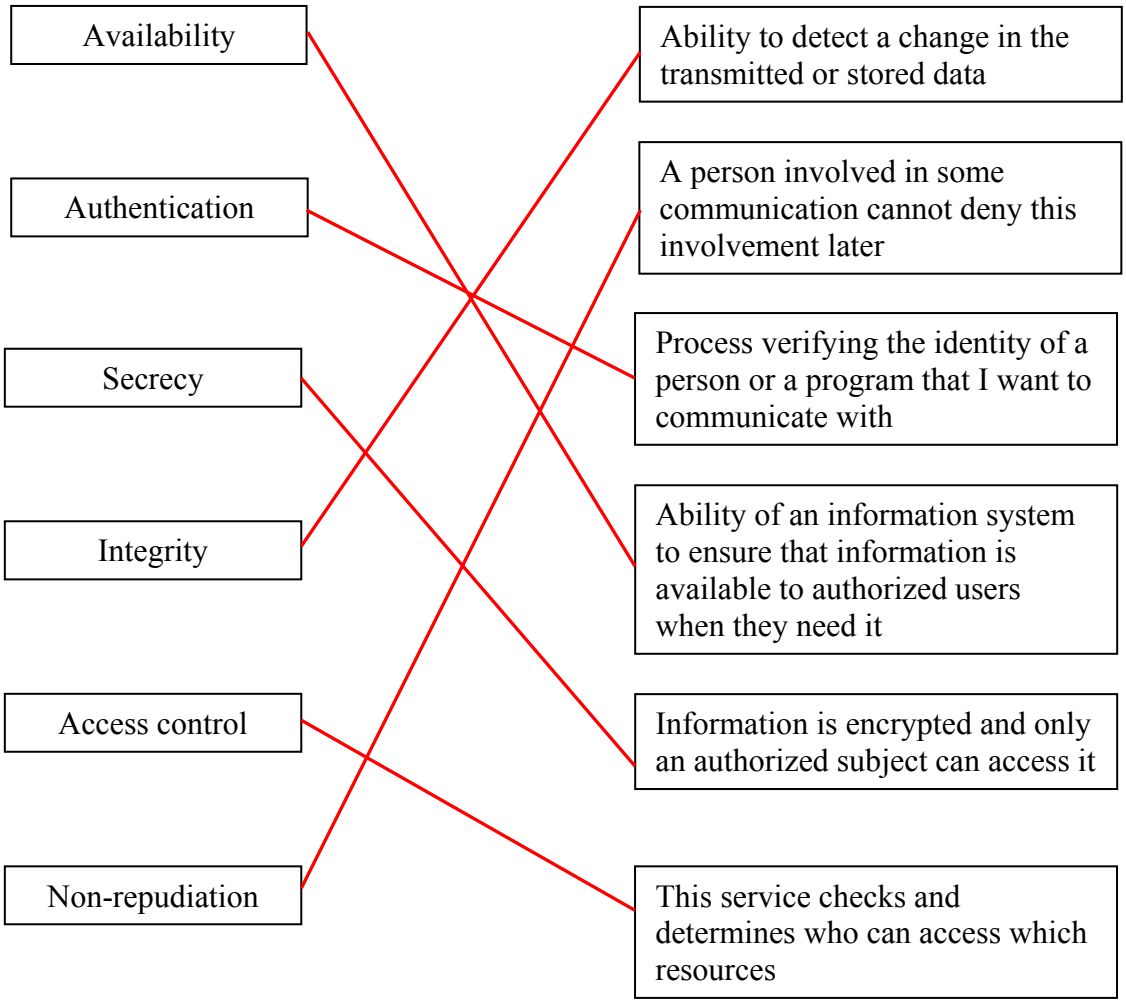
WORKSHEET C2/1

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



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.

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
UCEOE DP ZK DRDLQ QCEOE DP RZKBEO

Decrypt the text:

QCDP IDMCEO DP JLOE QCZK QUL QCLSPZKR XEZOP LHR
THIS CIPHER IS MORE THAN TWO THOUSAND YEARS OLD

---

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

One of the characteristic properties of (symmetric / ~~asymmetric~~) ciphers is (~~long~~ / short) key.

One of the characteristic properties of (~~symmetric~~ / asymmetric) ciphers is (long / ~~short~~) key.

(Symmetric / ~~Asymmetric~~) encryption is **100 to 1000** times (faster / ~~slower~~) than (~~symmetric~~ / asymmetric) encryption.

(~~Symmetric~~ / Asymmetric) encryption is **100 to 1000** times (~~faster~~ / slower) than (symmetric / ~~asymmetric~~) encryption.

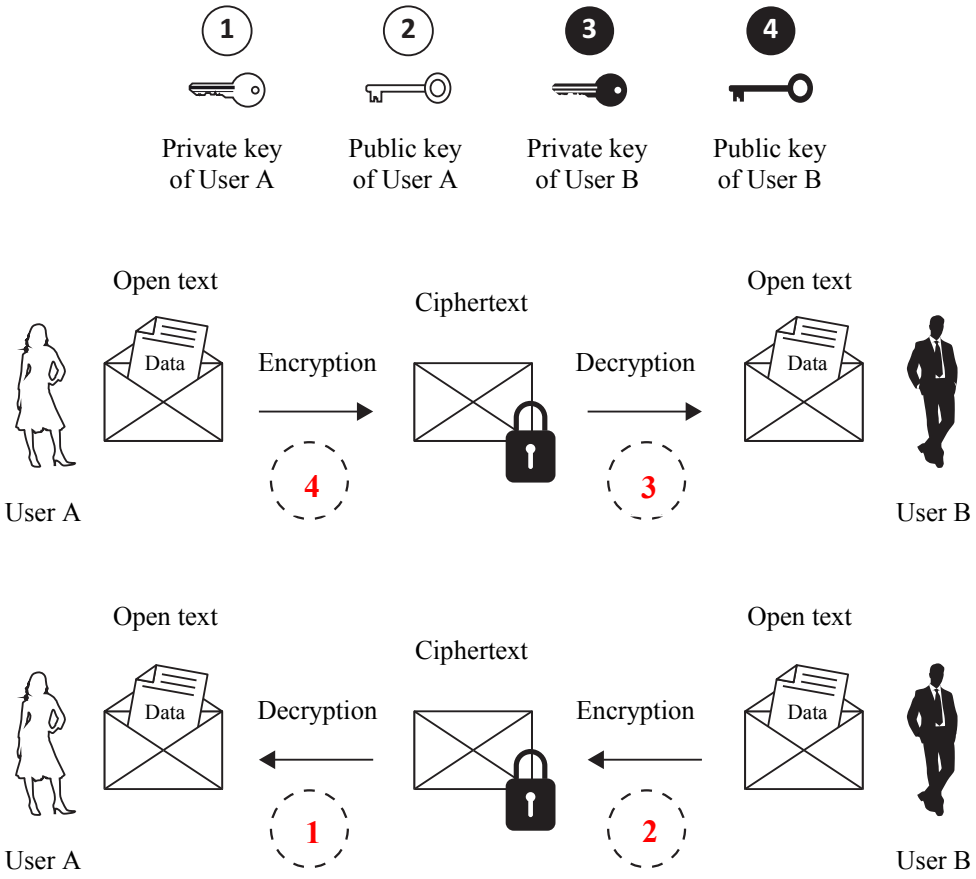
(~~Symmetric~~ / Asymmetric) encryption (can / ~~cannot~~) be used to create digital signature.

(Symmetric / ~~Asymmetric~~) encryption (~~can~~ / cannot) be used to create digital signature.

Lifelong Learning Programme

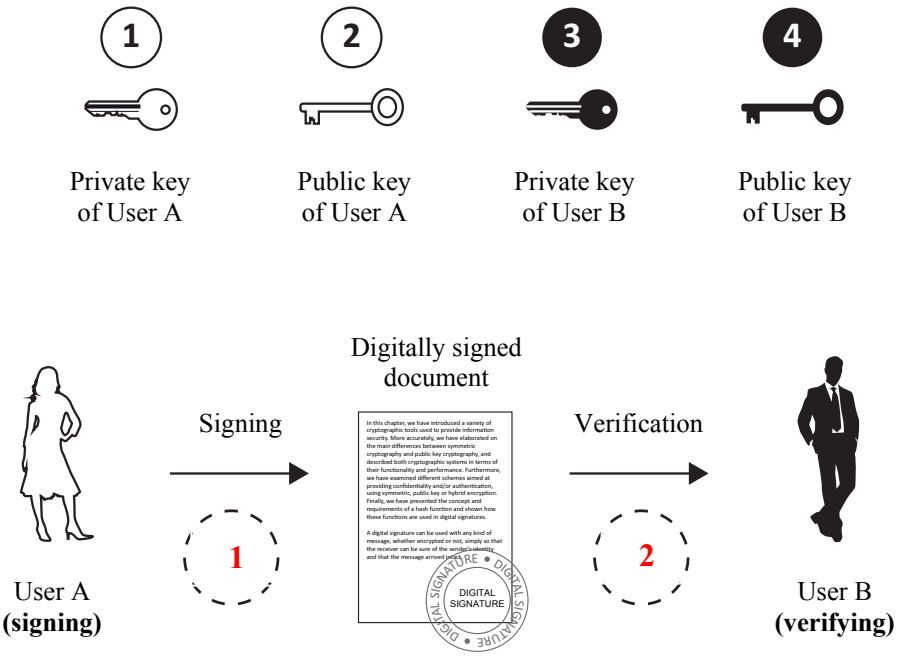
This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

4. In the following picture mark the correct keys to be used when the communicating parties want to use <u>asymmetric cipher</u> 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.



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:

3
6
8

1 – The minimum length of the input must be 1024 bits **(no)**
2 – The output length is variable **(no)**
3 – The output length is constant **(yes)**
4 – The inverse hash function can be used to retrieve the original data **(no)**
5 – Two different input messages **always** produce different outputs (so-called hash) **(no, there may occur collisions, usually undesirable)**
6 – Hash function is today commonly used to create digital signatures **(yes)**
7 – Hash function is today commonly used to encrypt data **(no)**
8 – Its purpose is to produce a unique output from a unique input message **(yes)**

---

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

Symmetric encryption uses (the same key / ~~two different keys~~) 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.