext letters are encoded as 8-bit ASCII and the given ciphertext is written in [hex](http://en.wikipedia.org/wiki/Hexadecimal)). What would be the one time pad encryption of the message "attack at dusk" under the same OTP key? (20 marks)

**Question #6**

Let *G*:*K*→{0,1}*n*  be a secure PRG. Define *G*′(*k*1,*k*2)=*G*(*k*1)⋀*G*(*k*2) where ⋀ is the bit-wise AND function.

Consider the following statistical test *A* on {0,1} *n* :   
*A*(*x*) outputs LSB(*x*), the least significant bit of *x*.   
What is *Adv*PRG[*A*,*G*′] ?    You may assume that LSB(*G*(*k*)) is 0 for exactly half the seeds *k* in *K*.   
Justify your answer. (20 marks)

**Numerical values assigned to English language alphabets in *Z26***



**ASCII Table**

