Question 1: [9 Marks]

1) **MCQ:** Fill the table with your answers **(a, b, c, or d)**

1	2	3	4	5	6
b	b	a	d	c	a

1. Which of the following is considered a safeguard to confidentiality:

   a) Audit logs
   b) Data encryption
   c) Message digest
   d) None

2. Eavesdropping is considered attack to:

   a) Integrity
   b) Confidentiality
   c) Availability
   d) Accountability

3. An example of attack on data integrity is:

   a) Cracking
   b) Packet sniffer
   c) DOS
   d) Sync flooding

4. Man-in-the-middle attack is an example of threat on:

   a) Data Integrity
   b) Data availability
   c) Data authenticity
   d) All of the above

5. Each subject is granted the most restrictive set of permissions is a principle in computer security called:

   a) Need to Know
   b) Separation of Duties
   c) Least privilege
   d) Defense in Depth

6. It is a _____, when most of the employees in your company easily falling for phishing, smishing or other common attacks.

   a) Threat
   b) Risk
   c) Vulnerability
   d) None

2) **True/False Fill the following table with answers**

1	2	3	4	5	6
F	T	F	T	T	F

[1] Software complexity becomes higher and the attacks are getting harder.
[2] Authorization is one of information characteristic that has been added to CIA triad.
[3] Privacy is a property of data while confidentiality is a property of software system.
[4] The complement of CIA triad is disclosure, alteration and destruction.
[5] Prevention, detection , and recovery are the three main goals of information security.
[6] Direct attack is the one that originates from a compromised system.

3) **Analysis: Indicate which information security characteristic(s) has/have been violated (compromised) by ticking (×) the suitable cell(s).** (*Additional/wrong answers deduct marks*)

	Scenario	Confidentially	Availability	Integrity
[1]	Nada rewrites the magnetic stripe on a gift card to change the amount from $10 to $100.	X -0.25		X
[2]	Nora uses a key logger to capture her brother banking password.	X		
[3]	Sara disables her friend's router by logging in remotely with the manufacturer's default password.	-0.5	X	
[4]	Fact: In 2021, The personal information of 533 million Facebook users was found posted online by a hacker, including names, birthdays, phone numbers, locations, and email addresses.	X		
[5]	Heavy rain last week lead to difficulty in connecting to KSU network and services.		X	

Question 2: [6 Marks] 3.5

1) **Identify the encryption schema:** Fill the following table with answers **(4 Marks)**

	Case	Encryption	Key *Write **none** if no key is required* !
[1]	**Plain Text** SAVEYOURSELF **Ciphertext** FLESRUOYEVAS	Transposition Keyed	1 2 3 4 5 6 7 8 9 10 11 12 12 11 10 9 8 7 6 5 4 3 2 1
[2]	**Plain Text** DISCONNECTTHEPLUGSNOW **Ciphertext** DSONCTELGNWICNETHPUSO	transposition is left Jumbled Keyless X	none
[3]	**Plain Text** NEVERTRUSTINSECURITYBYOBSCURITY **Ciphertext** ARIREGEHFGVAFRPHEVGLOLBOFPHEVGL	mono (Shift)	K = 13
[4]	**Plain Text** 10100110111 **Ciphertext** 01011001000	Substitution mono replace	1 → 0 0 → 1 01 ← 1 10

E → R
R → E

2) **True/False Fill the following table with answers (5 Marks)** 4.5

1	2	3	4	5	6	7	8	9	10
T	T	T	T	F	F	F	F	F	T

[1] Vigenère is an example of polyalphabetic substitution cipher.
[2] The public-key cryptosystem uses the public key to encrypt the message at the sender's side, while in the digital signature schema, the public key is used to verify the signature at the receiver's side.
[3] The idea behind asymmetric algorithms is using OWF which is easy to compute and difficult to reverse.
[4] Random number generators are useful for cryptography.
[5] Mono-alphabetic substitution ciphers do not preserve the language features.
[6] "Next-bit" test for cryptographically secure PRNG states that given sequences from bits $k+1$ on, it should be difficult to predict earlier bits.
[7] Asymmetric algorithms are developed to substitute the symmetric ones as the asymmetric algorithms solve most of the security and practical issues exist in the symmetric ones.
[8] Security of ElGamal is based on the problem of factoring two numbers.
[9] Diffie-Hellman is an encryption protocol that encrypts the exchanged messages using a shared secret key.
[10] Number of keys need to publish for public-key cryptographic system for n users is n keys.

3 users
3 Public key 3 Private

3) Analysis: Answer the following questions: **(3 Marks)** 3 :)

Deena is setting up the RSA key pair. She has selected p=3 and q=23:

a) What is n?

$n = p \times q$
$= 3 \times 23 = 69$

b) What is $\Phi(n)$?

$\phi(n) = (p-1)(q-1) = 2 \times 22 = 44$

c) She has picked e=3, Which of the following would work for **d: 7, 15, 29**? Why? (*Show all the calculation for all of three possible values of d)*

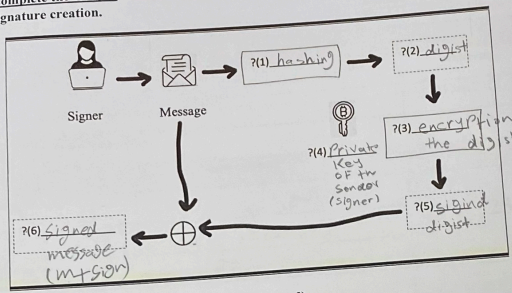
Value of *d*	valid/not valid	Why? (computations)
$d = 7$	not Valid	$d = e^{-1} \bmod \phi(n)$ $d * e = 1 \bmod \phi(n)$ $7 \times 3 = 1 \bmod 44$ 44 ⟌ 21 the remider = 21 should not 1
$d = 15$	Valid	$d * e = 1 \bmod \phi(n)$ $15 \times 3 = 1 \bmod 44$ the remider = 1 44 ⟌ 45 1 → remainder
$d = 29$	not Valid	$d * e = 1 \bmod \phi(n)$ $29 \times 3 = 1 \bmod 44$ the remiander = 43 it should not 1 44 ⟌ 87 43

d) What would be the public values for Deena and what should be kept private?

Public = (e, n) = (3, 69)
Private = (d, n) = (15, 69)

Question 3: [4 Marks]

4) **Complete the Graph:** **Fill in the missing parts to show the complete processes of the digital signature creation.** **(1.5 Marks)**



5) **MCQ:** Fill the table with your answers **(a, b, c, or d)**

7	8	9	10	11
a	b	c	d	b

7. Electronic files that are used to uniquely identify people and resources over the internet:
   a) Digital signature
   b) Digital certificate
   c) Encryption recourse
   d) None

8. An electronic file that uniquely identifies websites on the internet and enables secure, confidential communications.
   a) Digital signature
   b) Digital certificate
   c) Encryption
   d) Firewalls

9. What is the name of the issuer of public key infrastructure certificates?
   a) X.509
   b) Public key authority
   c) Certificate authority
   d) None

10. During digital signature verification process, the receiver uses _____
    e) The private key of the sender
    f) The public key of the receiver
    g) The public key of the sender
    h) The private key of the receiver

11. One issue of Kerberos protocol is:
    a) Need a key distribution protocol
    b) Need a key each time the client communicate with the server
    c) Single point of failure
    d) Not useful inside organizations

Table you might need:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25