Q1) Choose the best answer (write down the word/statement):

1- _____ Has two types of keys that are mathematically connected:
[Symmetric Cryptography / **Asymmetric Cryptography** / Both of them / None of Them]

2- $\emptyset(m) = m - 1 \; when \; m$:
[can be factorized to prime numbers / GCD(m, m-1)=1 / **cannot be factorized** / All of Them]

3- Bell-Lapadula model deals with:
[Integrity / Availability / **Confidentiality** / None of Them]

4- $71^{247} \; mod \; 83 =$ _____ : [1 / **71** / 59 / 80] Ans: (71^{3x82})x71 mod 83=71

5- _____ is a high level of security:
[**Cryptography** / Authorization / Access Control / Authentication]

6- Azad, cleared for (TOP SECRET, {A, C}), wants to access a document classified (CONFIDENTIAL, {A}). So, Azad can _____ the specified document:
[**Read** / Write / Both of Them / None of Them]

7- The full form of SSL is:
[Serial Session Layer/ **Secure Socket Layer**/ Session Secure Layer/ Series Socket Layer]

8- How many bytes should be created in Knapsack cryptosystem for a message that contains 10 letters and a super increasing sequence with size 13: [10 / 8 / **7** / 9]

9- _____ is a cryptographic protocol used for securing HTTPS based connection.
[TLS / SSL / **Both of Them** / None of Them]

10- How many digits in a key with size of 4096 bit: [617 / 155 / 308 / **1234**]

Q2) a) Some of scientists have the following opinion: "Nowadays, Authorization is the heart of information security". Do you agree or disagree with them? Why?

Answer: Disagree because nowadays with devlopment of technology cryptography is a high level of security which is considered as a heart of information security. Back in the computing dark ages, authorization was often considered the heart of information security. Today, that seems like a rather quaint notion.

Q2) b) What is the difference between Public and private cryptography key?

Private key is used for both encrypting and decrypting the sensitive data. It is shared between the sender and receiver of encrypted data.	Public key is used only for the purpose of encrypting the data.
The private key mechanism is faster.	The public key mechanism is slower.
The private key is kept secret and not public to anyone apart from the sender and the receiver.	The public key is free to use and the private key is kept secret only.
The private key mechanism is called "symmetric" because a single key is shared between two parties.	The public key mechanism is called "asymmetric" because there are two keys for different purposes.
The private key is to be shared between two parties.	The public key can be used by anyone but the private key is to be shared between two parties only.

Q3) Are the following keys being valid in Knapsack cryptosystem or not? Specify your answer in details? S={1, 2, 4, 9, 18, 36} , M= 71, W= 23

Answer: testing super increasing sequence

2>1 yes

4>3 yes

9>7 yes

18> 16 yes

36>34 yes

So s is super increasing sequence.

M=71≥ $\sum s_i = 70$ yes

$1 \leq w = 22 \leq m = 71$ yes

Finally we should check gcd(22,71)=1?

71=2(22)+5

22=4(5)+2

5=2(2)+1

2=2(1)+0

So, gcd(22,71)=1

So, yes the keys are valid.

Q4) Answer one of the following:

1. Encrypt the last letter from the word (Kurdistan) using RSA cryptosystem with keys: p=11, q=17 and e=29? (Hint: Index the letters from 0-25)

   Answer:

   n= p*q=11*17 =187

   to encrypt $n \equiv 13$ we should find $13^{29} \bmod 187$ using Binary or recursion method:

i	e_i	$C^2 \bmod 187$	cX13 mod 187
4	1	C=13	-
3	1	C=169	C=2197 mod 187=140
2	1	C=19600 mod 187=152	C=1976 mod 187=106
1	0	C=11236 mod 187=16	-
0	1	C=256 mod 187 = 69	C=897 mod 187=149

   So c= 149

2. Use RC4 Cryptography to decrypt (71, 110, 111, 106) using key = [1, 2, 3,6]?

S = [0, 1, 2, 3, 4, 5, 6, 7]

K = [1, 2, 3, 6, 1, 2, 3, 6]

i=0 → j=0+s[0]+k[0]=0+0+1=1 mod 8 = 1→ s= [1, 0, 2 ,3, 4 , 5, 6, 7]

i=1 → j=1+s[1]+k[1]=1+0+2=3 mod 8 = 3→ s= [1, 3, 2 ,0, 4 , 5, 6, 7]

i=2 → j=3+s[2]+k[2]=3+2+3=8 mod 8 = 0→ s= [2, 3, 1 ,0, 4 , 5, 6, 7]

i=3 → j=0+s[3]+k[3]=0+0+6=6 mod 8 = 6→ s= [2, 3, 1 ,6, 4 , 5, 0, 7]

i=4 → j=6+s[4]+k[4]=6+4+1=11 mod 8 = 3→ s= [2, 3, 1 ,4, 6 , 5, 0, 7]

i=5 → j=3+s[5]+k[5]=3+5+2=10 mod 8 = 2→ s= [2, 3, 5 ,4, 6 , 1, 0, 7]

i=6 → j=2+s[6]+k[6]=2+0+3=5 mod 8 = 5→ s= [2, 3, 5 ,4, 6 , 0, 1, 7]

i=7 → j=5+s[7]+k[7]=5+7+6=18 mod 8 = 2→ s= [2, 3, 7 ,4, 6 , 0, 1, 5]

i=(i+1)%8	j=(j+s[i])%8	s	t=s[i]+s[j]	NewKey
1	3	[2, 4, 7 ,3, 6 , 0, 1, 5]	7	5
2	2	[2, 4, 7 ,3, 6 , 0, 1, 5]	6	1
3	5	[2, 4, 7 ,0, 6 , 3, 1, 5]	3	0
4	3	[2, 4, 7 ,6, 0 , 3, 1, 5]	6	1

cipher	Binary	Bin.-Key	XOR	plain	Char
71	01000111	00000101	01000010	66	B
110	01101110	00000001	01101111	111	o
111	01101111	00000000	01101111	111	o

106	01101010	00000001	01101011	107	k

Message = Book

Q5) Answer the following about AES-128:

1. Find W_{12} if the previous round constituting of all ones?

   We are in round 3 → w_{12}
   Round2→ w_8=11 11 11 11, w_9= 11 11 11 11, w_{10}= 11 11 11 11, w_{11}=11 11 11 11
   Rot word of w_{11}= 11 11 11 11
   Sub word of w_{11}=82 82 82 82
   g(w_{11})= 82 82 82 82 XOR $Rcon_3$= 04 00 00 00 = 86 82 82 82
   w_{12}= w_8 XOR g(w_{11})= 11 11 11 11 XOR 86 82 82 82 = 97 93 93 93

2. Find the missing cell: $\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \times \begin{bmatrix} 63 & EB & 9F & A0 \\ 2F & 93 & 92 & C0 \\ AF & C7 & AB & 30 \\ A2 & 20 & CB & 2B \end{bmatrix} = \begin{bmatrix} BA & 84 & E8 & IB \\ 75 & A4 & \_\_ & 40 \\ F4 & 8D & 06 & 7D \\ 7A & 32 & 0E & 5D \end{bmatrix}$

   [2 Marks]

   Cell(2,3)=?
   01 × 9F= 01 × 10011111
   02 × 92 =02 × 10010010
   03 × AB =03 × 10101011
   01 × CB=01 × 11001011
   10011111
   00100100
   00011011
   10101011
   01010110
   00011011
   11001011 **XOR**
   10001101 ≡8D
   Cell(2,3)=8D

3. What are the operations that are computed in the last round of AES-128 Encryption process?
   Answer: Sub Byte, Shift Row, and Add round Key