1. Přiřaďte slova v levém sloupci ke správné definici vpravo.

Tato služba kontroluje a určuje, kdo má přístup k jakým zdrojům.

Informace je zašifrovaná a má k ní přístup pouze autorizovaný subjekt.

Člověk, který se účastní nějaké komunikace, nemůže v budoucnu tuto skutečnost popřít.

Schopnost zjistit změnu přenášených či uložených dat.

Schopnost informačního systému zajistit, že informace jsou pro oprávněné uživatele přístupné v okamžiku jejich potřeby.

Proces zjišťování identity člověka či programu, se kterým chci komunikovat.

Řízení přístupu

Utajení

Integrita

Nepopiratelnost

Dostupnost

Autentizace

1. Zašifrujte a dešifrujte text pomocí převodní tabulky (tzv. substituční šifra).

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| abeceda otevřeného textu | 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 |
| abeceda šifrovaného textu | 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 |

Zašifrujte text (citát Jana Wericha):

|  |
| --- |
| KDE BLB, TAM NEBEZPECNO. |
| GRE VHV QZJ KEVEYMEIKL |

Dešifrujte text:

|  |
| --- |
| QZQL PDAOZ FE PQZOZ TDIE KEY RTZ QDPDIE HEQ |
| TATO SIFRA JE STARA VICE NEZ DVA TISICE LET |

1. Upravte následující text tak, aby následující tvrzení byla správná.

Jednou ze základních vlastností šifer je jejich délka klíče.

Jednou ze základních vlastností šifer je jejich délka klíče.

šifrování je **100 až 1000** krát než šifrování.

šifrování je **100 až 1000** krát než šifrování.

šifrování použít k vytvoření digitálního podpisu.

šifrování použít k vytvoření digitálního podpisu.

1. Na obrázku vyznačte použití správných typů klíčů, když si uživatelé chtějí předat šifrovaný dokument pomocí asymetrické šifry.

sifrovani1l.eps

**1**

**2**

**3**

**4**

1. Na obrázku vyznačte použití správných typů klíčů, při vytváření a ověřování digitálního podpisu.

sifrovani2l.eps

**1**

**2**

1. Do tabulky doplňte čísla správných tvrzení, kterými se vyznačuje tzv. hašovací funkce.

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

Hašovací funkce se vyznačuje tím, že:

1 – vstup musí mít minimální délku 1024 bitů (ne)

2 – výstup má proměnou délku (ne)

3 – výstup má pevnou délku (ano)

4 – použitím inverzní hašovací funkcí lze získat zpět původní data (ne)

5 – dvě rozdílné vstupní zprávy mají vždy rozdílný výstup (tzv. haš) (ne, mohou existovat i zpravidla nežádoucí kolize)

6 – hašovací funkce se dnes využívá při vytváření digitálního podpisu (ano)

7 – hašovací funkce se dnes využívá k šifrování (ne)

8 - jejím cílem je z jedinečné vstupní zprávy vytvořit jedinečný výstup (ano)

1. Upravte následující text tak, aby následující tvrzení bylo správné.

Symetrické šifrování používá pro šifrování a dešifrování.