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

One of the major problems with $\begin{pmatrix}\text{symmetric}\\ \text{public key}\end{pmatrix}$ cryptography is the process of transferring keys to the recipient.

$\begin{pmatrix}\text{Symmetric}\\ \text{Public key}\end{pmatrix}$ encryption $\begin{pmatrix}\text{can}\\ \text{cannot}\end{pmatrix}$ be used to create digital signature.

When $\begin{pmatrix}\text{ECB}\\ \text{CBC}\end{pmatrix}$ operation mode is applied, the plaintext structural information is exposed.

When CBC operation mode is applied, there $\begin{pmatrix}\text{is}\\ \text{is not}\end{pmatrix}$ limited error propagation
limited.

In the case of errors in ciphertext, when $\begin{pmatrix}\text{CFB}\\ \text{OFB}\\ \text{CTR}\end{pmatrix}$ operation mode is used, these errors $\begin{pmatrix}\text{are propagated}\\ \text{are not progatated}\end{pmatrix}$ in the obtained plaintext.

Erasmus+
This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

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

Symmetric key cryptography	uses a keystream generated independently of the plaintext and of the ciphertext
Stream cipher	can be symmetric-key or public-key algorithms
Stream cipher	can offer separately data confidentiality or authentication
Block cipher	are always symmetric-key algorithms
Self-synchronizing stream cipher	uses a keystream that depends on the ciphertext
Synchronous stream cipher	operates with a time-varying transformation on individual digits of the plaintext
Public key cryptography	always offers at the same time data confidentiality or authentication

Erasmus+
This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

3. Mark the true statements.

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

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

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

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

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

☐ Different messages always have different hash values.

---

4. Classify the following attacks as active or passive.

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

Active	
Passive	

---

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

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)

Erasmus+
This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.