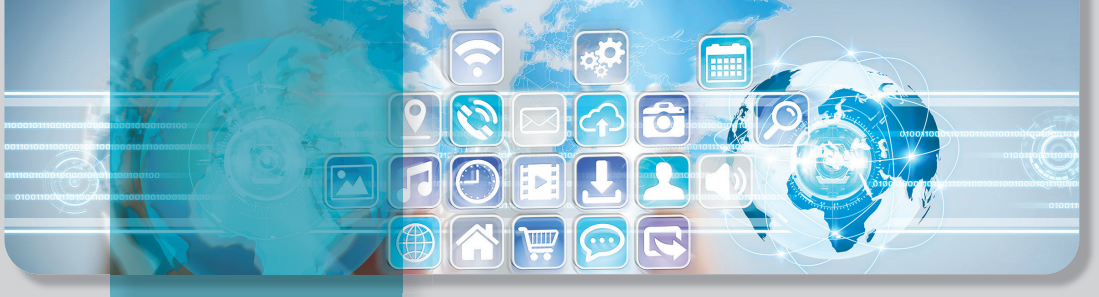


1. Elektronički svijet

1.1. Informacijske i komunikacijske tehnologije

1. Opiši barem tri načina na koja upotrebljavaš informacijsko-komunikacijske tehnologije u prometu.

2. Opiši barem tri načina na koja upotrebljavaš informacijsko-komunikacijske tehnologije prilikom učenja.

3. Opiši barem tri primjera upotrebe informacijsko-komunikacijskih tehnologija u primjeni kućanskih aparata.

1.2. Sigurnost i računalni virusi

4. U sljedećim tvrdnjama zaokruži ispravnu istaknutu riječ ili skupinu riječi tako da tvrdnja bude točna.

   a) Osnovni zadatak kriptografije jest omogućiti pošiljatelju i primatelju poruke **sigurnu** / **nesigurnu** komunikaciju preko **sigurnog** / **nesigurnog** komunikacijskog kanala tako da treća osoba ne razumije poruke.

   b) Pritom **pošiljatelj** / **primatelj** preoblikuje poruku prema unaprijed dogovorenom ključu koji je poznat samo **pošiljatelju** / **primatelju**.

   c) Dogovoreni ključ prema kojem se preoblikuje poruka naziva se **kriptogram** / **šifra**, a sam postupak preoblikovanja poruke šifriranje ili kriptiranje.

   d) Postupak kojim se poruka **šifrira** / **vraća** u prvobitni oblik, naziva se dešifriranje ili dekriptiranje.

   e) **Kriptirana** / **dekriptirana** poruka naziva se kriptogram.

   f) Funkcije kriptiranja i dekriptiranja zajedno čine **kriptosustav** / **kriptogram**.

5. Zaokruži slova ispred točnih tvrdnji.

   a) Prilikom kriptiranja tekstualnih poruka dvije su vrste šifri: blokovne i protočne.

   b) Protočnim se šiframa kriptira jedan po jedan blok elemenata poruke uz primjenu iste šifre.

   c) Blokovnim se šiframa kriptira element po element uz primjenu različitih šifri.

d) U istoj se poruci ne možemo koristiti objema vrstama šifri.

e) Osnovne metode kriptiranja su supstitucija i transpozicija.

f) Transpozicija je zamjena svakog elementa poruke nekim drugim elementom.

g) Prilikom kriptiranja metodom supstitucije svaki element poruke, znak bit će zamijenjen nekim drugim znakom prema određenom ključu.

h) Primjer kriptiranja metodom transpozicije je ASCII kôd.

i) Supstitucija je premještanje elemenata poruke.

j) Prilikom kriptiranja metodom transpozicije svaki element poruke, znak bit će premješten za nekoliko mjesta u nizu prema određenom ključu.

k) Prema vrsti ključa kriptosustavi se dijele na simetrične i asimetrične.

l) Simetrični kriptosustavi imaju jednak ključ za kriptiranje i dekriptiranje.

m) Kriptosustavi s javnim ključem su simetrični kriptosustavi.

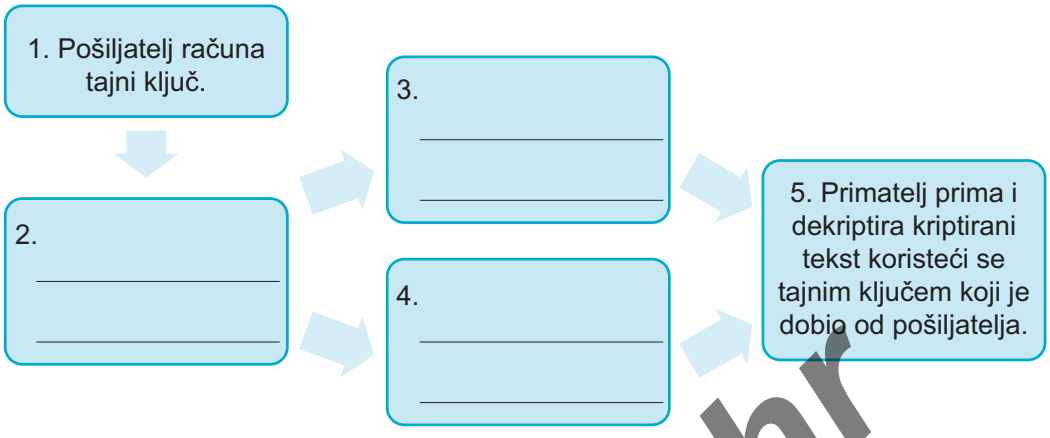
n) Danas je najrašireniji asimetrični kriptosustav DES.

o) Svaki sudionik u komuniciranju simetričnim kriptosustavom treba imati dva ključa: javni ključ kojim se kriptira i koji se javno obznanjuje te tajni ključ kojim se dekriptira, a poznaje ga samo vlasnik.

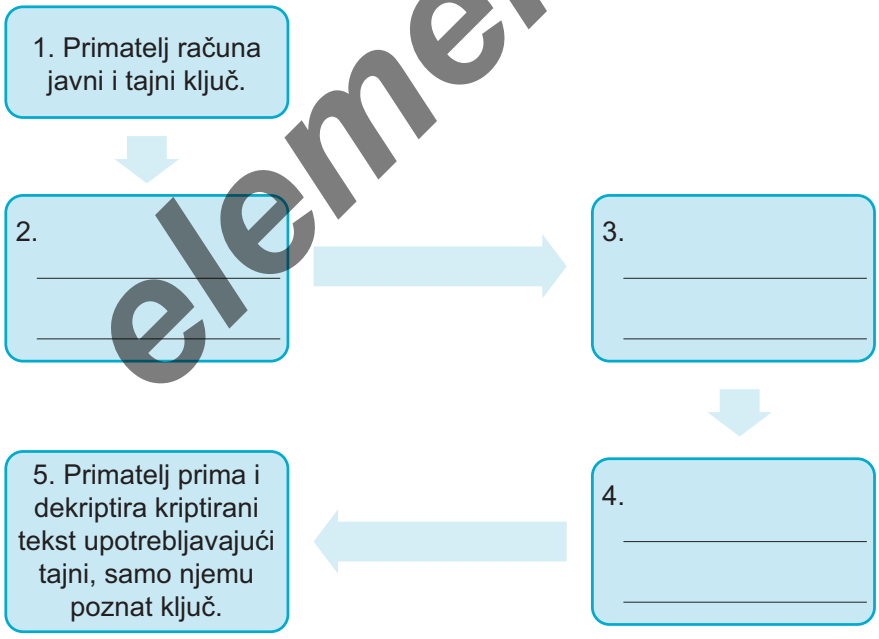
p) Asimetrično kriptiranje brže je od simetričnog, pa je prikladnije za prenošenje većih poruka.

6. Ispravi netočne tvrdnje iz prethodnog zadatka.

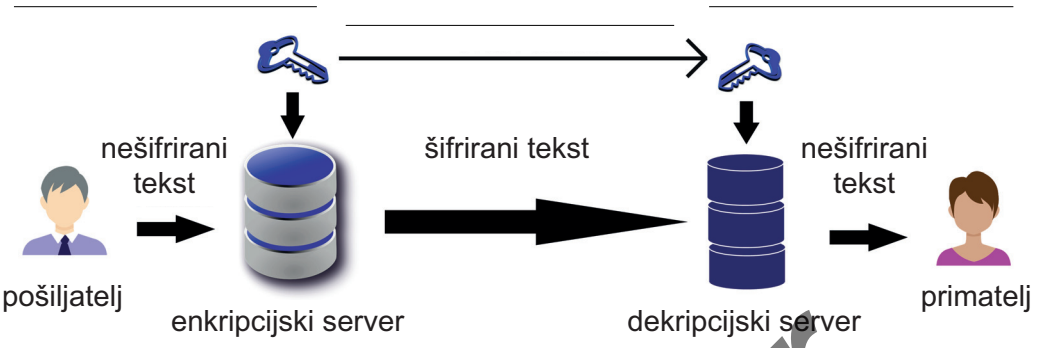
7. Na slici je prikazan dijagram tijeka slanja i primanja šifrirane poruke između sustava pošiljatelja i primatelja u simetričnom kriptosustavu. Dopuni tekst koji nedostaje u poljima pod rednim brojevima 2., 3. i 4.



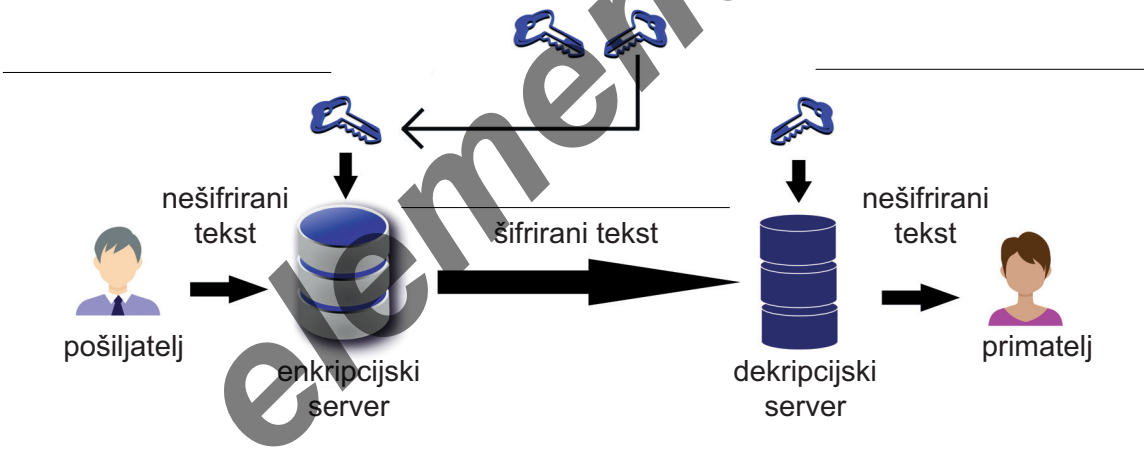
8. Na slici je prikazan dijagram tijeka slanja i primanja šifrirane poruke između sustava pošiljatelja i primatelja u asimetričnom kriptosustavu. Dopuni tekst koji nedostaje u poljima pod rednim brojevima 2., 3. i 4.



9. Na slici je prikazano načelo simetričnog kriptiranja. Na prazne linije upiši pojmove koji nedostaju.



10. Na slici je prikazano načelo asimetričnog kriptiranja. Na prazne linije upiši pojmove koje nedostaju.



11. Dopuni rečenice.

a) Digitalni potpis je _____ za svakog potpisnika.

b) Digitalni potpis radi na temelju protokola koji se naziva _____ _____ (engl. *Public Key Infrastructur*e, PKI).

c) PKI koristi matematički _____ za generiranje dvaju brojeva, javnog i privatnog ključa.

d) Kad potpisnik elektronički potpiše dokument, matematički algoritam stvara podatke koji se _____ s potpisanim dokumentom te dodatno _____ dokument privatnim ključem.

e) Digitalni potpis također je označen _____ potpisivanja dokumenta.