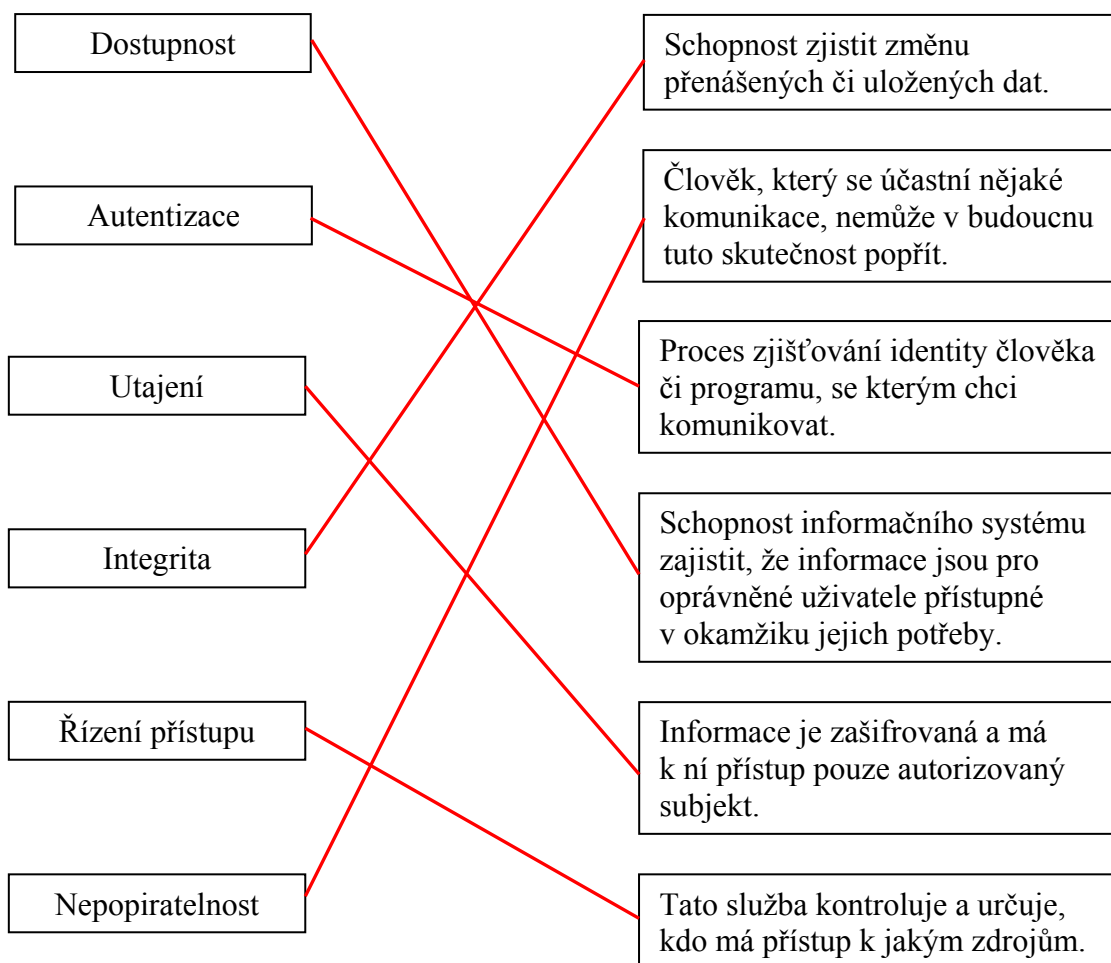


1. Přiřaďte slova v levém sloupci ke správné definici vpravo.



2. 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:

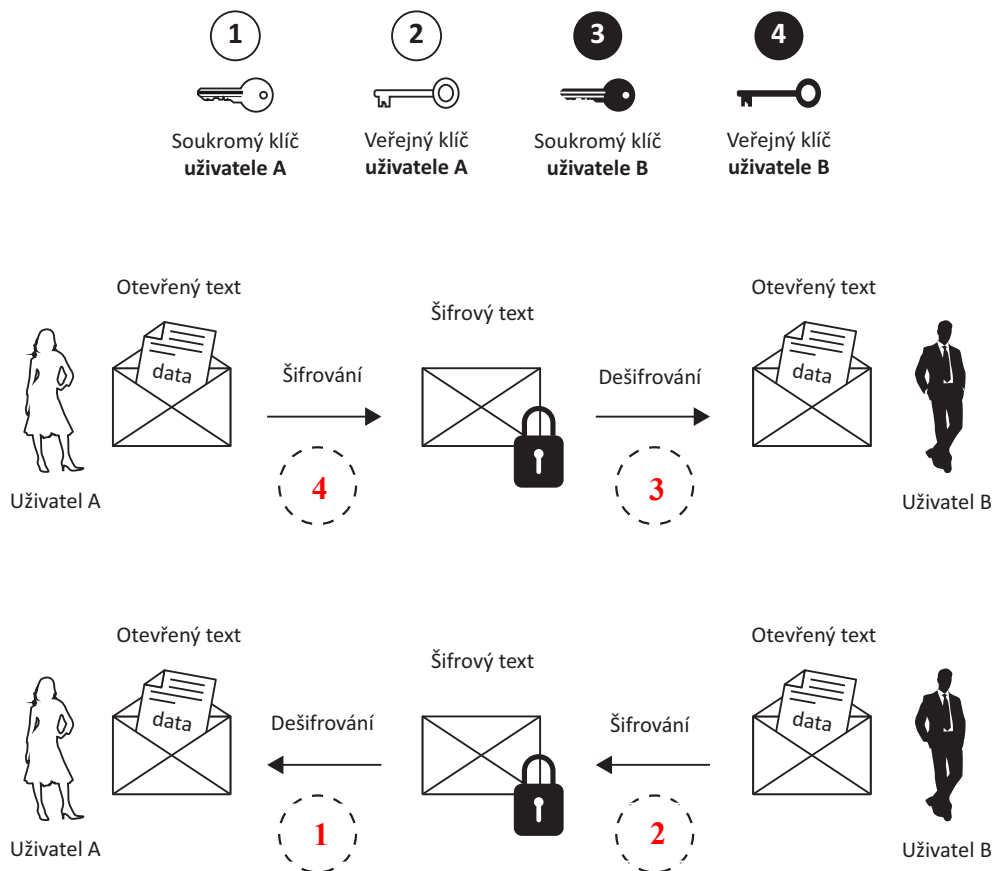
QZQL PDAOZ FE PQZOZ TDIE KEY RTZ QDPDIE HEQ

TATO ŠIFRA JE STARA VICE NEZ DVA TISICE LET

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

Jednou ze základních vlastností (**symetrických** / ~~asymetrických~~) šifer je jejich (~~velká~~ / **malá**) délka klíče.Jednou ze základních vlastností (~~symetrických~~ / **asymetrických**) šifer je jejich (**velká** / ~~malá~~) délka klíče.(**Symetrické** / ~~Asymetrické~~) šifrování je **100 až 1000** krát (**rychlejší** / ~~pomalejší~~) než (~~symetrické~~ / **asymetrické**) šifrování.(~~Symetrické~~ / **Asymetrické**) šifrování je **100 až 1000** krát (~~rychlejší~~ / **pomalejší**) než (**symetrické** / ~~asymetrické~~) šifrování.(~~Symetrické~~ / **Asymetrické**) šifrování (**lze** / ~~nelze~~) použít k vytvoření digitálního podpisu.(**Symetrické** / ~~Asymetrické~~) šifrování (~~lze~~ / **nelze**) použít k vytvoření digitálního podpisu.

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



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



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

Hašovací funkce se vyznačuje tím, že:

3
6
8

- 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 funkce 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)**

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

Symetrické šifrování používá (**stejný klíč**) pro šifrování a dešifrování.
~~dva různé klíče~~