Data Science – Dr. Nadine Zbib
Duration: 2 hours

الجامعة اللبنانية
كلية الإعلام

Final – Data Security – 2024/2025
First Session

Exercise 1: Multiple choice (20 pts)

1. Which of the following is an **asymmetric encryption algorithm**?
   a) AES
   b) DES
   c) RSA
   d) Blowfish
2. In RSA, the **public key** is composed of:
   a) (p, q)
   b) (d, n)
   c) (e, n)
   d) (p, e)
3. What is the main purpose of a **hash function**?
   a) Encrypt data
   b) Decrypt data
   c) Ensure data integrity
   d) Compress files
4. Which property ensures that a hash value **cannot be reversed** to get the original message?
   a) Collision resistance
   b) Determinism
   c) One-way property
   d) Avalanche effect
5. CFB (Cipher Feedback Mode) is used with:
   a) Asymmetric ciphers
   b) Block ciphers
   c) Hash functions
   d) Digital signatures
6. In CFB mode, encryption turns a block cipher into:
   a) A hash function
   b) A stream cipher
   c) A public-key cipher
   d) A signature algorithm
7. You are creating a number of user objects for a team of your organization's temporary workers. They will work daily from 9:00 A.M. to 5:00 P.M. on a contract that is scheduled to begin in one month and end two months later. They will not work outside of that schedule. Which of the following properties should you configure initially to ensure maximum security for the objects?
   i. Password
   ii. Account Expires
   iii. Account Is Trusted For Delegation
   iv. Password Never Expires
8. Which of the following is true about Public Key Infrastructure?
   i. PKI is a combination of digital certificates, public-key cryptography, and certificate authorities that provide enterprise wide security.

ii. PKI uses two-way symmetric key encryption with digital certificates, and Certificate Authority.
iii. PKI uses private and public keys but does not use digital certificates.
iv. PKI uses CHAP authentication.

9. What are the three fundamental principles of security?
   i. Accountability, confidentiality, and integrity
   ii. Confidentiality, integrity, and availability
   iii. Integrity, availability, and accountability
   iv. Availability, accountability, and confidentiality
10. Making sure that the data is accessible when and where it is needed is which of the following?
   i. Confidentiality
   ii. integrity
   iii. acceptability
   iv. availability

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 = 7, q = 13:

1. Compute n and z.
2. Which of the following values: e=2, e=3 and e=5 is the best suitable for encrypting? Justify.
3. User B want to send you the message m=10. Determine the cipher text C resulting from encryption of the message m.
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=26, d=27 and d=29, is the best suitable for d? Justify.
5. Decrypt the cipher text C.

Exercise III. CFB: Cipher FeedBack (25 pts)

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

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

1- Give the encryption and decryption algorithms of this type.
2- Let **IV = 110000010000** the key for permutation encryption method, **M = 10011 00111 00100 00001 10100 00010 01010 is** the plaintext. The used key will be to reverse the block. **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 IV. Hash (25 pts)

1- Define **collision resistance**.
2- Explain why **salted hashing** is used in password storage.
3- A system uses **SHA-1** to verify file integrity.
   a) Is this secure? Why or why not?
   b) Suggest a better alternative.