Kriptografija

ŠIFRIRANJE TAJNIH PORUKA

Vaši zadaci

Dragi učenici 4. razreda, vaši zadaci su sljedeći:

1. Pročitajte tekst koji se nalazi na sljedećim stranicama ovog dokumenta.

2. Odgovorite na pitanja koja se nalaze na zadnjoj stranici ovog dokumenta.

Odgovore pošaljite u obliku privatnih poruka na Yammeru.

Odgovore možete poslati do sljedećeg utorka.

Povjerljive informacije

Svakim danom kroz internet prolazi mnoštvo informacija.

Neke od tih informacija nisu važne, a neke su iznimno važne. Primjeri informacija koje su veoma važne su informacije koje šalju banke, vojska, policija.

Za takve važne informacije kažemo da su **povjerljive** – nisu namijenjene za svakoga, nego samo za određenu osobu ili više njih.

Internet se sastoji od velikog broja uređaja koji omogućuju protok informacija od izvorišta do odredišta te od velikog broja žičanih i bežičnih veza između takvih uređaja.

Jedna informacija vrlo često prevali dug put od pošiljatelja do primatelja. Na tom putu neke zlonamjerne osobe mogu pročitati informacije koje nisu namijenjene za njih te ih potom zloupotrijebiti.

Kriptografija

Kako takve povjerljive informacije ne bi bile zloupotrijebljene ili ukradene, osmišljeni su načini šifriranja takvih informacija. **Šifriranje** je pretvaranje izvorne poruke (informacije) u skup simbola koji na prvi pogled nemaju smisla. **Dešifriranje** je vraćanje poruke u izvorni oblik (obrnuti postupak od šifriranja).

Osoba koja šalje poruku (informaciju) i osoba koja prima poruku unaprijed se dogovore na koji će način šifrirati i dešifrirati takve poruke. Na taj način bilo koja druga osoba ne može razumjeti sadržaj poruke ako se ona šifrira.

Kriptografija je znanost koja se bavi proučavanjem načina sigurne komunikacije, odnosno načinima šifriranja i dešifriranja poruka kako bi se poruka sakrila i ostala privatna.

Još jedan pojam koji se često koristi u kriptografiji je **ključ**. To je informacija koja nam govori kako točno poruku šifrirati ili dešifrirati. Ključ bi trebao biti poznat jedino osobi koja šalje i šifrira poruku i osobi koja prima i dešifrira poruku.

Primjer šifriranja

U sljedećoj tablici svako slovo predstavljeno je dvoznamenkastim brojem. Primjerice slovo A predstavljeno je brojem 01. Ova tablica ujedno predstavlja ključ za šifriranje i dešifriranje.

Kod:znak	Kod:znak	Kod:znak	Kod:znak	Kod:znak
01:A	07:DŽ	13:I	19:N	25:Š
02:B	08:Đ	14:J	20:NJ	26:T
03:C	09:E	15:K	21:O	27:U
04:Č	10:F	16:L	22:P	28:V
05:Ć	11:G	17:LJ	23:R	29:Z
06:D	12:H	18:M	24:S	30:Ž

Kada bismo šifrirali ime Ana, to bi izgledalo ovako: 011901 (A – 01, N – 19, A - 01).

Pitanja

1. Što je šifriranje?

2. Što je kriptografija?

3. Zbog čega je potrebno određene informacije šifrirati?

4. Što označava pojam ključ u kriptografiji?

5. Promotrite tablicu na prethodnoj stranici ovog dokumenta. Koristeći tu tablicu, šifrirajte svoje ime!