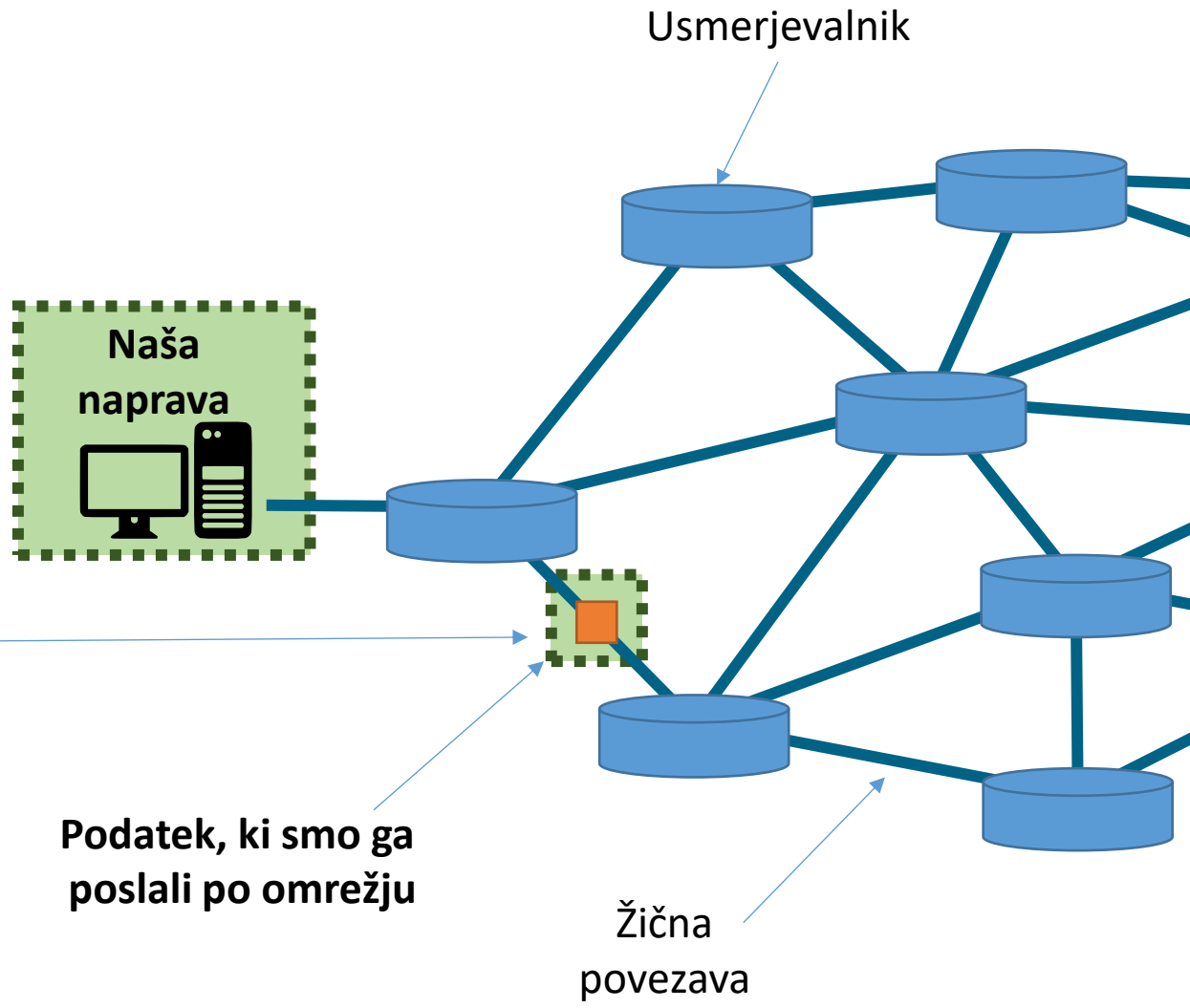
Zasebnost na internetu

Ranljivost na internetu

- Na računalniškem omrežju smo ranljivi na več nivojih:
  - Ranljivi so **viri na napravah** – dostop le avtoriziranim uporabnikom. S tem se ukvarja področje **računalniške varnosti**.
  - Ranljivi so **podatki, ki se prenašajo po omrežju** – dostop le pošiljateljem in naslovnikom. S tem se ukvarja področje **zasebnosti**.



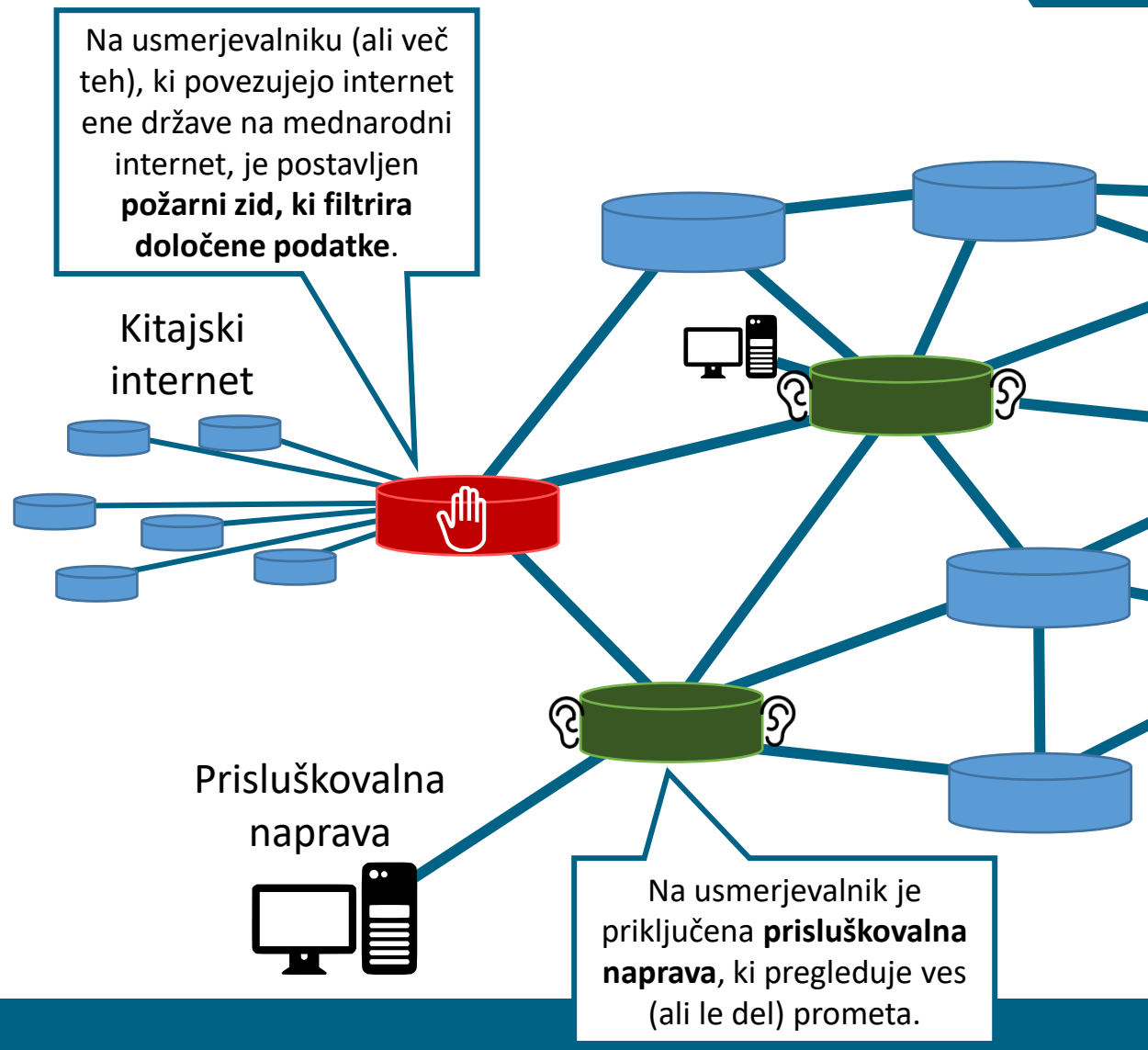
Zasebnost podatkov

- Za ranljivost podatkov v omrežju pa poskrbimo z zasebnostjo. **Zasebnost na omrežju** (angl. *cyber privacy*) združuje tehnike kako podatke ohranimo **zaupne**, **celovite** in **avtorizirane**.
  - **Zaupnost** – vpogled v podatke ni mogoča vsem.
  - **Celovitost** – podatki pridejo na cilj v enaki obliki kot so bili poslani.
  - **Avtoriziranost** – podatke je v omrežje poslal res nekdo, ki trdi, da jih je poslal.

- S primerno tehnologijo in znanjem lahko prisluškujemo prometu na internet. To lahko povzroči veliko škodo (ekonomsko in politično).
  - Če lahko vsebino podatkov kdorkoli **pregleda**, imamo problem z **zaupnostjo**.
  - Če lahko vsebino podatkov kdorkoli **spreminja**, imamo problem s **celovitostjo**.
  - Četudi so podatki kriptirani, obstajajo metode, ki “slabše” enkripcije obidejo. *Kdo ima vire, za prebiranje kriptiranih podatkov?*

Prisluškovanje in filtriranje podatkov

- Tehnično je možno (in se opravlja) **prisluškovanje** in **filtriranje** (nadzirajo) internetnega prometa.
  - Filtriranje ali blokada: Great Firewall na Kitajskem; filtriranje interneta v Iranu, Siriji, Turčiji…; blokada v Severni Koreji…
  - Prisluškovanje v preteklosti: Echelon, Carnivore, Project Minaret, Shamrock
  - Prisluškovanje danes: Prism, XKeyscore, Tempora, Muscular, Project 6, Stateroom…



Argumenti proti in za zasebnost

- **Argumenti proti zasebnosti**:
  - Za večjo varnost, moramo žrtvovati nekaj zasebnosti.
    - Boj proti terorizmu, cyber warfare, omejevanje (otroške) pornografije, vohunstvo in protiobveščevalna dejavnost…
  - *„Če nimamo kaj skrivati, zakaj rabimo zasebnost?“*

- **Argumenti za zasebnost**:
  - Kaj pa, če nič ne skrivamo, ampak informacije želimo le zaščititi?
    - Npr. zdravstvene informacije, o naši simpatiji, o naši ljubezni do Justin Bieberja…
  - Kaj pa, če se naši moralno etični ali politični pogledi ne skladajo z vladajočimi?
  - Kaj pa svoboda govora, svoboda odločitve in pravica do informacij?

Spremljanje menstrualnih ciklov žensk za preprečevanje splavov

Prepoved varnih chat programov

Omejenost dosegljivosti Wikipedije

Enkripcija oz. šifriranje

- Osnovna naloga enkripcije je zapisati podatke tako, da jih **neavtorizirana oseba ne more prebrati** – naslavlja **zaupnost**. Katere podatke pa?
  - informacije o kreditni kartici,
  - osebni podatki,
  - občutljivi podatki podjetja...

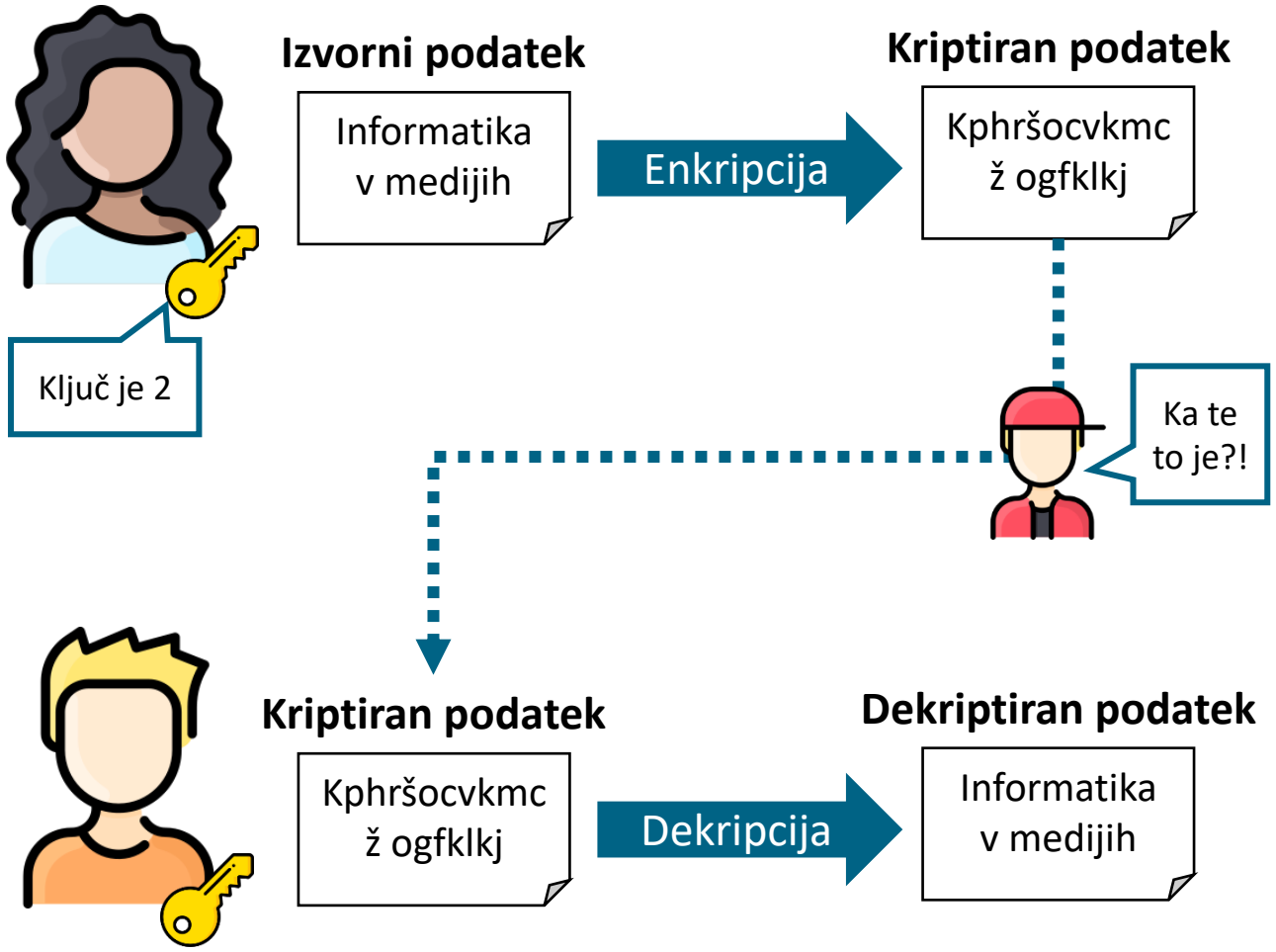
- Sporočilo je uspešno kriptirano (šifrirano), če ga razumeta samo oddajnik in sprejemnik, ne pa ostali (potencialni) posredniki.

- Z računalniško enkripcijo se ukvarja **kriptografija**.
  - Aktualno že v preteklosti: cezarjeva šifra v času Rimskega imperija, Enigma v času 2. svetovne vojne.

Simetrična enkripcija

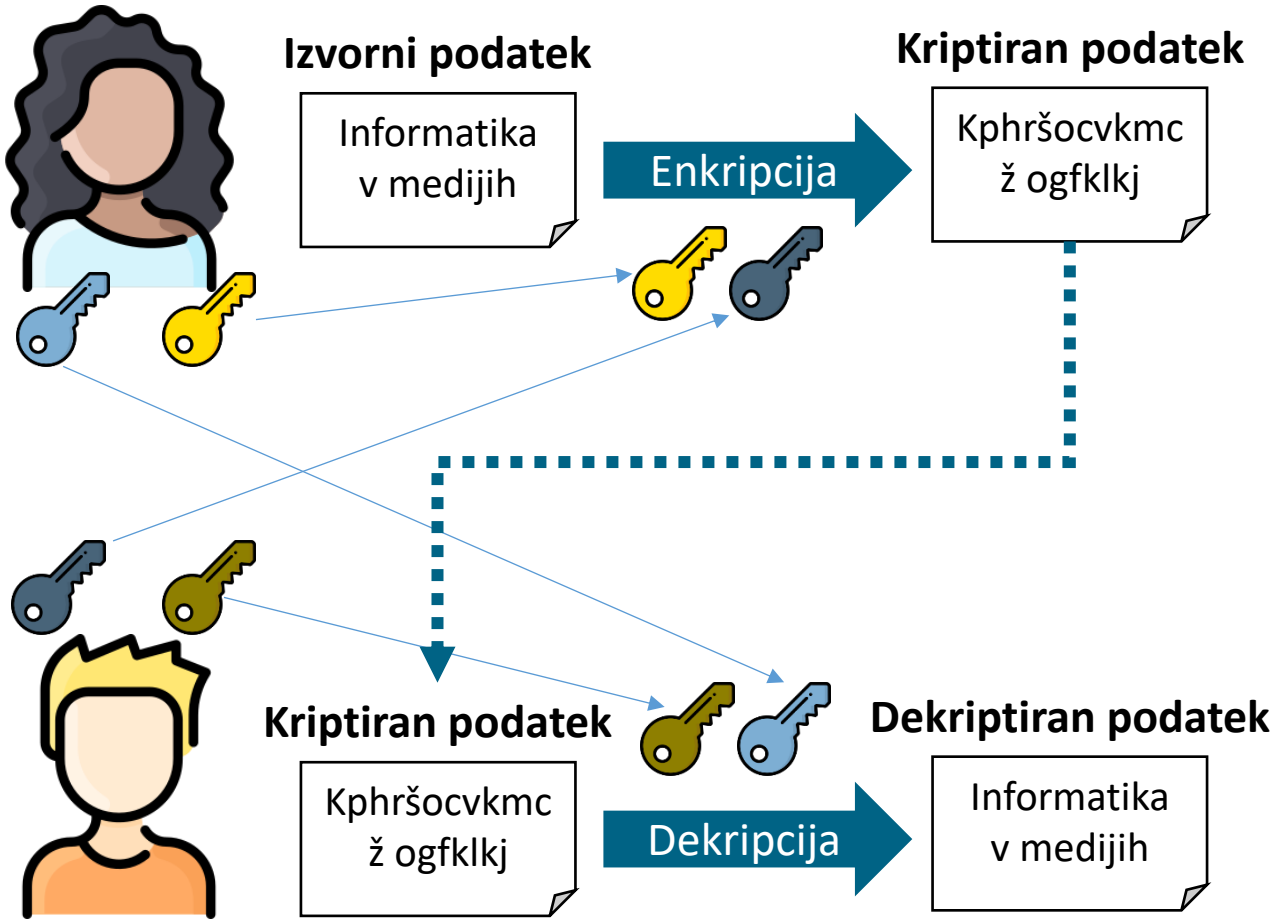
- Za enkripcijo in dekripcijo se uporablja isti ključ.
- **Ključ enkripcije** je način, kako se podatke spremeni.
- Preprost primer Cezarjeve šifre: vsak znak spremenimo tako, da ga premaknemo za X mest po abecedi.

  Primer
- *Problem? Kaj če Jure izda, da je Metin ključ 2?*



Asimetrična enkripcija

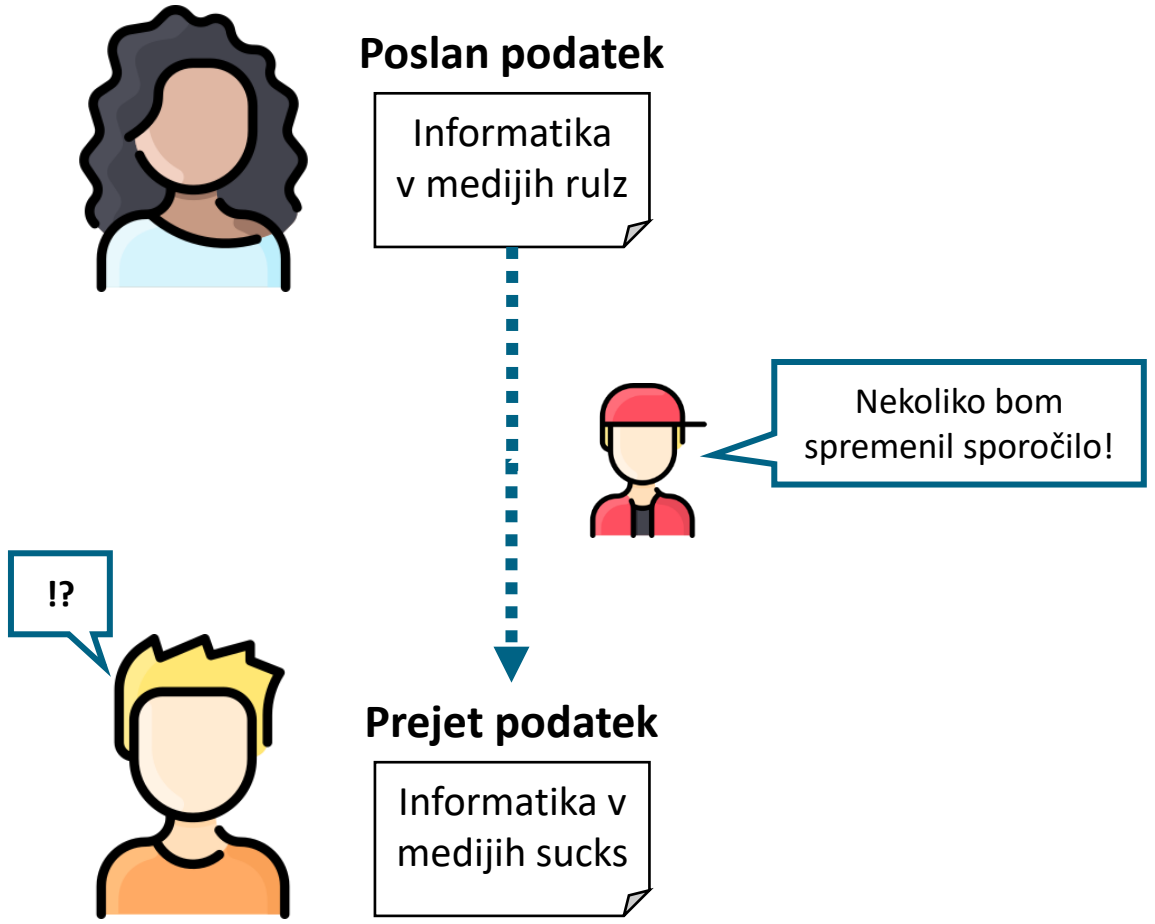
- Za enkripcijo in dekripcijo se uporablja drugačen ključ.
- Vsak ima dva ključa:
  - **Javni ključ**, ki ga lahko pozna vsak.
  - **Privatni ključ**, ki ga moramo zadržati za sebe.
    - Ni potrebno, da si obe strani delita ključe. Ni možnosti izdaje ključa!
- Za enkripcijo rabimo svoj privatni in naslovnikov javni ključ.
- Z dekripcijo rabimo pošiljateljev javni in svoj privatni ključ.



Podpisovanje podatkov

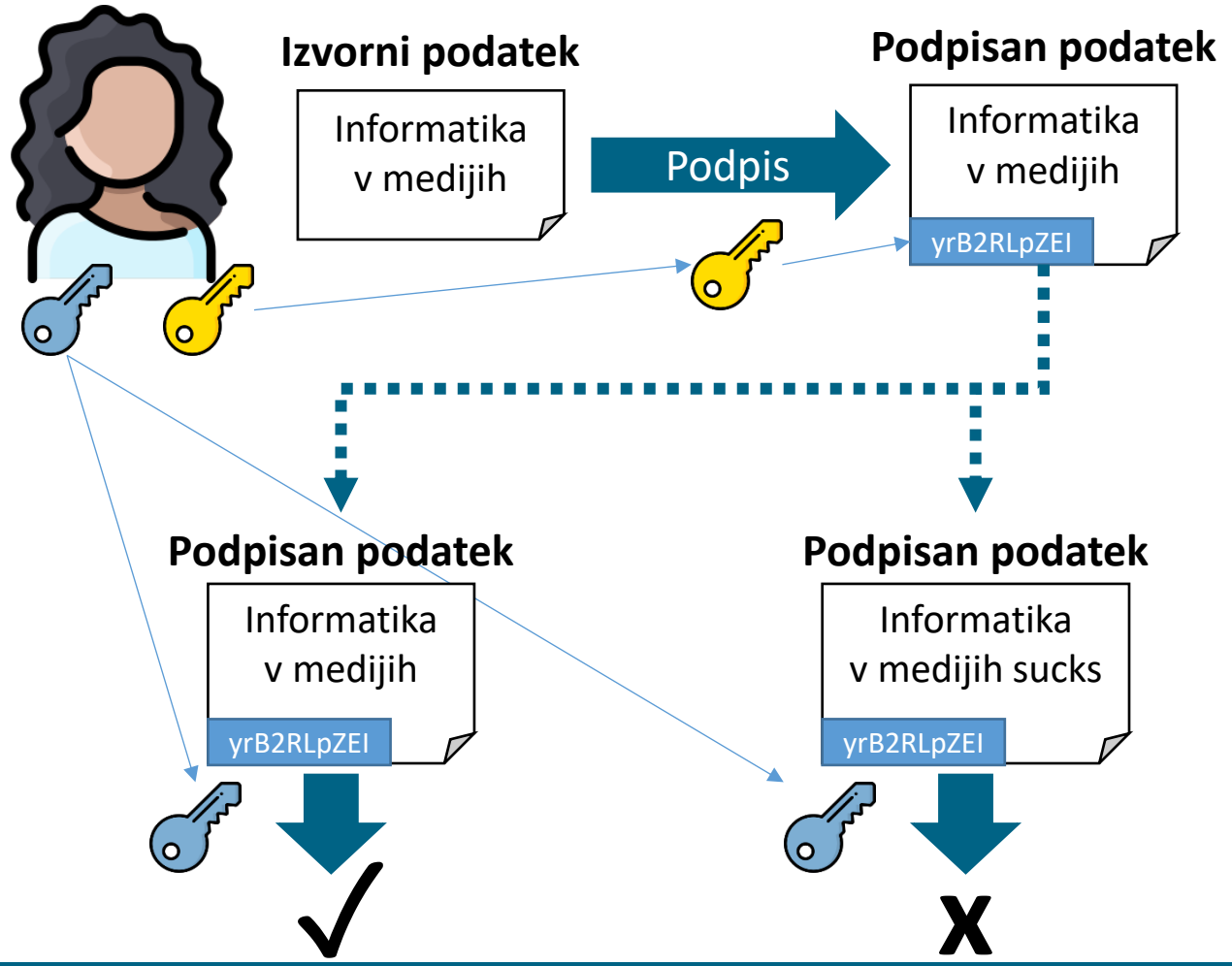
- **Avtorizacija podatkov** – kako se prepričamo, da nam je podatke res poslal klient, iz katerega naslova so prišli podatki?

- **Celovitost podatkov** – kako se prepričamo, da v procesu pretoka podatkov preko interneta ni kdo podatkov spremenil?



Podpisovanje podatkov

- Uporabimo **digitalni podpis** (digitalni certifikat).
- Uporabimo dva ključa:
  - **Javni ključ**, ki ga lahko pozna vsak.
  - **Privatni ključ**, ki ga moramo zadržati za sebe.
- Za podpisovanje rabimo svoj privatni ključ. Podpis nastane s kombinacijo privatnega ključa in vsebine podatkov. Podpis se pripne sporočilo in se z njim pošlje do naslovnika.
- Za pregled podpisanih podatkov rabimo pošiljateljev javni ključ.



Edward Snowden leaks

- **Edward Snowden** je bil zunanji sodelavec pri **NSA** in je skrbel, da vsi njihovi sistemi tečejo nemoteno. Pri tem je imel vpogled v vso delo.

- Zaradi svojih etičnih in političnih prepričanj se je odločil, da javnosti preda informacije o delu obveščevalnih služb (NSA, britanski GCHQ…).
  - Prisluškovanje internetnemu prometu in telefonskim klicem s sistemom PRISM.
  - Neomejeni dostop do podatkov privatnih podjetij brez zaprositve dovoljenja teh podjetij ali uporabnikov (Facebook, Google, Apple…).
  - Sledenje lokaciji mobilnih telefonov.
  - Namerno širjenje slabih načinov enkripcije.
  - Prisluškovanje zaveznikom (EU, Nemčiji…).

Več o tem v dokumentarcu Citizenfour

Anonimnost na internetu

Anonimnost na internetu

- Anonimnost se razlikuje od zasebnosti. Pri **zasebnosti** gre za to, da so podatki na voljo le avtenticiranim uporabnikom. Uporabniki, ki imajo dostop do teh podatkov so znani, le vsebina podatkov ni znana.
  - Primer: vemo, da Luka pošilja neke podatke na naslov NLB.si, ne vemo pa kaj je njihova vsebina (mogoče geslo, mogoče bančno nakazilo?).

- Za **anonimnost** pa gre, ko so lahko (ni pa nujno) podatki vidni vsem, le lastniki teh podatkov želijo ostati neimenovani.
  - Primer: vemo, da nekdo pošilja sliko kužeka na neznan naslov. Ne vemo pa od kod prihajajo in kam so namenjeni (lahko je kdorkoli povezan na internet).

Problem anonimnosti – prstni odtisi

- Brskalniška funkcionalnost privatnega brskanja (v Chrome Incognito način) **ne zagotavlja anonimnosti** – le ne shranjuje podatke o brskanju na naše računalniku.

- Na spletu smo hitro izpostavljeni. Iz podatkov poslanih v podatkih HTTP(S) protokola se namreč skriva kar nekaj naših podatkov – izda nas naš brskalnik!

- Nastavitve našega brskalnika so skorajda unikatne na celotnem spletu. Pravimo, da imamo prstni **odtis brskalnika** (angl. *browser fingerprint*). Do teh nastavitev imajo dostop vse spletne strani, saj le iz teh vedo kako nam naj prikažejo spletno stran.
  - Preveri, svojo unikatnost si na spletu.

Problem anonimnosti – piškoti

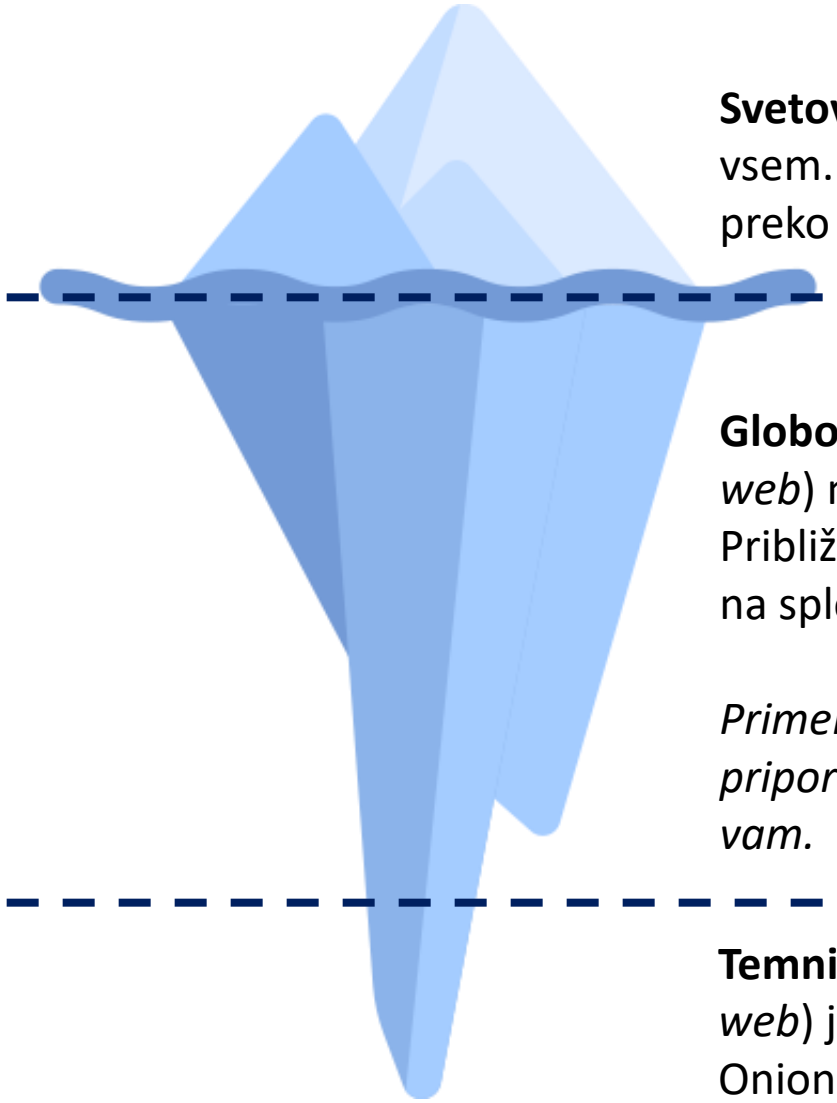
- Za namen izboljšanja UX, spletne strani uporabljajo **piškote** (angl. *cookies*) – majhne datoteke, ki vsebujejo informacije o nas.
  - Ko gremo na Facebook, se na računalniku naredi piškot, ki vsebuje naše Facebook podatke.
  - Zaradi piškota, Facebook ve kako naj vam “zgradi” news feed.
  - Zaradi tega druge strani vedo, ko ste na napravi prijavljeni na Facebook.

- Če spletna stran pregleda vse vaše piškote, ve kaj obiskujete in iz samih piškotov dobi informacije o teh spletnih strani. Pri črpanju informacij iz piškotov lahko hitro ugotovimo kdo stoji za napravo.

- Proti temu se borimo z zakonodajo (EU) in tehnologijo (blokado piškotov bodisi kar z brskalnikom ali vtičnikom blokade reklam).

Temni splet

- Danes je splet že precej cenzuriran – včasih zasluženo (prodaja drog, orožja in belega blaga), včasih pa nezasluženo (politično sporne informacije).
- Vzpostavitev spletnega strežnika, ki bi ponujal vsebine, ki niso zaželene, je danes zelo težko. Hitro pride do odkritja in izključitve iz dovoljenih naslovov (usmerjevalniki več ne usmerjajo do prepovedanih naslovov).
- **Onion** je protokol spleta, ki spletne strani ponuja na alternativen način – skrit navadnim uporabnikom interneta.



Svetovni splet je dosegljiv vsem. Najdemo ga lahko preko spletnih iskalnikov.

Globoki splet (angl. *deep web*) ni dostopen vsem. Približno 90% vse vsebine na spletu.

Primer: stran z YouTube priporočili je dosegljive le vam.

Temni splet (angl. *dark web*) je dostopen le preko Onion protokola.

Anonimnost s preusmeritvami – Tor

- VPN strežnik pozna svoje kliente in ve katere zahteve naredijo. Kaj pa, če želimo kliente in cilje ohraniti anonimne?
  - Primer: Turška vlada zahteva od VPN storitev, da ji posredujejo podatke, kdo je vse preko njih dostopal do Wikipedije (tam je namreč blokirana).

- Kaj pa, če so naslovi VPN strežnikov znani, in določeni usmerjevalniki že blokirajo dostop do njih? Mi pa želimo končne naslove anonimne?
  - Primer: Kitajska blokira uporabo znanih VPN storitev.

- Rešitev: uporabimo več zaporednih nadomestnih strežnikov, ki delujejo po takem protokolu, da je identifikacija klienta (skorajda) nemogoča. Temu protokolu pravimo **Tor**.
  - Dostop do Onion strani je možen le preko Tor protokola.