Université Libanaise
Faculté d'Information
Br I

الجامعة اللبنانية
كلية الاعلام
الفرع الاول

بتول حمية
9722

امتحان الفصل الثالث
للعام الجامعي 2025/2024

| | |
|---|---|
| المرحلة: اجازة | المادة: Data Security |
| السنة المنهجية: الثالثة | المدة:ساعة |
| الاستاذ: د. نادين زيبيب | الدورة: |

## Question I : choose the correct answer( s )

| | |
|---|---|
| **1. Which protocol is used to send emails?**<br>A. FTP<br>B. HTTP<br>C. SMTP<br>D. DNS | **6. Which protocol is connection-oriented and guarantees delivery of data?**<br>A. UDP<br>B. TCP<br>C. IP<br>D. ICMP |
| **2. Digital signatures are primarily used to ensure:**<br>A. Confidentiality<br>B. Integrity and authenticity<br>C. Faster encryption<br>D. Data compression | **7. In symmetric encryption, the key used for encryption is:**<br>A. Public<br>B. Private<br>C. The same for encryption and decryption<br>D. Different for encryption and decryption |
| **3. In asymmetric encryption, the key pair consists of:**<br>A. Two public keys<br>B. One key for encryption, one identical key for decryption<br>C. One public key and one private key<br>D. Two private keys | **8. What is the main purpose of public key cryptography?**<br>A. Speed up encryption<br>B. Secure communication without sharing a secret key in advance<br>C. Make decryption faster<br>D. Generate random numbers |
| **4. Which layer of the TCP/IP model is responsible for routing packets between networks?**<br>A. Application<br>B. Transport<br>C. Internet<br>D. Network Access | **9. In block cipher encryption, plaintext is divided into:**<br>A. Bits<br>B. Bytes<br>C. Fixed-size blocks<br>D. Streams of characters |
| **5. Which mode of operation ensures that identical plaintext blocks produce different ciphertexts using an IV?**<br>A. ECB<br>B. CBC<br>C. CFB<br>D. OFB | **10. Which protocol is responsible for delivering packets from the source to the destination IP address?**<br>A. TCP<br>B. UDP<br>C. IP<br>D. HTTP |

## Question II

1) What is the difference between passive and active security attacks?
2) List and briefly define categories of security services.

## Question III. CFB Mode with Bitwise Rotation Cipher

1- Give the encryption and decryption algorithms of this type.
2- Explain the operation of this mode and the difference with CBC.
3- Let **M = 1010110001101111011000101** is the plaintext. **Initialization Vector (IV): 01010101 and K = 3 (number of bits to rotate)** the key for permutation encryption method. **Notice if that there isn't a full bits in the last block of plaintext you should to alternate by a binary bit.** Determine the cipher text C.
4- Decrypt the cipher text C to obtain your plain text M.

## Question IV. Columnar Transposition

let's encrypt the message " **LEARN CRYPTOGRAPHY AND HAVE FUN**" using the keyword ***SECRET***.

1- Give the Ciphertext using columnar transposition Encryption
2- Verify your plaintext.

$$P_i = E_k(C_{i-1}) \oplus C_i$$