Data Science – Dr. Nadine Zbib
Duration: 2 hours

الجامعة اللبنانية
كلية الإعلام

Final – Data Security – 2024/2025
First Session

Exercise I: Short answers(20 pts)

1) What is the difference between passive and active security attacks?
2) List and briefly define categories of security services.
3) In CBC-mode encryption, if a single bit of the plaintext is changed, which ciphertext blocks are affected (assume the same IV is used)?
4) In CBC-mode decryption, if a single bit of the ciphertext is changed, which plaintext blocks are affected?

Exercise II. Asymmetric Encryption 'RSA' (30 pts)

Asymmetric key encryption uses different keys for encryption and decryption. These two keys are mathematically related and they form a key pair. One of these two keys should be kept private, called private-key, and the other can be made, called public-key. Popular private-key algorithm is RSA (invented by Rivest, Shamir and Adlemen). The public key is (n, e) and the private key is (n,d).
Suppose you want to exchange data by using the RSA algorithm. By choosing p = 17, q = 13:

1. Compute n and z.
2. Which of the following values: e=35, e=27 and e=33 is the best suitable for encrypting? Justify.
3. User B want to send you the message m=78. Determine the cipher text C resulting from encryption of the message m. $78^{35} \bmod 221$
4. In order to decrypt the cipher text C and obtain the same initial message m sent by the user B, e and d must verify the relation: ed=1 mod(z).
   Which of the following values, d=13, d=11 and d=9, is the best suitable for d? Justify.
5. Decrypt the cipher text C.

Exercise IV. CFB: Cipher FeedBack (25 pts)

1- Give the encryption and decryption algorithms of this type.
2- Let **K = 1100 0001 0000** the key for permutation encryption method, **M = 1001 1 001 11 00 100 0 0001 10100 00010 01010** is the plaintext. **Notice if that there isn't a full 12 bits in the last block of plaintext. To resolve this problem, we will use padding. We will alternate 1's and 0's until a complete block is made.** Determine the cipher text C.
3- Decrypt the cipher text C to obtain your plain text M.

Exercise V. Hash (25 pts)

1. What is a hash in cryptography?
2. What is the role of a compression function in a hash function?
3. What is cryptography hash function?
4. What are the applications of cryptographic hash function?
5. Describe Secure hash Algorithm in detail.