University Djilali Bounaama of Khemis Miliana

Department of Computer Science

L3 - Computer Systems (S6) - 2025/2026

Subject: Computer Security

Pre-Course Glossary

1	**Cybersecurity**	The practice of protecting computer systems, networks, and data from attacks and unauthorized access
2	**Information System**	A combination of hardware, software, data, and users that processes and stores information
3	**Asset**	Anything of value that needs protection, such as data, servers, or network infrastructure
4	**Threat**	A potential cause of harm to a system or organization (e.g., hacker, malware, natural disaster)
5	**Vulnerability**	A weakness in a system that can be exploited by a threat
6	**Risk**	The likelihood and impact of a threat exploiting a vulnerability
7	**Attack**	A deliberate attempt to compromise the security of a system
8	**Malware**	Malicious software designed to damage, disrupt, or gain unauthorized access to systems
9	**Virus**	Malware that attaches to legitimate programs and spreads when they are executed
10	**Worm**	Malware that spreads automatically across networks without user interaction
11	**Trojan horse**	Malware disguised as legitimate software that performs malicious actions
12	**Confidentiality**	Ensuring that information is accessible only to authorized users
13	**Integrity**	Ensuring that data is accurate and has not been altered without authorization
14	**Availability**	Ensuring that systems and data are accessible when needed
15	**Authentication**	The process of verifying the identity of a user or system
16	**Authorization**	The process of granting or denying access to resources after authentication
17	**Access control**	Mechanisms used to restrict access to systems and data
18	**Encryption**	The process of converting data into a secure, unreadable form to protect confidentiality
19	**Decryption**	The process of converting encrypted data back into its original form
20	**Cryptographic Key**	A secret or public value used in encryption and decryption
21	**Hash function**	A function that converts data into a fixed-length value for integrity verification
22	**Digital signature**	A cryptographic mechanism used to verify authenticity, integrity, and non-repudiation
23	**Firewall**	A security device or software that controls network traffic based on rules
24	**IDS**	Intrusion Detection System: A system that monitors networks or systems for suspicious activity
25	**DoS**	Denial of Service: An attack that aims to make a system or service unavailable
26	**Phishing**	A social engineering attack that tricks users into revealing sensitive information
27	**Social engineering**	Manipulating people into performing actions that compromise security
28	**Offensive security**	The practice of testing systems by simulating attacks to find vulnerabilities
29	**Defensive security**	The practice of protecting systems, detecting attacks, and responding to incidents
30	**Countermeasure**	A technical or organizational action taken to reduce security risks
31	**IPS**	A security system that monitors network traffic and blocks or prevents detected attacks in real time
32	**Eavesdropping**	Unauthorized listening to private communications to obtain sensitive information without altering the data
33	**Sniffing**	A technique used to capture and analyze network packets as they travel across a network
34	**Monitoring**	Continuous observation of systems, networks, and logs to detect suspicious activity or security breaches
35	**Wiretapping**	Interception of communications over networks to listen/record data transmissions without authorization
36	**Rootkit**	Malware designed to hide malicious activity and provide attackers with privileged access to a system
37	**Defense-in-Depth**	A security strategy that uses multiple layers of protection
38	**Cipher**	An algorithm or method used to transform plaintext into ciphertext in order to protect information
39	**Ciphertext**	The encrypted and unreadable form of data produced after applying a cipher to plaintext
40	**Breach**	An incident in which security controls fail

University Djilali Bounaama of Khemis Miliana

Department of Computer Science

L3 - Computer Systems (S6) - 2025/2026

Subject: Computer Security

Quiz N° 01

Match each of the following concepts with the appropriate definition:

1)

A	Integrity	A	Ensures that the content of a communication or file is not accessible to third parties
B	Confidentiality	B	Guarantees the identity of a given entity or the origin of a communication or file
C	Authenticity	C	Ensures that the content of a communication or file has not been modified

2)

A	Cryptosystem	A	Encryption algorithm
B	Cipher program	B	Encrypted text
C	Cryptogram	C	Ciphergram

3)

A	Cryptanalysis	A	To transform plaintext messages into unreadable text
B	Ciphering	B	To analyze the encrypted messages in order to decrypt them
C	Decryption	C	To decode the encoded messages

4)

A	To encode	A	Letter-level substitution
B	To cipher	B	Word-level substitution
C	To Transpose	C	Sentence-level substitution

5)

A	Symmetric cryptography	A	It uses the same key to encrypt/decrypt
B	Secret-key cryptography	B	It uses two different keys to encrypt/decrypt
C	Asymmetric cryptography	C	It does not use secret conventions before exchanging secret messages

6)

A	Worm	A	Self-Replicate by inserting into hosts
B	Virus	B	Spread through the network
C	Trojan horse	C	Activity that appears legitimate but is malicious

7)

A	Detection	A	Create virtual disks
B	Prevention	B	Create a restore point
C	Recovery	C	Block/Delete suspicious connections/files
D	Filtering	D	Restore the last known good configuration

8)

A	Confidentiality breach	A	Log in with someone else's username and password
B	Integrity breach	B	Intercepting a secret communication
C	Authenticity breach	C	Modify the amount of a monetary transaction
D	Repudiation	D	Bombarding a server with TCP-SYN requests
E	Availability breach	E	Deny sending or receiving a message