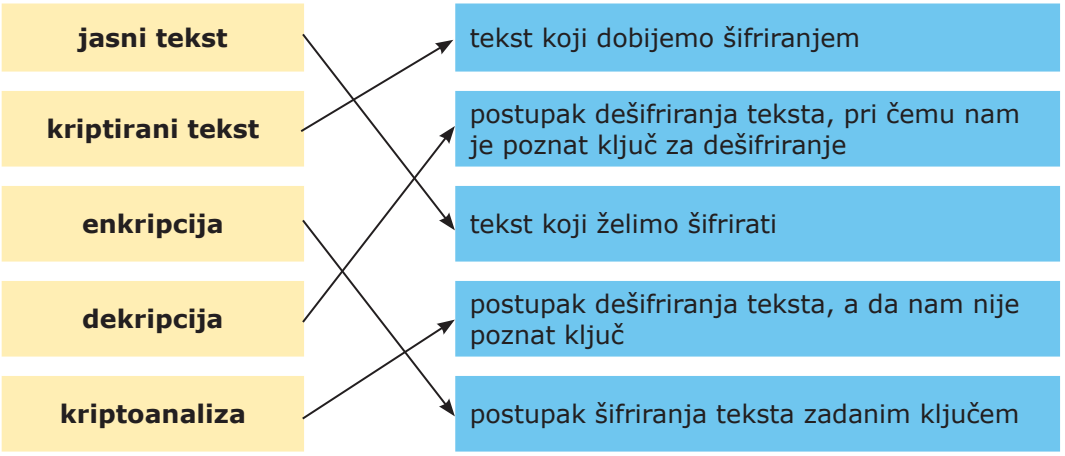
Zadatci za ponavljanje

RJEŠENJA

1.



2. Kod Cezarovog kriptiranja se svako slovo jasnog teksta pomiče udesno za tri mjesta, tako je *A* kodiran slovom *D*. Dakle, ključ kriptiranja je 3 i ključ je simetričan.

3. Osnovne vrste ključeva kod kriptiranja su simetrični i nesimetrični odnosno javni i tajni.

4. Cezarovo kriptiranje ima tajni, simetrični ključ.

5.
a. `NULSWRJUDILMD`
b. `SURJUDPLUDQMH`
c. `FHCDURYRNULSWLUDQMHMHMHGQRVWDYQR`

6. Kod kriptiranja s pomakom možemo samostalno ključ je bilo koji prirodan broj, dok je kod Cezarova kriptiranja on uvijek 3.

7. Kod monoalfabetskih sustava za kriptiranje neko se slovo uvijek kriptira istim slovom, za razliku od polialfabetskih sustava za kriptiranje gdje se neko slovo može kriptirati različitim slovima.

8. SKOLA

9.

1	1
2	4
3	5
4	2
5	3
6	6

10. Primjer polialfabetskog sustava je Vigenèreovo kriptiranje koji za kriptiranje koristi i posebnu tablica.

11. **a.** BUEUXUNO **b.** OSKOESA **c.** ZZEYEKWX

12. **a.** TERIKHPAJXYJGKIORMEXPNOSZ
b. OIENIRAEMOPANZLRMJAJGRJIV

13. **a.** MATEMATIKA JE KORISNA
b. OVO JE JASNI TEKST A NE KRIPTOGRAM

14. Primjer modernog kriptiranja s tajnim ključem je: DES .

15. Kod kriptografije s nesimetričnim ključem postoje dvije vrste ključeva, a to su: tajni i javni ključ.

16. U faktoriziranju velikih brojeva.

17. Uzmimo dva prosta broja p i q.
$n = p * q = 133$
$f = (p - 1) * (q - 1) = 108$
Odaberemo prirodan broj e koji je relativno prost s f.
Odaberemo prirodan broj d takav da je $d * e \% f = 1$.
Poruka treba biti broj m koji je manji od p.
Pripadna kriptirana poruka je: $c = m^e \% n$.

18. Spor je.

19. **a.** $((x^2 \cdot x)^2 \cdot x)^2$
b. $(((x^2 \cdot x)^2 \cdot x)^2)^2 \cdot x$
c. $((((x^2)^2)^2)^2)^2$

20. **a.** 8 **b.** 3 **c.** 6

21. $n = p * q = 33$
$f = (p - 1) * (q - 1) = 20$
Pripadna kriptirana poruka je: $c = m^e \% n = 9^7 \% 33 = 15$.
Dekriptiranje poruke: $m = c^d \% n = 15^3 \% 33 = 9$.