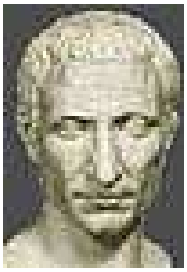
KLASIČNE ŠIFRE IN ZDRAVSTVENA KARTICA, 1. del

Pomena informacije se v naši družbi dobro zavedamo – na koncu koncev se veliko posameznikov in podjetij preživlja zgolj z zbiranjem, urejanjem in posredovanjem informacij. Včasih želimo tudi omejiti dostop do informacij in ena izmed možnosti je njihovo **šifriranje**. Takemu postopku pravimo **šifra** (angl. cipher), izhaja pa iz hebrejske besede *saphar*, ki pomeni *šteti/označiti*. S problemom, kako si osebi (poimenujmo ju Anita in Bojan) izmenjata sporočilo, ne da bi ga opazovalec (Oskar) razvozlal, se (med drugim) ukvarja **kriptologija**. Ta izraz je sestavljen iz grških besed *kryptos*, ki pomeni skrivnost, in *logos*, ki pomeni beseda. Spoznali bomo dva pristopa za reševanje tega problema. V prvem delu predstavimo *zasebne* oziroma *simetrične* šifre, v drugem delu pa še *šifre z javnimi ključi* oziroma *asimetrične* šifre.

Zelo enostaven način za šifriranje besedila so poznali že v rimskih časih, šifrirali so tako, da so zamaknili abecedo za nekaj znakov. Število, ki nam pove, za koliko znakov smo zamaknili abecedo, označimo s K in predstavlja *ključ* za šifriranje in odšifriranje sporočila. Če si izberemo $K = 3$, namesto črke A v sporočilu pišemo Č, namesto B črko D in tako naprej do Ž, namesto katerega pišemo črko C. To šifriranje je pogosto uporabljal tudi Julij Cezar in ni preveč varno, saj bi lahko vsakdo v kratkem času kar "na roko" preveril vseh 24 možnosti.



Cezar ukazal napad

↓

Ehbčt žnčbčo rčšcg

Slika 1: Cezarjeva šifra zašifrira njegovo ime v Ehbčt.

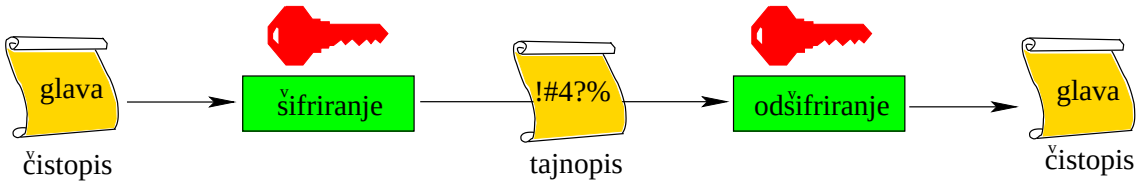
Najbolj razširjena šifra po drugi svetovni vojni je bil DES (Data Encription Standard) in je uporabljal 56-bitne ključe, kar pomeni 2^{56} možnosti za izbiro ključa. Zaradi vse hitrejših računalnikov so ga leta 2000 nadomestili z AES (Advanced Encription Standard), ki lahko uporablja ključe dolžin 128, 196 in 256 bitov.

DES in AES *sta bločni šifri, ker delujeta na blokih (tj. skupini zaporednih znakov). Znake mešata v več krogih s pomočjo enostavnih operacij, katerih vrstnega reda ne moremo spreminjati ne da bi ostala šifra nespremenjena. Take operacije so modularna aritmetika, ekskluzivni ali, ciklični zamik, pogled v tabele itd. Podroben opis teh šifer pa žal presega okvire tega sestavka. Za računske moči napadalcev si oglejte* `http://crypto-systems.com/keylength.html`

Preden si lahko Anita in Bojan začneta pošiljati sporočila, se morata dogovoriti, na kakšen način bosta šifrirala sporočila, in določiti *skrivni ključ* K. Bistveno je, da napadalec Oskar ne izve za skrivni ključ, saj bi lahko sicer brez težav prebiral (in ponarejal) sporočila. Načina šifriranja pa običajno ne skrivamo, saj izkušnje kažejo, da ga napadalec slej ko prej odkrije.

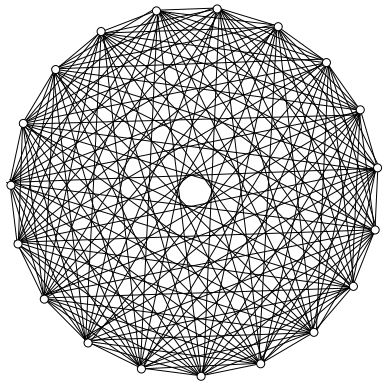
(**Kerckhoffov princip**) *"Nasprotnik" pozna šifro oziroma algoritme, ki jih uporabljamo, ne pa tudi ključev, ki nam zagotavljajo varnost.*

Varnost šifriranja je tako odvisna od zasebnega ključa, za katerega se dogovorita Anita in Bojan. Za tako šifro pravimo, da je *zasebna* oziroma *simetrična*, saj imata Anita in Bojan enak zasebni ključ (glej sliko 2).



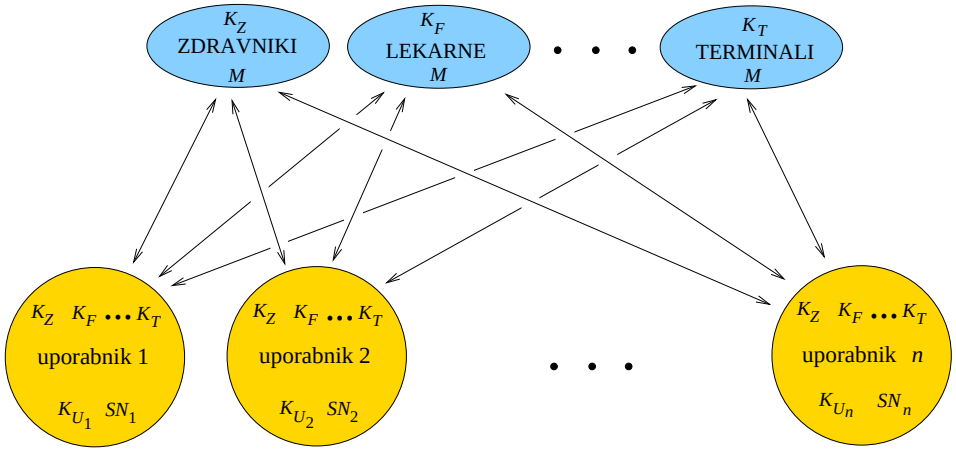
Slika 2: Simetrična šifra uporablja isti ključ za šifriranje in odšifriranje.

Največja nevšečnost takšnega pristopa je torej, da se morata Anita in Bojan pred dopisovanjem sestati. To je za zaljubljen par vsekakor smiselno, v primeru internetnega trgovanja pa nikakor ne. Omenimo še eno pomanjkljivost, ki jo ima takšen način: če povečujemo število posameznikov, ki želijo varno komunicirati v omrežju, narašča tudi število ključev za vsakega uporabnika. Na sliki 3 lahko vidimo primer omrežja z devetnajstimi uporabniki.



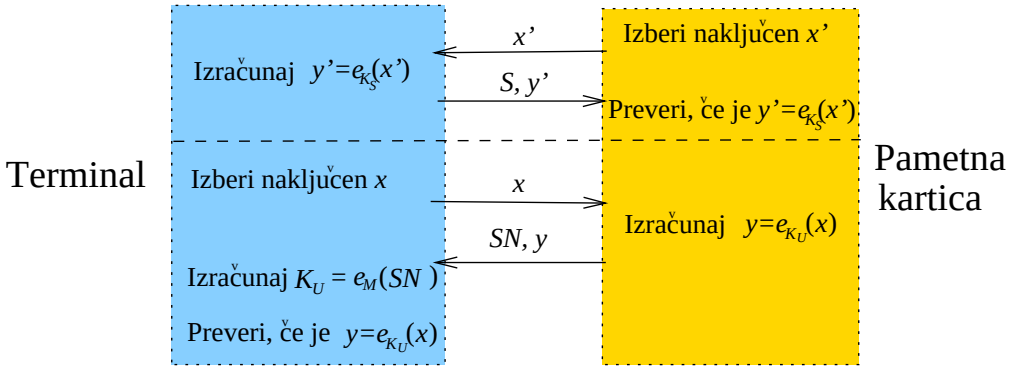
Slika 3: Če v kriptosistemu, ki uporablja simetrično šifro, predstavimo uporabnike s točkami, je ključ za vsak par predstavljen z ustrezno povezavo. Že pri devetnajstih uporabnikih postane prostor okrog vsakega uporabnika precej zapolnjen.

Za občutek kakšen problem predstavlja prostor za shranjevanje ključev, si zamislimo, da jih uporabniki shranjujejo na pametnih karticah (mednje štejemo npr. SIM kartice v mobilnih telefonih, zdravstvene kartice ...). Če imamo na razpolago npr. 8 KB pomnilnika in uporabljamo 128-bitne ključe, lahko na kartico shranimo le 512 ključev. To je odločno premalo že za varno komunikacijo uslužbencev v velikem trgovskem podjetju. Tudi če bi imeli na razpolago večji pomnilnik, pa za potrebe bank, pošt ali zdravstva nikakor ne bi mogli v njem hraniti vseh ključev prebivalcev naše države. V praksi problem pomanjkanja prostora rešimo tako, da uporabnike razdelimo v skupine (glej sliko 4).



Slika 4: Delitev na skupine pri naši zdravstveni kartici. S K so označeni posamezni ključi, glavni ključ je označen z M. Vsak uporabnik ima tudi enolično serijsko številko SN_i.

Vsak uporabnik ima svoj ključ in ključe vsake skupine. Vsaka skupina ima ključ za to skupino in t.i. "glavni" ključ (angl. master key), s katerim lahko iz serijske številke uporabnika izračuna uporabnikov ključ. S pomočjo teh ključev se uporabnik in skupina medsebojno overita (tj. preverita pristnost) na način, prikazan na sliki 5.



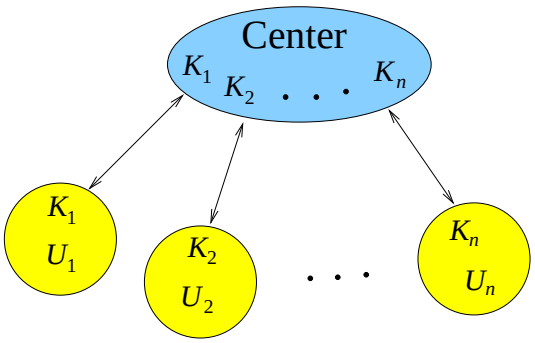
Slika 5: Pametna kartica predstavlja uporabnika, terminal pa skupino. Z e_K označimo šifrirno funkcijo s ključem K. Le-ta pretvori s pomočjo ključa K vsebino v oklepaju v šifrirano besedilo. V zgornjem delu kartica overi terminal s pomočjo skupinskega ključa K_S skupine S, v spodnjem delu pa terminal overi pametno kartico s pomočjo glavnega ključa M in serijske številke kartice (SN). Kartica vsebuje samo K_U in K_S ne pa tudi M, medtem ko terminal ne pozna K_U, ampak ga izračuna s pomočjo M.

Vendar pa imajo vsi kriptosistemi, ki temeljijo na takšni shemi, kar nekaj pomanjkljivosti. Ena izmed večjih je ta, da varnost celotnega sistema temelji na varnosti ene same kartice. Če namreč uspemo odpreti uporabniško kartico, se dokopljemo do vseh skupinskih ključev. To nam omogoča, da se predstavimo ostalim uporabnikom kot katerakoli skupina, ne da bi uporabnik posumil, da ne komunicira s pravim članom skupine. Če pa se dokopljemo do glavnega ključa, lahko enostavno ponarejamo uporabniške kartice, saj si serijsko številko izmislimo, ustrezen uporabnikov ključ pa nato s pomočjo glavnega ključa preprosto izračunamo.

Varnost celotnega kriptosistema ne sme biti odvisna od varnosti ene same kartice.

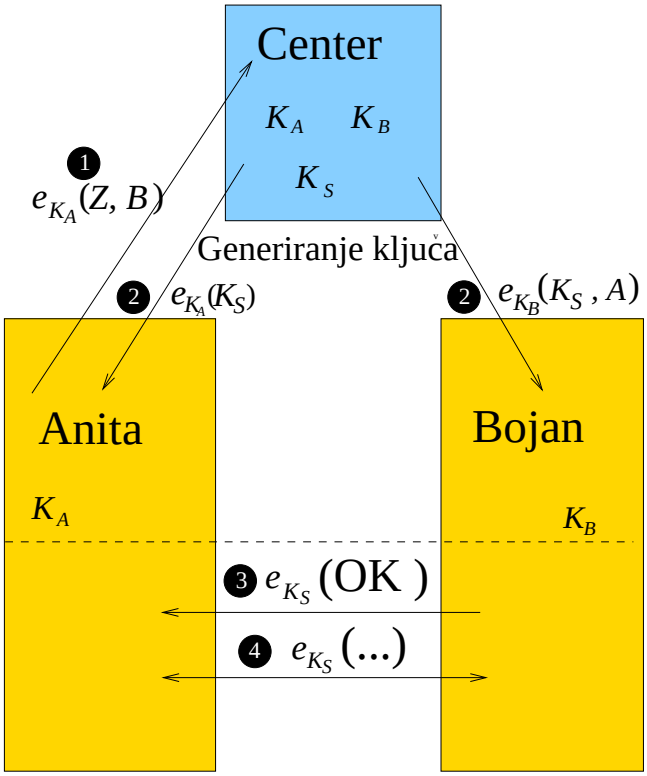
Naslednja pomanjkljivost je ta, da so vse osebe znotraj ene skupine enakovredne, tj. če uporabnik komunicira npr. z lekarno, lahko katerakoli oseba iz skupine lekarn prisluškuje pogovoru. Pa ne samo to, osebe znotraj ene skupine so tudi neločljive, kar pomeni, da se lahko ena oseba iz iste skupine izgovarja, da nečesa ni naredila, čeprav v resnici temu ni tako. Poleg tega je shema povsem neuporabna, če nimamo naravne hierarhične zgradbe, ki nam omogoča delitev na skupine.

Druga rešitev problema s prostorom pa je prikazana na sliki 6, njen najbolj poznan predstavnik pa je Kerberos.



Slika 6: Centralna rešitev s simetričnim sistemom.

V tem primeru imamo center, s katerim vsak uporabnik deli svoj skrivni ključ. Ko želi Anita komunicirati z Bojanom, pošlje centru zašifriran zahtevek. Center generira ključ in zašifriranega pošlje Aniti in Bojanu. Bojan nato obvesti Anito, da je prejel ključ in komunikacija se lahko začne. Celoten potek je prikazan na sliki 7.



Slika 7: V prvem koraku Anita pošlje centru zašifriran zahtevek za pogovor z Bojanom. Center nato v drugem koraku generira ključ in ga pošlje obema. Bojanu tudi sporoči, kdo želi komunicirati z njim. Bojan v četrtem koraku pošlje sporočilo Aniti, da potrdi sprejetje ključa. Nato se začne komunikacija.

Očitna pomanjkljivost te sheme je, da moramo vsakič, ko želimo komunicirati, najprej vzpostaviti povezavo s centrom. Pogosto to ni zaželeno ali pa sploh ni možno. Če uporabniški ključi v centru niso primerno zaščiteni, je varnost celotne sheme ogrožena.

Kartic ni potrebno vedno odpirati, da bi prišli do ključev, ki jih hranijo, pač pa je dovolj, da znamo natančno izmeriti porabo energije v času računanja ter uporabiti nekaj statistike.

Zaradi vseh teh pomanjkljivosti se sheme, ki temeljijo na simetričnem pristopu, uporabljajo bodisi v zaprtih okoljih bodisi tam, kjer ni velike potrebe po varnosti. Takšne sheme se na primer uporabljajo za kartice, ki hranijo administrativne podatke, tako da ni potrebno ročno vnašati podatkov v formularje. Naša zdravstvena kartica je tipičen primer take kartice. Za hranjenje občutljivih podatkov pa so takšne sheme primerne le v okoljih, kjer so vsi uporabniki ves čas povezani v mrežo. V primeru naše zdravstvene kartice pa temu ni tako, saj nam sicer ne bi bilo potrebno skoraj vsakič, ko jo želimo uporabiti, iti najprej do terminala, da ji podaljšamo veljavnost.

Aleksandar Jurišić in Urban Perko