University of Jordan

Computer Engineering Department

Information and network security

First exam date: 6 April 2023

Name: Number:

Which of the following is a block cipher?

DES
3-DES
AES
All of the above
None of the above

Message authentication provides mainly:

Confidentiality
Integrity
Availability
All of the above

Ali and Ahmad are friends. Ali sends a signed message to Ahmad.

Describe the operations that Ali has undertaken to do that.

How many keys are used in creating a digital envelope? What are they? What is the purpose of each key?

Active attacks can harm:

Confidentiality
Integrity
Availability
All of the above
None of the above

The most commonly used symmetric encryption is:

DES
3-DES
AES
SES

Ali and Ahmad are friends. Ali sends a signed message to Ahmad.

Describe the operations that Ahmad has to undertake to authenticate the source of the message.

What are the main components of a digital certificate?

(2) 1) key information
2) User ID
3) Certificate Authority information

What happens first, authorization or authentication?

Authorization
Authentication
Authorization and authentication are the same
None of the mentioned

Which of the following does authorization aim to accomplish?

Restrict what operations/data the user can access
Determine if the user is an attacker
Flag the user if he/she misbehaves
Determine who the user is
None of the above

Which of the following is an authentication method?

Secret question
Biometric
Password
SMS code
All of the above

Assume password authentication.

Describe the protocol of a secure remote log-in.

(2) 1) the user sends a request to the host
2) the host replies with random number "r", h() and f()
3) then the user assigns his Password with the hash function and f() → f(r, h(P'))
.. the host compares the received f(r, h(P')) with the f(r, h(P)) stored.

Why is one-time password safe?

It is easy to generate

It cannot be shared

It is different for every access

It is a complex encrypted password

Which of the following does authentication aim to accomplish?

Restrict what operations/data the user can access

Determine if the user is an attacker

Flag the user if he/she misbehaves

Determine who the user is

None of the above

In role-based access control, each user is assigned one or more roles, and the roles determine which parts of the system the user is allowed to access.

True
False

Stream cipher encryption encrypts data:

One bit at a time
One byte at a time
One block at a time
Only a and b
All of the above

Which of the following cannot be used in digital signatures?

RSA
Diffie-Hell man
DSS
Elliptic Curve

Digital signature can be achieved by:

Stream cipher
Block cipher

4

Symmetric encryption
Public key encryption

Public Key encryption is stronger than symmetric key encryption

True
False

Hashing provides:

Data integrity
Data confidentiality
Data availability
All of the above
None of the above

Encryption provides:

Data integrity
Data confidentiality
Data availability
All of the above
None of the above

For the next two questions assume statistical biometric authentication method.

Description: The profiles of the biometric characteristic indicate that the average matching value of the genuine user is less than the average matching value of the imposter with some overlap of the probability density function

The effect of increasing the decision threshold on the false match possibility will:

Increase
Decrease
Does not change
None of the above

The effect of increasing the decision threshold on the false non-match possibility will:

Increase
Decrease
Does not change
None of the above

Biometric authentication system can be used for verification and/or identification.

What is the aim of each procedure?

(2) identification → identify if the user is enrolled in the system (user identified or not)

verification → verify that the given ID from the user is related to his biometric access type (takes the ID and biometric as inputs and compares them)