ata Science – Dr. Nadine Zbib
uration : 2 hours – Open Book

الجامعة اللبنانية
كلية الإعلام

Final – Data Security – 2022/2023
First Session

ercise I: choose the correct answer(s): (10 points)

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

Which of the following are characteristics of a strong password?

i. Is at least seven characters' long
ii. Contains your user name
iii. Contains keyboard symbols
iv. Contains a dictionary word

3) From which tab on a user's Properties dialog box can you set logon hours?

i. General tab
ii. Account tab
iii. Profile tab
iv. Security tab

4) The name you select for a group to use a common machine is called?

i. tree
ii. domain
iii. site
iv. OU

) Plaintext is the

i. the scrambled message produced as output
ii. original message or data that is fed into the algorithm as input
iii. private secret key
iv. public sharing key

) A user has forgotten his or her password and attempts to log on several times with an incorrect password. Eventually, the user receives a logon message indicating that the account is either disabled or locked out. The message suggests that the user contact an administrator. What must you do?

i. Delete the user object and re-create it
ii. Rename the user object
iii. Enable the user object
iv. Reset the password for the user object

7) 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.

8) 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

9) Which of the following prevents, detects, and corrects errors so that the integrity, availability, and confidentiality of transactions over networks may be maintained?

i. Communications security management and techniques
ii. Networks security management and techniques
iii. Clients security management and techniques
iv. Servers security management and techniques

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: Short answers:

1) *What is the difference between passive and active security attacks?* (10 pts)
2) *List and briefly define categories of security services.* (10 pts)

Exercise III. 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 IV. CBC: Cipher Block Chaining (40 pts)

1- Give the encryption and decryption algorithms of this type.

2- Explain the operation of this mode.

3- Let **K = 110000010000** the key for permutation encryption method, **M = 10011 00111 00100 00001 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.

4- Decrypt the cipher text C to obtain your plain text M.