

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 $\left(\begin{smallmatrix} \text{symmetric} \\ \text{public key} \end{smallmatrix} \right)$ is used.

In order to verify a digital signature, it is needed the $\left(\begin{smallmatrix} \text{private key of the signer} \\ \text{public key of the signer} \\ \text{private key of the receiver} \\ \text{public key of the receiver} \end{smallmatrix} \right)$.

The key length in symmetric ciphers is $\left(\begin{smallmatrix} \text{shorter} \\ \text{longer} \end{smallmatrix} \right)$ than in public key ciphers.

In symmetric cipher, the encryption process is $\left(\begin{smallmatrix} \text{slower} \\ \text{faster} \end{smallmatrix} \right)$ than in public key ciphers.

$\left(\begin{smallmatrix} \text{Symmetric} \\ \text{Public key} \end{smallmatrix} \right)$ encryption uses $\left(\begin{smallmatrix} \text{the same key} \\ \text{different keys} \end{smallmatrix} \right)$ for encryption and decryption.

$\left(\begin{smallmatrix} \text{Symmetric} \\ \text{Public key} \end{smallmatrix} \right)$ encryption uses $\left(\begin{smallmatrix} \text{the same key} \\ \text{different keys} \end{smallmatrix} \right)$ for encryption and decryption.

In hybrid encryption, the user data is ciphered using $\left(\begin{smallmatrix} \text{symmetric} \\ \text{public key} \end{smallmatrix} \right)$ algorithms.

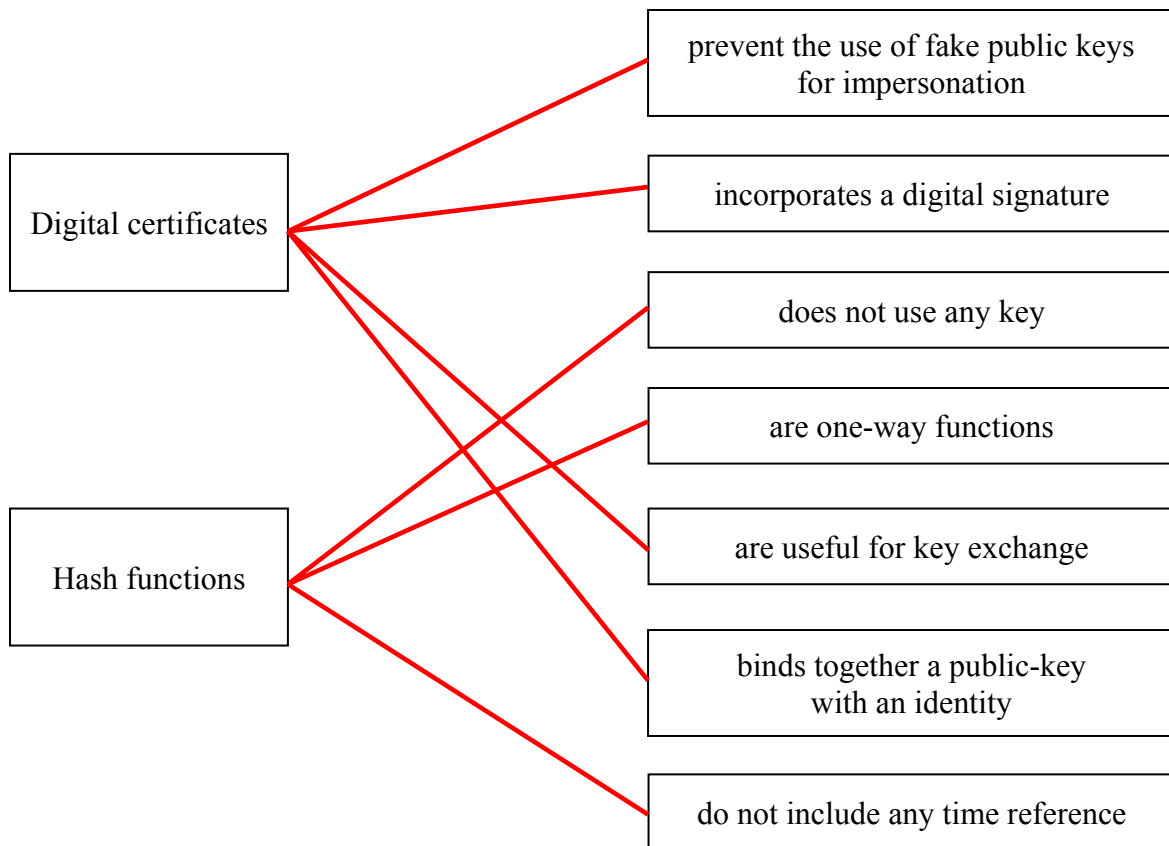
In hybrid encryption, the $\left(\begin{smallmatrix} \text{private key of the sender} \\ \text{public key of the sender} \\ \text{private key of the receiver} \\ \text{public key of the receiver} \end{smallmatrix} \right)$ is used for encryption of $\left(\begin{smallmatrix} \text{user data} \\ \text{session key} \end{smallmatrix} \right)$.

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.



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



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

1
3
4

- 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.

