UNIVERSITY OF PERADENIYA

Faculty of Engineering

MID SEMESTER EXAMINATION, MARCH 2017

CO 325 – Computer and Network Security

Time: One Hour

Answer ALL THREE questions

1.

a. Briefly describe the three goals of security: *Confidentiality*, *Integrity* and *Availability*. [10 Marks]

b. Briefly describe *Cryptography* and *Steganography*. [10Marks]

c. An Affine cipher is defined by the equation P = K1 + K2 mod 26.

   i. What is the condition that K2 has to satisfy in order to ensure decryption? [10 Marks]

   ii. If K1 = 2 and K2 = 3, what is the cipher text of P = 4? [10 Marks]

   iii. Show that 9 is the inverse of 3 mod 26? [10 Marks]

   iv. Show that the above cipher text produces the plaintext when decrypted. [10 Marks]

d. *Substitution* and *Transposition* are the two techniques used in both conventional and modern symmetric key ciphers. Briefly explain their meanings. [10 Marks]

e. Draw a Straight P Box with 8 inputs that shifts the input bits by one bit left. [15 Marks]

f. Given below is a part of an S-Box used in DES. What is the output if 101010 is given as the input? [15 Marks]
(Bits 1 and 6 define the row and bits 2, 3, 4 and 5 define the column)

15	1	8	14	6	11	3	4	……
3	13	4	7	15	2	8	14	……
0	14	7	11	10	4	13	1	……
13 8	.	.	.	.	.	.	……	

2.

a. Briefly describe ECB (Electronic Code Book) and CBC (Cipher Block Chaining) modes of operation of block ciphers and their advantages and disadvantages. [20 Marks]

b. What is the difference between a block cipher and a stream cipher? [10 Marks]

c. Draw the block diagram of a stream cipher constructed using a Liner Feedback Shift Register (LFSR) with bits b0, b1, b2 and b3 with a feedback function created by XORing b0 and b1. [25 Marks]

d. If the seed is 1000 (corresponding to b0, b1, b2 and b3, respectively), write the generated key stream. [25 Marks]

e. What is the maximum period of a LFSR? [10 Marks]

f. What is the difference between Symmetric Key (Private Key) Cryptography and Asymmetric Key (Public Key) Cryptography? [10 Marks]

3.

a. RSA is a popular public key algorithm. The following are the parameters of a particular instance of ~~usage of~~ RSA usage.

p=17, q=11

i. Calculate n, Phi(n) [20 Marks]

ii. Selecting the encryption key e=7, show that the decryption key is 23 [20 Marks]

iii. Taking plain text M=88, show that the cipher text C=11 [20 Marks]

iv. Show that the cipher text C produces the plain text M when decrypted. [20 Marks]

b. Security of RSA depends on the difficulty of factorization. Briefly explain. [10 Marks]

c. Write a protocol of a hybrid cryptosystem where a symmetric key exchange takes place using public key encryption/ decryption. [10 Marks]