Please fill out the next table with your answers of Part1:

Q. No.	Chosen Answer	Q. No.	Chosen Answer	
1	c	7	b	
2	c	8	b	
3	b	9	a	
4	c	10	a	
5	a	11	b	Total
6	b	12	b	5

Part1. Choose the correct answer (6 pts: 0.5 each).

LO1.1:1) The number of symmetric keys required for a team of 4 members to establish a pair-wise secure channel is: $\frac{4(4-1)}{2}$

a) 16
b) 8
c) 6 ✓
d) 20

LO1.1: 2) An attacker creates counterfeit objects; this threat is?

a) Interruption
b) Interception
c) Fabrication ✓
d) Modification

LO1.1: 3) Organized, directed and silent are characteristics of which threat:

a) Benign threat
b) APT ✓
c) Natural causes threat
d) Impersonation

LO1.1: 4) To ensure confidentially of messages using Asymmetric cryptography. You need to use ..... for encryption and ..... decryption?

a) The recipient's Public key, recipient's Private key
b) The sender's Private keys, The senders Public key
c) The recipient's Public key, sender's Private key ✓
d) The sender's Private keys, The senders Public key

A ✗

LO1.1: 5) Choose the False statement about Federated Identity management:

a) Requests an additional individual authentication ✓
b) Replaces authentication in all other systems
c) Unifies the authentication process for a group of systems
d) Maintains one profile with one authentication method ✓

LO1.1: 6) The number of possible passwords of length 3 using (English capital letters, decimal digits and $) is:

a) 36^3
b) 37^3
c) $37 \times 36 \times 35$
d) $26 \times 10 \times 1$

LO1.2: 7) Given the following Diana's certificate. To verify the certificate, you computed the hash value of Diana's public key and you got CA332. This means that:

Name: Diana Position: Division Manager Public key: 17EF83CA ...	hash value 128C4

a) Diana's public key is wrong and has been modified
b) You used the wrong private key to decrypt the signature
c) Diana's private key is wrong and has been modified
d) None of the above

LO1.2: 8) Hash function should be one-way so……:

a) The attacker could not change the input and regenerate the hash value
b) The attacker could not recover the list of inputs that generate the same hash value
c) The attacker could not modify the hash value
d) The attacker could not try different messages that generate the same hash value

LO1.2: 9) The attack model where the cryptanalyst has the exact copy of the plaintext and ciphertext is:

a) Known plaintext
b) Ciphertext only
c) Probable plaintext
d) Chosen plaintext

LO1.2: 10) One generated half of the encryption algorithm of DES can be expressed as:

a) $R_j = L_{j-1} \oplus f(R_{j-1}, k_j)$
b) $R_{j-1} = L_{j-1} \oplus f(R_{j-1}, k_j)$
c) $L_j = R_j \oplus f(R_{j-1}, k_j)$
d) $L_j = L_{j-1} \oplus f(R_j, k_j)$

LO2.2: 11) ..... states that programs and users be given just enough privileges to perform their tasks.

a) Principle of operating system privilege
b) Principle of least privilege
c) Principle of process scheduling privilege
d) Principle of access control privilege

LO2.2: 12) A system with a large number of users should implement …….. as an access control:

a) Access control directory
b) Access control list
c) Privilege list
d) Capability

Part2. Matching Questions (1 pts each).

LO1.1: 13) Match the security term with its definitions:

Interception
Interruption

a) Prevent authorized access
b) Prevent denying sending data
c) Unauthorized viewing
d) Create false data

interception (c)
interruption (a)

LO1.1: 14) Match the example with the violated security goal:

1-Alice knew that Bob has a file named "Project1.pdf" in his device

2-Alice blocked Bob from accessing his email by entering many wrong passwords

a) Availability
b) Integrity
c) Confidentiality

Part3. Short Answer Questions (1 pts each).

LO1.2: 15) What is the appropriate encryption algorithm for the following purposes:

(Hint: consider all types of ciphers)

a) To send a live streaming video

stream chiper

b) To distribute the secret key

RSA

LO1.2: 16) Assume there is a cipher called ARX that takes 1 GB of plaintext and generates a 2 GB ciphertext.

Is this a good cipher, explain your answer?

not good

becuse The ciphertext large Then Plaintext

العددين أختلفة

ولازم عددهم يكون واحد

LO1.2: 17) Suppose you intercept these two ciphertexts C1 and C2.

a- What do you learn from these ciphertext blocks?

b- Name the cipher used to generate these ciphertexts? DES

C1= FFA10C	KS4R!C	5OPWE
C2= ABC44#	KS4R!C	RT23!S

a)

same words becuse the cipher text similrate

a)DES

b)The same plaintext blocks encrypted

LO2.2: 18) Specify the type of controls used in each of the following examples:

a) **Placing your PC in a locked room, every time you leave Home.**

Physical control ✓

b) **Turning on the firewalls every time you use a public network.**

Tehqhical control ✓

LO2.2: 19) Name the following attacks:

a) **An attacker computes a list of common passwords' hash functions to use later.**

Rinbow Table ✓

b) **An attacker collects personal information about users to attack their passwords.**

inferaring ✓

LO2.2: 20) A failure occurs on one of the Amazon website servers.
As a website administrator, you need to know the last user who accesses the server and causes the problem.
How can you know that?

audit Loging ✓

LO2.2: 21) Given these RSA parameters: p=18 , q=29 , n=522

Are they valid parameters? explain why.

Not valid

becuse 18 not prime number