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

The sender and the receiver do not need to share any secret keys when (symmetric / public key) is used.

In order to verify a digital signature, it is needed the (private key of the signer / public key of the signer / private key of the receiver / public key of the receiver).

The key length in symmetric ciphers is (shorter / longer) than in public key ciphers.

In symmetric cipher, the encryption process is (slower / faster) than in public key ciphers.

(Symmetric / Public key) encryption uses (the same key / different keys) for encryption and decryption.

In hybrid encryption, the user data is ciphered using (symmetric / public key) algorithms.

In hybrid encryption, the (private key of the sender / public key of the sender / private key of the receiver / public key of the receiver) is used for encryption of (user data / session key).

---

**2. Mark the true statements.**

☐ The digital signature must be a bit pattern that depends on the message being signed.

☐ The realization and implementation of the digital signature must be relatively easy without the signer private key.

☐ The forgery of the digital signature must be computationally infeasible, either by constructing a new message for an existing digital signature or by constructing a fraudulent digital signature for a given message.

☐ Given a digital signature, it is possible to find the message.

☐ The public key of the signer is required to verify her digital signature.

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. Assign the terms from the left column to the corresponding properties on the right (one or more).**

| | |
|---|---|
| Digital certificates | prevent the use of fake public keys for impersonation |
| | incorporates a digital signature |
| | does not use any key |
| | are one-way functions |
| Hash functions | are useful for key exchange |
| | binds together a public-key with an identity |
| | do not include any time reference |

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.

**4. Fill the numbers of correct statements concerning attack mechanisms in the following table.**

| |
|---|
| |
| |
| |
| |
| |

**1** – Traffic analysis refers to the process of intercepting and examining messages in order to deduce information from patterns in communication.

**2** – Host attacks refers to all types of attacks intended to overwhelm a computer or a network in such a way that legitimate users of the computer or network cannot use it.

**3** – Protocol-based attacks, which take advantage of known (or unknown) weaknesses in network services.

**4** – In Man in the Middle (MitM) attacks, the intruder intercepts communications between two parties, usually an end user and a website.

**5** – Denial of service attacks take advantage of vulnerabilities of the victim computer operating systems or in how the system is set up and administered.

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.