University Djilali Bounaâma of Khemis Miliana
Department of Computer Science
L3 – Computer Systems-S6-(2025/2026)
Final Examination: Computer Security/Correction
May 2026

Correct: + 0.25 2 x Wrong = - 0.25

Circle the correct answers

(Wrong answers will be penalized)

1. Cybersecurity mainly deals with:
A. Only software protection
B. **Protection of systems and data**
C. Network cables only
D. **Reducing unauthorized actions**

2. Which can be considered an asset?
A. **Database**
B. **Server**
C. Malware
D. Virus

3. A threat can be:
A. A protection method
B. **A possible harmful event**
C. A vulnerability
D. A backup

4. A vulnerability:
A. Is always intentional
B. **Exists without attack**
C. Is a threat itself
D. Cannot be exploited

5. An attack is:
A. Always external
B. **Intentional action**
C. **Sometimes internal**
D. Always accidental

6. A virus usually:
A. **Needs execution**
B. Spreads alone always
C. Is harmless
D. Does not attach

7. A worm:
A. Needs user click
B. **Spreads via network**
C. **Self-replicates**
D. Looks legitimate

8. Trojan horse:
A. Is always visible
B. **Looks normal**
C. **Hides malicious actions**
D. Self-replicates

9. Confidentiality can be broken by:
A. DoS
B. **Sniffing**
C. **Eavesdropping**
D. Backup

10. Integrity relates to:
A. Data secrecy
B. **Data correctness**
C. Availability
D. Authentication

11. Availability is affected by:
A. Phishing
B. **DoS**
C. **Ransomware**
D. Encryption

12. Authentication:
A. Grants access
B. **Checks identity**
C. Logs activity
D. Encrypts data

13. Authorization may occur:
A. Before authentication
B. **After authentication**
C. Without identity
D. Only in networks

13. Firewall may:
A. Encrypt data
B. **Filter traffic**
C. Store passwords
D. Detect all attacks

14. IDS can:
A. Block attacks
B. **Detect anomalies**
C. Encrypt traffic
D. Replace firewall

15. IPS differs from IDS because it:
A. Only monitors
B. **Can block attacks**
C. Cannot detect
D. Is passive

The corrected version with a detailed grading scale will be published on http://intelligencedz.blogspot.com and elearning platform.

16. DoS attack aims to:
A. Modify data
B. **Disrupt service**
C. Steal passwords
D. Encrypt files

17. Phishing often:
A. Uses malware only
B. **Targets users**
C. **Tricks for information**
D. Uses firewall

18. Sniffing is:
A. Blocking packets
B. **Capturing traffic**
C. Encrypting messages
D. Deleting logs

19. Eavesdropping differs from sniffing because it:
A. Always modifies data
B. **Focuses on listening**
C. Encrypts data
D. Prevents attacks

20. Rootkit:
A. Detects malware
B. **Hides attacker presence**
C. Improves security
D. Is firewall

21. Defense-in-depth means:
A. One strong defense
B. **Multiple layers**
C. No redundancy
D. Over-encryption

22. Offensive security includes:
A. Monitoring logs
B. **Penetration testing**
C. **Ethical hacking**
D. Backup

23. Defensive security includes:
A. Attacking systems
B. **Detection**
C. **Response**
D. Ignoring threats

24. Which relate to confidentiality attacks?
A. **Sniffing**
B. **Phishing**
C. SQL injection
D. DoS

25. Which relate to integrity attacks?
A. Sniffing
B. Phishing
C. SQL injection
D. DoS

26. Which relate to availability attacks?
A. Sniffing
B. Phishing
C. SQL injection
D. DoS

27. Which are detection mechanisms?
A. Firewall
B. **IDS**
C. **Monitoring**
D. Encryption

28. Which statement is correct?
A. Encryption guarantees availability
B. IDS prevents all attacks
C. Worm needs host program
D. Firewall detects identity

Exercise 1 (5.5 pts): We aim to encrypt the word "WORLD" using RSA. The ASCII values of its letters are 87, 79, 82, 76, and 68, respectively.

Consider the following RSA configurations and encryption methods:

RSA Configuration	Encryption method
1) p = 5, q = 7, e = 5, d = 5 2) p = 3, q = 29, e = 5, d = 45 3) p = 17, q = 19, e = 5, d = 173	1) Letter by letter encryption using ASCII values 2) Encrypt the sum of ASCII values 3) Encrypt the sum (mod n)

Choose one RSA configuration and one encryption method to efficiently encrypt the word "WORLD".

Exercise 2 (4.5 pts): Use the following cipher table and the initialization vector (IV) to decrypt the bitstreams S1, S2, and S3. The bitstreams were encrypted using the PCBC, CFB, and CBC cipher modes, respectively. (Use diagrams to illustrate.)

Cipher Table		IV = 101
000 ⇒ 111	100 ⇒ 000	S1 = 111100111110
001 ⇒ 110	101 ⇒ 001	S2 = 100001011111
010 ⇒ 101	110 ⇒ 010	S3 = 111010011111
011 ⇒ 100	111 ⇒ 011	

Solution:

Exercise N°1:

Choice: Configuration 3 and method 1.

1) Method choice: **(0.75 pt)**

Letter by letter is more efficient in decryption. We can't encrypt using the sum (392) in this example because it is greater than any public n. We also can't encrypt using sum (mod n) because we will lose information of the initial word to encrypt, then we can't decrypt. The only valid method is Method 1.

2) Configuration choice: **(0.75 pt)**

Configurations 1 and 2 are not appropriate for the encryption of the word WORLD. In configurqtion 1 n = 35, and in configuration 2, n = 87, However, $0 \leq M < n$, which is not valid for all letters.

Conclusion: only configuration 3 and method 1 are valid for RSA encryption. **(01 pt)**

3) Encryption (Using modular exponentiation method):**(03 pts)**

C(W) = 87^5 (mod 323) = 83

C(O) = 79^5 (mod 323) = 129

C(R) = 82^5 (mod 323) = 233

C(L) = 76^5 (mod 323) = 247

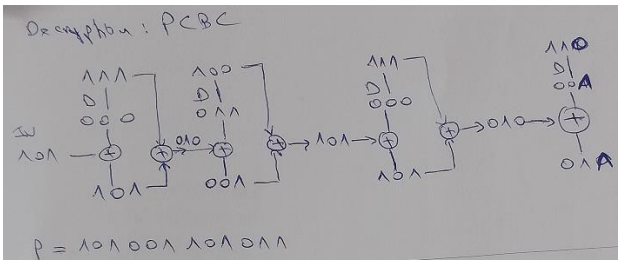
C(D) = 68^5 (mod 323) = 102

Cryptogram: 83, 129, 233, 247, 102

Exercise N°2:

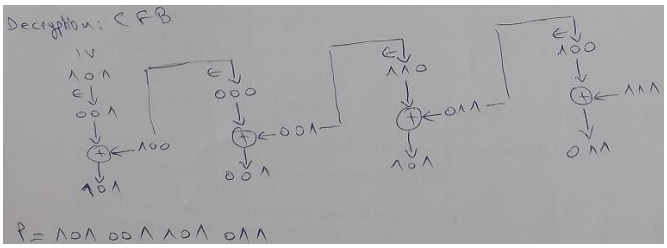
1) PCBC Decryption: (S1 = 111100111110)

⇒ Plaintext = 101001101011 **(1.5 pt)**



2) CFB Decryption: (S2 = 100001011111)

⇒ Plaintext = 101001101011 **(1.5 pt)**



3) CBC Decryption: (S3 = 111010011111)

⇒ Plaintext = 101001101011 **(1.5 pts)**