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

This service checks and determines who can access which resources

Information is encrypted and only an authorized subject can access it

A person involved in some communication cannot deny this involvement later

Ability to detect a change in the transmitted or stored data

Ability of an information system to ensure that information is available to authorized users when they need it

Process verifying the identity of a person or a program that I want to communicate with

Access control

Secrecy

Integrity

Non-repudiation

Availability

Authentication

1. 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 |

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

One of the characteristic properties of ciphers is key.

One of the characteristic properties of ciphers is key.

encryption is **100 to 1000** times than encryption.

encryption is **100 to 1000** times than encryption.

encryption be used to create digital signature.

encryption be used to create digital signature.

1. 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.

sifrovani1a.eps

**2**

**3**

**4**

**1**

User A

User B

User B

User A

Data

Data

Data

Data

Encryption

Decryption

Ciphertext

Ciphertext

Decryption

Encryption

Open text

Open text

Open text

Open text

Public key  
of User B

Private key   
of User B

Public key  
of User A

Private key   
of User A

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

sifrovani2a.eps

DIGITAL

SIGNATURE

Digitally signed document

Verification

Signing

User B

**(verifying)**

User A

**(signing)**

Private key   
of User B

Public key  
of User B

Public key  
of User A

Private key   
of User A

**1**

**2**

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

|  |
| --- |
| 3 |
| 6 |
| 8 |
|  |
|  |
|  |

Hash function characteristics include:

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)

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

Symmetric encryption uses for encryption and decryption.