1. Priraďte slova v ľavom stĺpci k správnej definícii vpravo.

Táto služba kontroluje a určuje, kto má prístup k akým zdrojom.

Informácia je zašifrovaná a má k nej prístup iba autorizovaný subjekt.

Človek, ktorý sa zúčastni nejakej komunikácie, nemôže v budúcno-sti túto skutočnosť poprieť.

Schopnosť zistiť zmenu prenášaných či uložených údajov.

Schopnosť informačného systému zabezpečiť, že informácie sú pre oprávnených používateľov prístupné v okamžiku ich potreby.

Proces zisťovania identity človeka alebo programu, s ktorým chcem komunikovať.

Riadenie prístupu

Utajenie

Integrita

Nepopierateľnosť

Dostupnosť

Autentifikácia

1. Zašifrujte a dešifrujte text pomocou prevodovej tabuľky (tzv. substitučná šifra).

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| abeceda otvoreného 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 TDZI KEY RTE QDPDI OLGLT |
| TATO SIFRA JE STARA VIAC NEZ DVE TISIC ROKOV |

1. Upravte nasledujúci text tak, aby nasledujúce tvrdenia boli správne.

Jednou zo základných vlastností šifier je ich dĺžka kľúča.

Jednou zo základných vlastností šifier je ich dĺžka kľúča.

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

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

šifrovanie použiť na vytvorenie digitálneho podpisu.

šifrovanie použiť na vytvorenie digitálneho podpisu.

1. Na obrázku vyznačte použitie správnych typov kľúčov, keď si používatelia chcú poslať šifrovaný dokument pomocou asymetrickej šifry.

sifrovani1l.eps

**2**

**3**

**4**

**1**

1. Na obrázku vyznačte použitie správnych typov kľúčov pri vytváraní a overovaní digitálneho podpisu.

sifrovani2l.eps

**2**

**1**

1. Do tabuľky doplňte čísla správnych tvrdení, ktorými sa vyznačuje tzv. hašovacia funkcia.

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

Hašovacia funkcia sa vyznačuje tým, že:

1 – vstup musí mať minimálnu dĺžku 1024 bitov (nie)

2 – výstup má premenlivú dĺžku (nie)

3 – výstup má pevnú dĺžku (áno)

4 – použitím inverznej hašovacej funkcie je možné získať späť pôvodné dáta (nie)

5 – dve rozdielne vstupné správy majú vždy rozdielny výstup (tzv. haš) (nie, môžu existovať aj spravidla nežiaduce kolízie)

6 – hašovacia funkcia sa dnes využíva pri vytváraní digitálneho podpisu (áno)

7 – hašovacia funkcia sa dnes využíva na šifrovanie (nie)

8 - jej cieľom je z jedinečnej vstupnej správy vytvoriť jedinečný výstup (áno)

1. Upravte nasledujúci text tak, aby nasledujúce tvrdenie bolo správne.

Symetrické šifrovanie používa na šifrovanie a dešifrovanie.