1. Modify the following texts so that the statements are true.

One of the major problems with cryptography is the process of transferring keys to the recipient.

encryption be used to create digital signature.

encryption be used to create digital signature.

When operation mode is applied, the plaintext structural information is exposed.

When CBC operation mode is applied, there limited error propagation

limited.

In the case of errors in ciphertext, when operation mode is used, these errors in the obtained plaintext.

In the case of errors in ciphertext, when operation mode is used, these errors in the obtained plaintext.

In the case of errors in ciphertext, when operation mode is used, these errors in the obtained plaintext.

1. Assign the terms from the left column to the corresponding definitions on the right.

**7**

**6**

**5**

**4**

**3**

**2**

**1**

uses a keystream generated independently of the plaintext and of the ciphertext

Symmetric key cryptography

can be symmetric-key or

public-key algorithms

Stream cipher

Stream cipher

can offer separately data

confidentiality or authentication

are always symmetric-key algorithms

uses a keystream that depends on the ciphertext

operates with a time-varying transformation on individual digits of the plaintext

Block cipher

Self-synchronizing stream cipher

Public key cryptography

always offers at the same time data confidentiality or authentication

**5**

**4**

**7**

**2**

**6**

**3**

**1**

Synchronous stream cipher

1. Mark the true statements.

□ The digital signature only depends on the authors, it does not depend on the message.

x The digital signature must use some information unique to the sender, to prevent both forgery and denial.

x The output of a hash function has a fixed length.

□ Given a message, it is easy to find its hash and viceversa.

x It is computationally infeasible to find two distinct messages that hash to the same result

□ Different messages always have different hash values.

1. Classify the following attacks as active or passive.

Eavesdropping, masquerade, traffic analysis, replay, denial of service, modification

|  |  |
| --- | --- |
| Active | masquerade, replay, denial of service, modification |
| Passive | eavesdropping, traffic analysis |

1. Fill the numbers of correct statements concerning digital certificates in the following table.

|  |
| --- |
| 2 |
| 4 |
|  |
|  |
|  |

**1** – A digital certificate contains the secret key of a subject or certificate holder, as well as the identification data of the certificate holder

**2** – Digital certificates are signed with the private key of a certification authority (CA).

**3** – Only the secret key certified by the certificate will work with the corresponding public key possessed by the entity identified by the certificate.

**4** – Digital certificates binds together a public-key with an identity.

**5** – A digital certificate contains the public key of the corresponding certification authority (CA)