WORKSHEET C2/1

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

Availability	Ability to detect a change in the transmitted or stored data
Authentication	A person involved in some communication cannot deny this involvement later
Secrecy	Process verifying the identity of a person or a program that I want to communicate with
Integrity	Ability of an information system to ensure that information is available to authorized users when they need it
Access control	Information is encrypted and only an authorized subject can access it
Non-repudiation	This service checks and determines who can access which resources

Lifelong Learning Programme

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.

WORKSHEET C2/1

2. Encrypt and decrypt a text using a conversion table (so-called substitution cipher).

plaintext alphabet	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
ciphertext alphabet	Z	V	I	R	E	A	B	C	D	F	G	H	J	K	L	M	N	O	P	Q	S	T	U	W	X	Y

Encrypt the text (quoting Jan Werich – famous Czech writer, actor etc.):

WHERE IS AN IDIOT THERE IS DANGER

Decrypt the text:

QCDP IDMCEO DP JLOE QCZK QUL QCLSPZKR XEZOP LHR

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

One of the characteristic properties of $\begin{pmatrix}\text{symmetric}\\\text{asymmetric}\end{pmatrix}$ ciphers is $\begin{pmatrix}\text{long}\\\text{short}\end{pmatrix}$ key.

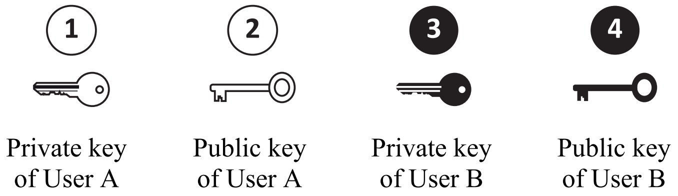
$\begin{pmatrix}\text{Symmetric}\\\text{Asymmetric}\end{pmatrix}$ encryption is ____ times $\begin{pmatrix}\text{faster}\\\text{slower}\end{pmatrix}$ than $\begin{pmatrix}\text{symmetric}\\\text{asymmetric}\end{pmatrix}$ encryption.

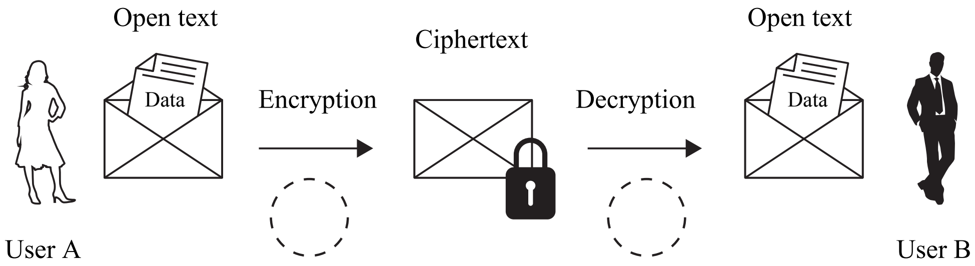
$\begin{pmatrix}\text{Symmetric}\\\text{Asymmetric}\end{pmatrix}$ encryption $\begin{pmatrix}\text{can}\\\text{cannot}\end{pmatrix}$ be used to create digital signature.

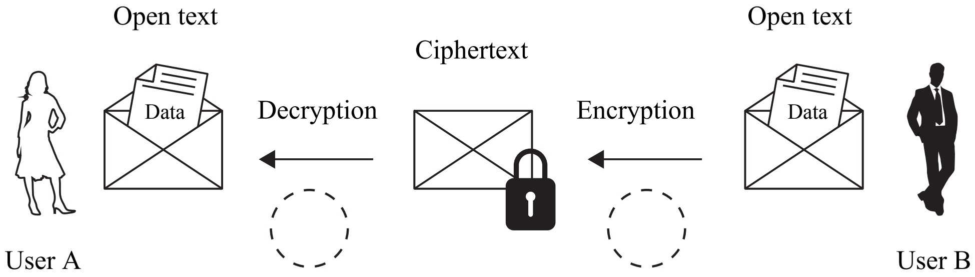
Lifelong Learning Programme

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.

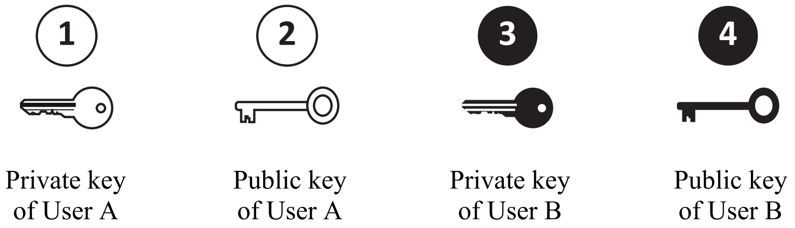
4. **In the following picture mark the correct keys to be used when the communicating parties want to use asymmetric cipher for secure transmission of a document.**

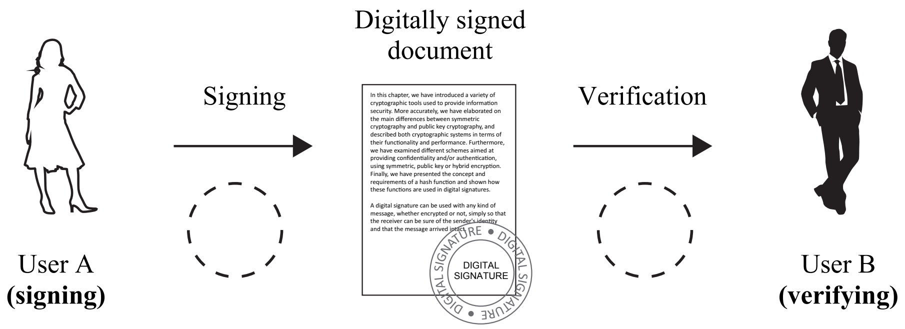






5. **In the following picture mark the correct keys to be used for when digital signature should be created and verified.**





In this chapter, we have introduced a variety of cryptographic tools used to provide information security. More accurately, we have elaborated on the main differences between symmetric cryptography and public key cryptography, and described both cryptographic systems in terms of their functionality and performance. Furthermore, we have examined different schemes aimed at providing confidentiality and/or authentication, using symmetric, public key or hybrid encryption. Finally, we have presented the concept and requirements of a hash function and shown how these functions are used in digital signatures.

A digital signature can be used with any kind of message, whether encrypted or not, simply so that the receiver can be sure of the sender's identity and that the message arrived intact.

Lifelong Learning Programme

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.

6. Fill the numbers of correct statements concerning hash functions in the following table.

Hash function characteristics include:

1 – The minimum length of the input must be 1024 bits
2 – The output length is variable
3 – The output length is constant
4 – The inverse hash function can be used to retrieve the original data
5 – Two different input messages always produce different outputs (so-called hash)
6 – Hash function is today commonly used to create digital signatures
7 – Hash function is today commonly used to encrypt data
8 – Its purpose is to produce a unique output from a unique input message

7. Modify the following text so that the statement is true.

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

Lifelong Learning Programme

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.