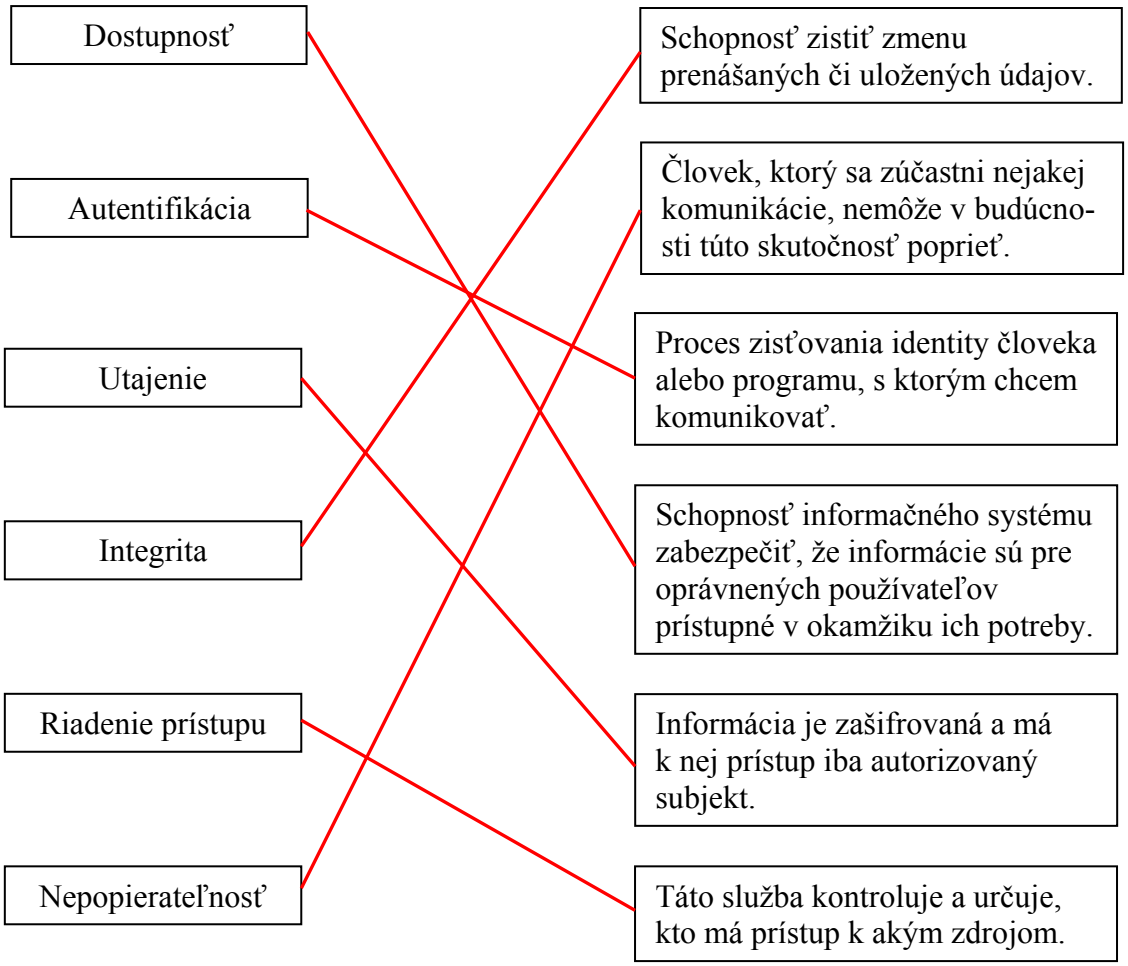
PRACOVNÝ LIST C2/1

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



Program celoživotného vzdelávania

Tento projekt bol financovaný s podporou Európskej Komisie.
Táto publikácia (dokument) reprezentuje výlučne názor autora a Komisia nezodpovedá za akékoľvek použitie informácií obsiahnutých v tejto publikácii (dokumente).

2. 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

---

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

Jednou zo základných vlastností (**symetrických** / ~~asymetrických~~) šifier je ich (~~veľká~~ / **malá**) dĺžka kľúča.

Jednou zo základných vlastností (~~symetrických~~ / **asymetrických**) šifier je ich (**veľká** / ~~malá~~) dĺžka kľúča.

(**Symetrické** / ~~Asymetrické~~) šifrovanie je **100 až 1000** krát (**rýchlejšie** / ~~pomalšie~~) než (~~symetrické~~ / **asymetrické**) šifrovanie.

(~~Symetrické~~ / **Asymetrické**) šifrovanie je **100 až 1000** krát (~~rýchlejšie~~ / **pomalšie**) než (**symetrické** / ~~asymetrické~~) šifrovanie.

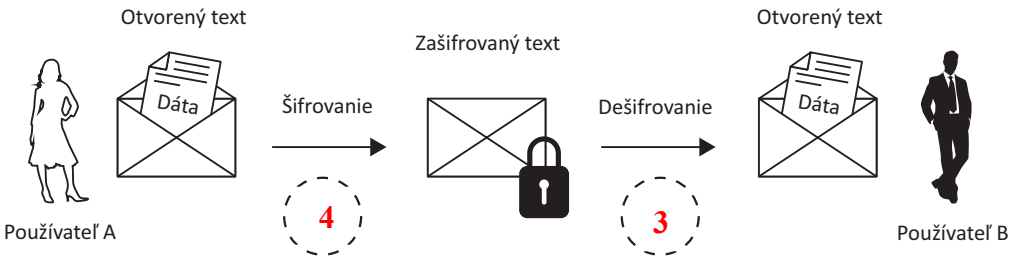
(~~Symetrické~~ / **Asymetrické**) šifrovanie (**možno** / ~~nemožno~~) použiť na vytvorenie digitálneho podpisu.

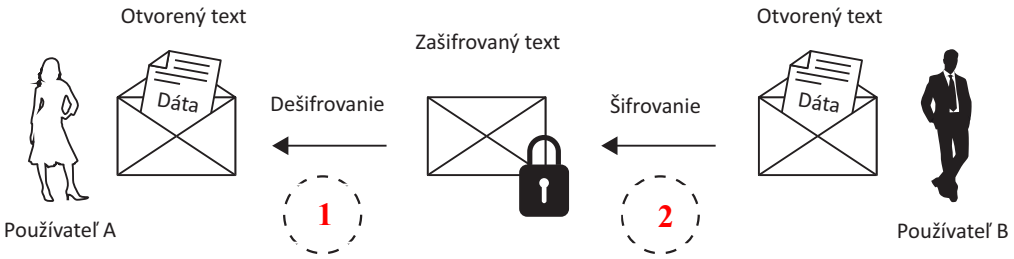
(**Symetrické** / ~~Asymetrické~~) šifrovanie (~~možno~~ / **nemožno**) použiť na vytvorenie digitálneho podpisu.

Program celoživotného vzdelávania

Tento projekt bol financovaný s podporou Európskej Komisie.
Táto publikácia (dokument) reprezentuje výlučne názor autora a Komisia nezodpovedá za akékoľvek použitie informácií obsiahnutých v tejto publikácii (dokumente).

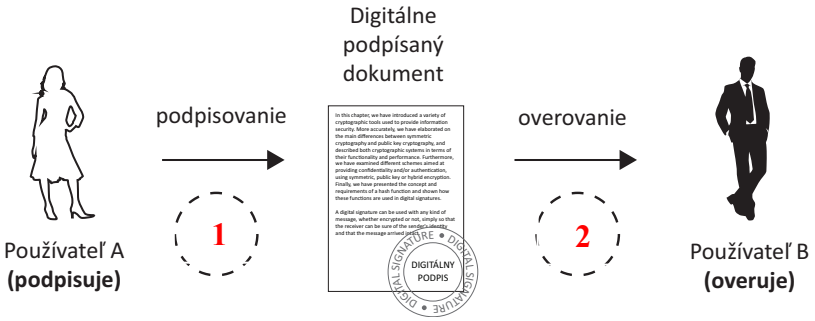
4. Na obrázku vyznačte použitie správnych typov kľúčov, keď si používatelia chcú poslať šifrovaný dokument pomocou asymetrickej šifry.





---

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



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

Program celoživotného vzdelávania

Tento projekt bol financovaný s podporou Európskej Komisie.
Táto publikácia (dokument) reprezentuje výlučne názor autora a Komisia nezodpovedá za akékoľvek použitie informácií obsiahnutých v tejto publikácii (dokumente).

Hašovacia funkcia sa vyznačuje tým, že:

3
6
8

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)**

---

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

Symetrické šifrovanie používa (**rovnaký kľúč** ~~dva rôzne kľúče~~) na šifrovanie a dešifrovanie.

Program celoživotného vzdelávania

Tento projekt bol financovaný s podporou Európskej Komisie.
Táto publikácia (dokument) reprezentuje výlučne názor autora a Komisia nezodpovedá za akékoľvek použitie informácií obsiahnutých v tejto publikácii (dokumente).