PRACOVNÍ LIST C2/1

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

Dostupnost	Schopnost zjistit změnu přenášených či uložených dat.
Autentizace	Člověk, který se účastní nějaké komunikace, nemůže v budoucnu tuto skutečnost popřít.
Utajení	Proces zjišťování identity člověka či programu, se kterým chci komunikovat.
Integrita	Schopnost informačního systému zajistit, že informace jsou pro oprávněné uživatele přístupné v okamžiku jejich potřeby.
Řízení přístupu	Informace je zašifrovaná a má k ní přístup pouze autorizovaný subjekt.
Nepopiratelnost	Tato služba kontroluje a určuje, kdo má přístup k jakým zdrojům.

Program celoživotního učení

Tento projekt byl realizován za finanční podpory Evropské unie.
Za obsah publikací (sdělení) odpovídá výlučně autor. Publikace (sdělení) nereprezentují názory Evropské komise a Evropská komise neodpovídá za použití informací, jež jsou jejich obsahem.

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.

Dešifrujte text:

QZQL PDAOZ FE PQZOZ TDIE KEY RTZ QDPDIE HEQ

---

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

Jednou ze základních vlastností (symetrických / asymetrických) šifer je jejich (velká / malá) délka klíče.

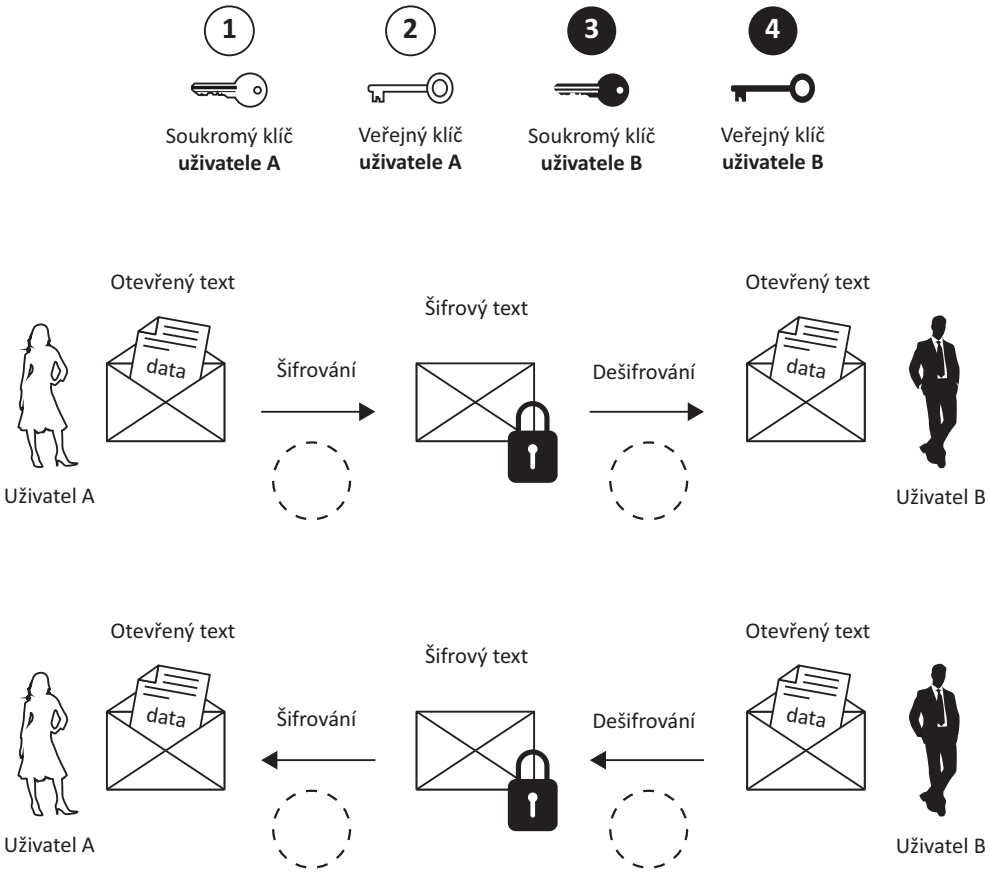
(Symetrické / Asymetrické) šifrování je ____ krát (rychlejší / pomalejší) než (symetrické / asymetrické) šifrování.

(Symetrické / Asymetrické) šifrování je (lze / nelze) použít k vytvoření digitálního podpisu.

Program celoživotního učení

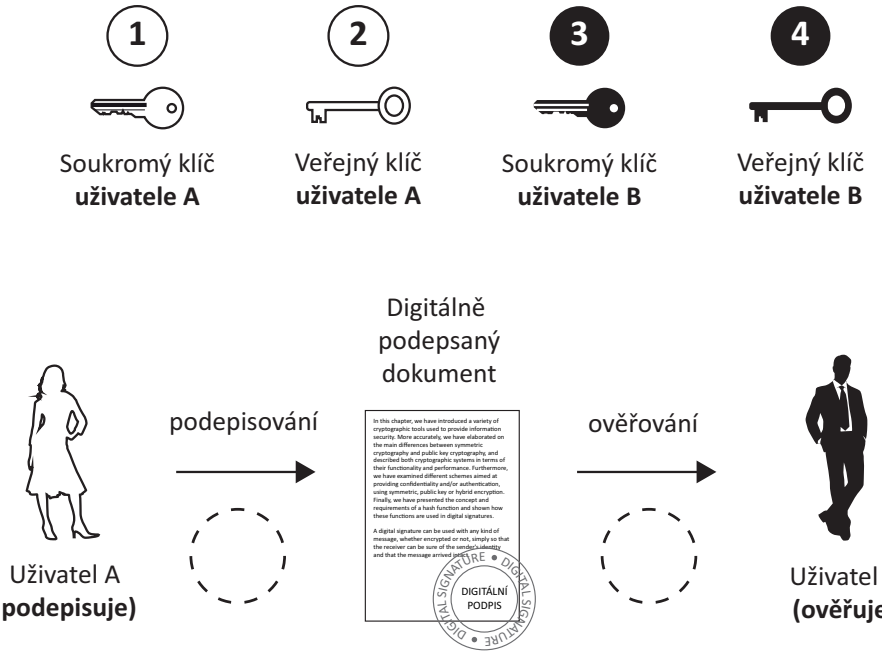
Tento projekt byl realizován za finanční podpory Evropské unie.
Za obsah publikací (sdělení) odpovídá výlučně autor. Publikace (sdělení) nereprezentují názory Evropské komise a Evropská komise neodpovídá za použití informací, jež jsou jejich obsahem.

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.



Program celoživotního učení

Tento projekt byl realizován za finanční podpory Evropské unie.
Za obsah publikací (sdělení) odpovídá výlučně autor. Publikace (sdělení) nereprezentují názory Evropské komise a Evropská komise neodpovídá za použití informací, jež jsou jejich obsahem.

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

Hašovací funkce se vyznačuje tím, že:

1 – vstup musí mít minimální délku 1024 bitů
2 – výstup má proměnou délku
3 – výstup má pevnou délku
4 – použitím inverzní hašovací funkcí lze získat zpět původní data
5 – dvě rozdílné vstupní zprávy mají vždy rozdílný výstup (tzv. haš)
6 – hašovací funkce se dnes využívá při vytváření digitálního podpisu
7 – hašovací funkce se dnes využívá k šifrování
8 - jejím cílem je z jedinečné vstupní zprávy vytvořit jedinečný výstup

---

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

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

Program celoživotního učení

Tento projekt byl realizován za finanční podpory Evropské unie.
Za obsah publikací (sdělení) odpovídá výlučně autor. Publikace (sdělení) nereprezentují názory Evropské komise a Evropská komise neodpovídá za použití informací, jež jsou jejich obsahem.