University of Technology
Department of Computer Science
BSc. Study /Fourth Class (SE, AI and MM)
Final Exam / First Try / 2016 -2017

Subject: data security *Date: / /2017*
Examiner: Dr. soukaena Hassan *Time: 3 Hours*

Note1: Answer four (4) Questions Only. Each Question (15 Marks).

Note2: according table of character coding below encrypt and decrypt.

a =0	*b=1*	*c =2*	*d=3*	*e=4*	*f=5*	*g=6*	*h=7*	*i=8*	*j=9*
k=10	*l=11*	*m=12*	*n=13*	*o=14*	*p=15*	*q=16*	*r=17*	*s=18*	*t=19*
u=20	*v=21*	*w=22*	*x=23*	*y=24*	*z=25*				

Q1: Answer two of the following (each branch 7.5 marks)

1. Define confidentiality and explain the confidentiality threats.
2. Define availability and explain availability threats.
3. Define authentication and explain the authentication methods.

Q2: Answer two of the following (each branch 7.5 marks)

1. LCM (433, 34), Φ (17) and Φ (20)
2. Find (X= 2^3 mod 5) using fast exponential procedure
3. Define steganography, show steganography types, and then use LSB approach to hide the character (01010111), if you know that the sequence of 8 bytes had the values:
   01011101 01110101 01011100 00110111 01101101 01010111 01110010 01110010

Q3: Answer two of the following (each branch 7.5 marks)

1. Just Encrypt the message= "love" using Hill cipher algorithm with key = $\begin{matrix} 3 & 5 \\ 7 & 4 \end{matrix}$
2. Encrypt and decrypt the message= "hello" with key="hi" using Beaufort algorithm.
3. Encrypt and decrypt the message= "secrete disclosed" using keyless transposition number of columns=2.
4. Encrypt and decrypt the message= "top" using multiplicative cipher with k= 3 and k^{-1} = 9.

Q4: answer one of the following (15 marks)

1. In DES algorithm, if key (56)=1111000 0110011 0010101 0101111 0101010 1011001 1001111 0001111, Find key(48) since left shift (LS)= 1 and PC-2 table is as follows:

PC-2

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

2. The knapsack = [1, 2 4, 9], Create the hard knapsack sequence and encrypt then decrypt the message P= 0100 1011 1010 0101 using Diffie-Hellman algorithm.

Q5: answer one of the following (15 marks)

1. Encrypt and decrypt the plaintext (***h***); using RSA cipher, where p = 11 and q= 3, find n, Φ (n), *e, and d*.

2. Create a linear feedback shift register LFSR with 5 cells in which b5=b4 xor b_2 xor b_0. Show the output for 12 transitions (shifts) if the seed is $(10101)_2$, then encrypt and decrypt the message "0110000101110010".

Good luck