

ENKRIPC IJA

Kako enkripcija čuva vaše poruke

Šta je enkripcija, kako funkcioniše i šta je ugrožava –
kroz razgovor Olivere i Marka.



OSNOVE

Šta je enkripcija?

Enkripcija šifruje informacije tako da ih mogu razumjeti samo oni koji imaju „ključeve“.



Važno: enkripcija čini informacije nerazumljivim, a ne nedostupnim. Neko i dalje može doći do vaših podataka, ali oni za njega nemaju nikakvog smisla.

ZNAČAJ ENKRIPCije

Zašto je enkripcija važna

U našim sve digitalnijim životima, uloga enkripcije nikad nije bila važnija.

 **Koristite je svaki dan**



1

Privatne poruke

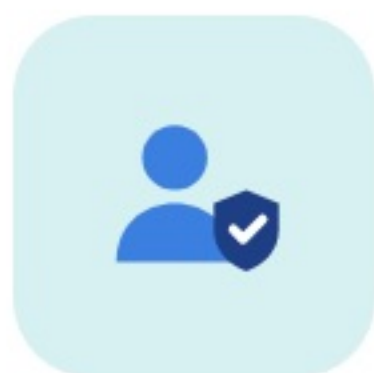
Temelj je bezbjednog interneta i čuva privatnost vaše prepiske.



2

Svaki dan

Od video-poziva do kontrole letjenja i elektronskog glasanja.



3

Vaš identitet

Sprečava da se neko lažno predstavlja kao vi ili kao ljudi kojima vjerujete.



4

Nacionalna bezbjednost

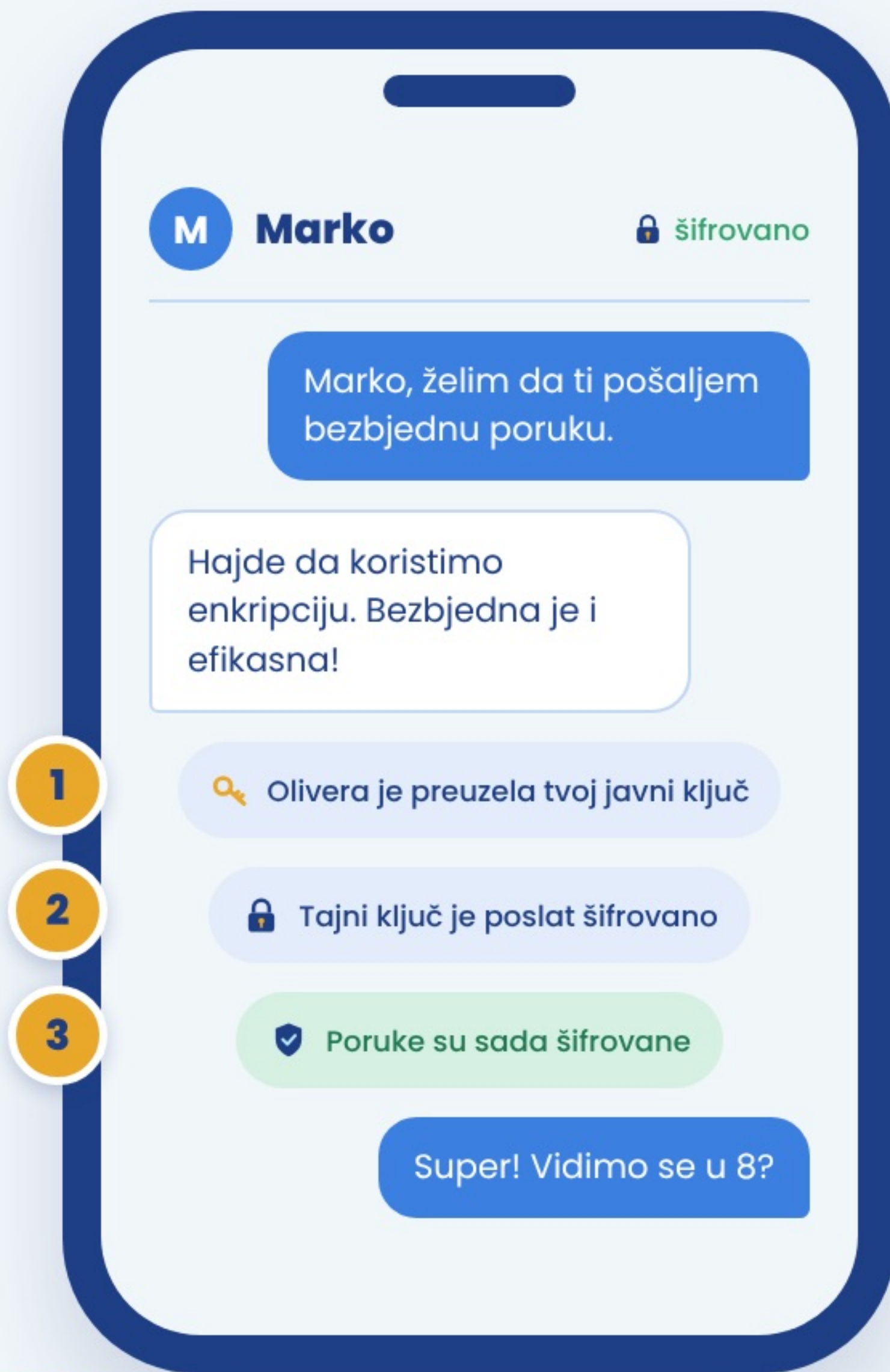
Štiti društvo od terorista, kriminalaca i neprijateljskih vlada.



5

Lični podaci

Drži vaše povjerljive podatke dalje od kriminalaca.



KORAK PO KORAK

Kako funkcioniše enkripcija?

- 1** Svako ima dva ključa: **javni** i **privatni**. Olivera pronalazi Markov javni ključ i kopira ga na svoj uređaj.
- 2** Olivera pravi tajni ključ, šifruje ga Markovim javnim ključem i šalje mu ga. Marko ga otključava svojim privatnim ključem.
- 3** Sada oboje imaju isti tajni ključ za brzu i efikasnu **simetričnu** enkripciju.

Ukratko: početna razmjena ključeva koristi asimetričnu enkripciju, a sami podaci se prenose simetričnom.

NIJE SVAKA ENKRIPCIJA ISTA

Vrste enkripcije

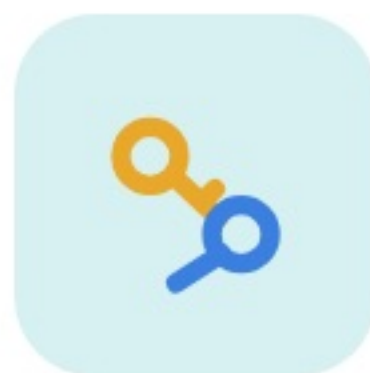
Najbolji sistemi postižu ravnotežu između bezbjednosti i efikasnosti.



Simetrična enkripcija

Kao kasa: svi korisnici imaju isti tajni ključ kojim vide šta je unutra.

- ✓ Brza i efikasna
- ✗ Ranjiva na presretanje



Asimetrična enkripcija

Svaki korisnik ima svoj javni i privatni ključ, što pruža dodatnu bezbjednost.

- ✓ Bezbjedna i pouzdana
- ✗ Složenost znači manju efikasnost



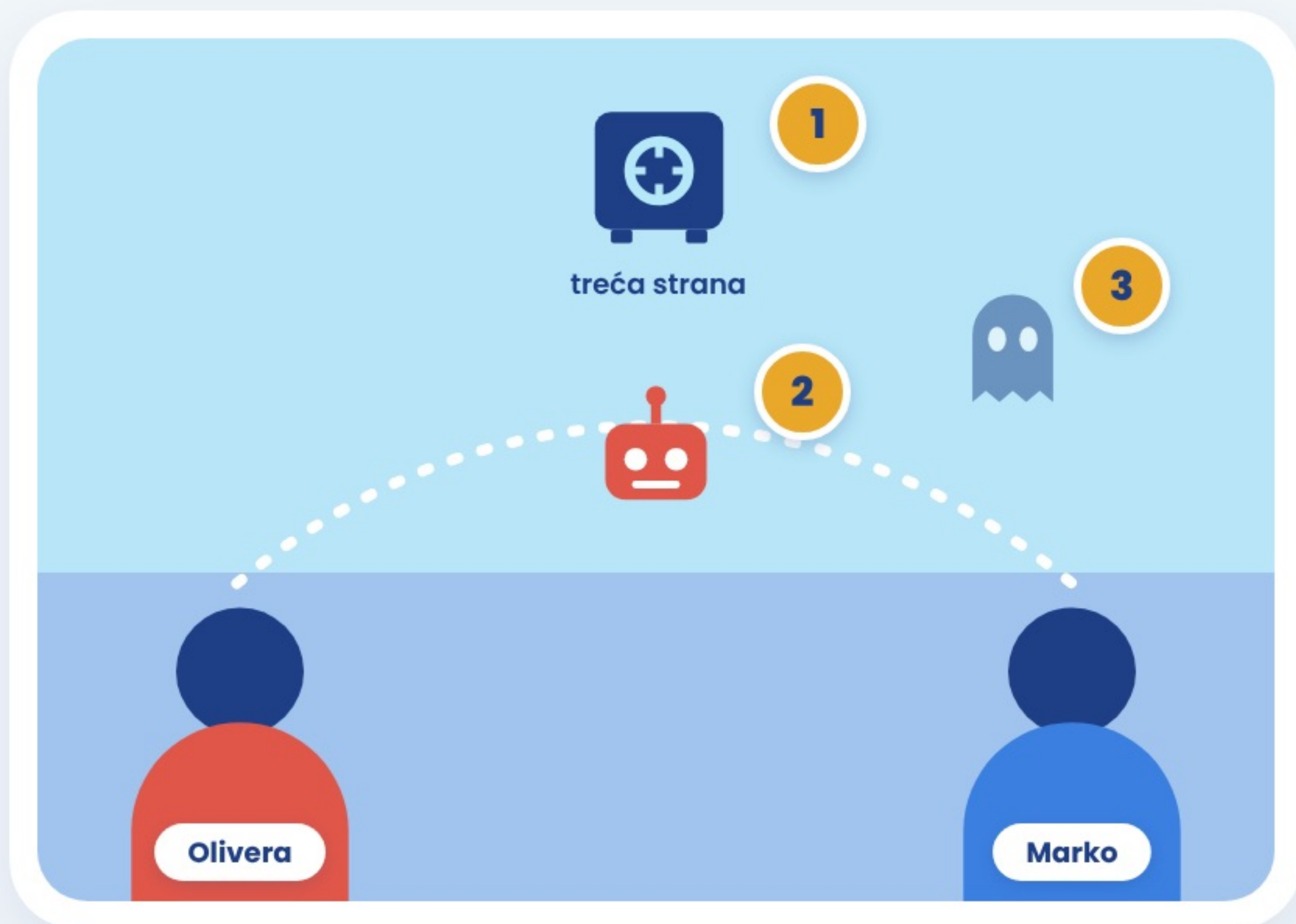
Najbolje od oba svijeta

Hibridna enkripcija

Asimetrična enkripcija za bezbjednu razmjenu ključeva, a simetrična za prenos samih podataka.

- ✓ Bezbjedna i pouzdana
- ✓ Brza i efikasna

Šta ugrožava enkripciju?



Deponovanje ključeva

1

Treća strana čuva ključeve. Ako je pouzdana, nema problema – ali to je potencijalna slabost.

Napad „mašina u sredini“ (MITM)

2

Napadač presreće razgovor, pa može da mijenja poruke i krade podatke.

Prijedlozi „nevidljivog učesnika“

3

Olivera i Marko misle da razgovaraju nasamo, a neko bi mogao tajno da sluša.

Prijetnje mogu doći od pojedinaca, kompanija, pa čak i vlada. One narušavaju povjerenje u internet.

Odakle dolaze prijetnje

Kada znamo ko želi pristup našim podacima, jasno je koliko ih je važno čuvati.

 **Slaba enkripcija otvara vrata**



1

„Zadnja vrata“

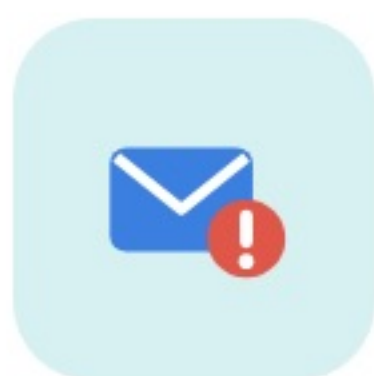
Pojedini organi vlasti ih traže, ali njih mogu iskoristiti i zlonamjerni.



2

Vlade

Mnoge vlade žele da probiju enkripciju kako bi čitale poruke građana.



3

Ucjenjivači

Ciljaju privatne poruke, fotografije i snimke.



4

Novac i ekonomija

Ranjivosti vode do krađe novca i finansijskih podataka.



5

Krađa identiteta

Slaba enkripcija pomaže im da se predstave kao vi.