# KRIPTOGRAFSKI SISTEMI

Matej Šalamon, Tomaž Dogša
Fakulteta za elektrotehniko, računalništvo in informatiko
Univerza v Mariboru, Smetanova 17, 2000 Maribor
matej.salamon@uni-mb.si

**Povzetek**

Zagotavljanje tajnosti sporočil brez kriptografskih sistemov je za področje računalniških komunikacij nemogoča naloga, saj so metode prisluškovanja tako enostavne, da jih obvlada vsak povprečen programer. V prispevku bodo opisani koncepti različnih kriptografskih sistemov, ki jih uporabljamo predvsem na področju računalniških komunikacij.

***Abstract***

*Computer network eavesdropping is a very easy task for an average programmer. It is almost impossible to assure confidentiality of information without using cryptographic systems. Various concepts of cryptographic systems that are currently used in the computer networks will be briefly presented.*

## 1. Uvod

Z razvojem računalniških omrežij se je izredno povečal tudi pretok informacij. V začetnem obdobju Interneta je elektronska pošta omogočala samo prenos besedil, današnji protokoli pa omogočajo prenos poljubnih datotek. Sistem za prenos podatkov naj zagotavlja predvsem:

- *zasebnost (tajnost)*: prenašano sporočilo naj bo razumljivo le avtorizirani osebi to je osebi, ki je upravičena oziroma pooblaščena za to, da ga sme npr. prebrati, tiskati in prikazovati.
- *verodostojnost - avtentičnost*: pošiljatelj sporočila naj bo pravilno identificiran oziroma, njegova identifikacija ne sme biti lažna.
- *celovitost:* sprejeta sporočila morajo biti prav takšna kot smo jih poslali, t.j. nespremenjena. Pod spreminjanjem razumemo: pisanje, brisanje, zakasnitev ali ponavljanje sporočila.
- *preprečitev zanikanja:* niti pošiljatelj niti prejemnik ne moreta zanikati poslanega ali prejetega sporočila.
- *dostopnost:* pravico dostopa do sporočila mora imeti le verodostojna oseba t.j. oseba s pravilno identifikacijo.

V tem prispevku se bomo omejili le na zagotavljanje zasebnosti. Razlaga bo temeljila na preprostem modelu, ki je sestavljen iz izvora in ponora sporočil ter informacijskega kanala. Ker je informacijski kanal medij za prenos sporočil oziroma informacij, ki ga velikokrat ni mogoče fizično zaščititi, je po njem prenašano sporočilo izpostavljeno raznovrstnim *napadom*. Ti so zasnovani tako, da skušajo onemogočiti eno ali več zahtev, ki smo jih postavili glede prenosa podatkov. Proti napadom se lahko borimo z oviranjem (npr. šifriranje) in alarmiranjem (detekcija napada). Zasebnost lahko zagotavljamo s *šifrirno napravo*, ki jo vstavimo med izvor sporočila in informacijski kanal. Šifrirna naprava napadov ne more preprečiti, ampak jih lahko samo v večji ali manjši meri ovira. Šifrirna naprava, ki izvorno sporočilo *šifrira* t.j. pretvori v nerazumljivo obliko, poskrbi v prvi vrsti za zasebnost sporočila, hkrati pa lahko v kombinaciji z drugimi podsistemi zagotovi tudi verodostojnost, celovitost in prepreči možnost zanikanja. Onemogočanje ali kršenje zasebnosti sporočil imenujemo *kriptografski napad*.

Namen tega prispevka je prikaz raznih kriptografskih sistemov, ki se najpogosteje uporabljajo v računalniških omrežjih.

## 2. Kriptografski sistemi

Kadar želimo zagotoviti zasebnost nekega sporočila, ga moramo pretvoriti v nerazumljivo obliko, kar pomeni, da ga moramo *šifrirati*. Sporočilo mora biti šifrirano tako, da ga zna dešifrirati samo tisti, ki mu je sporočilo namenjeno, vsem ostalim pa mora biti njegova vsebina nerazumljiva.

Šifriranje je uporabljal že Julij Cezar pred več kot 2000 leti, ko je pošiljal pošto Ciceru. Uporabljal je zelo enostaven postopek šifriranja. Vse črke v besedilu je zamenjal s črkami, ki so bile za tri mesta naprej v latinski abecedi. Beseda CESARUS je bila na ta način šifrirana v FHVDUAV. Cezar je uporabljal isti postopek tudi, ko si je dopisoval z drugimi prijatelji. Ker so morali vsi poznati postopek, da so lahko prebrali svojo pošto, jim je to omogočalo, da so prebrali tudi pošto namenjeno Ciceru. Nekdo, ki se danes ukvarja s šifriranjem, bi tak postopek z lahkoto razvozlal že na osnovi dveh do treh

šifriranih stavkov. Kljub tej enostavnosti je v tem postopku skrita osnovna ideja šifriranja.

Šifrirati je mogoče klasična in elektronska sporočila. Šifriranje in dešifriranje elektronskih sporočil je preprostejše, saj ta dva postopka opravi računalnik. Veda, ki se ukvarja s šifranjem sporočil (*kriptografija*) in z razkrivanjem šifriranih podatkov (*kriptoanaliza*) se imenuje *kriptologija*. Beseda izhaja iz grških izrazov: *kryptos logos* kar pomeni skrita beseda. Oglejmo si najprej nekatere osnovne pojme v kriptografiji.

## 2.1 Osnovni pojmi v kriptografiji

Namen kriptografije je načrtovanje šifrirnih in dešifrirnih algoritmov, s pomočjo katerih je mogoče zagotoviti osnovne lastnosti sporočil: zasebnost, verodostojnost, celovitost in preprečitev zanikanja.

Pri šifriranju (slika 1) gre za transformacijo *odprtega sporočila*[1] ali *čistopisa* (angl.plaintext) v nerazumljivo *šifrirano sporočilo* ali *tajnopis* (angl. ciphertext). Tovrstna transformacija, ki se običajno izvaja kar z računalnikom, poteka v skladu s *transformacijskimi tabelami* ali *šifrirnimi algoritmi* (angl. cipher). Šifrirni postopek mora biti reverzibilen, saj je le v tem primeru tajnopis mogoče dešifrirati oziroma transformirati nazaj v originalno odprto sporočilo.

Šifriranje in dešifriranje vhodnega sporočila poteka na osnovi *ključa*, ki mora biti tajen, kar pomeni, da ga sme poznati samo pošiljatelj sporočila in tisti, ki mu je sporočilo namenjeno. Ključ, ki mora biti povsem neodvisen od odprtega sporočila, tvorijo izbrane vrednosti parametrov šifrirnega oziroma *dešifrirnega algoritma* (angl. decipher).

## 2.2 Splošna klasifikacija kriptografskih sistemov

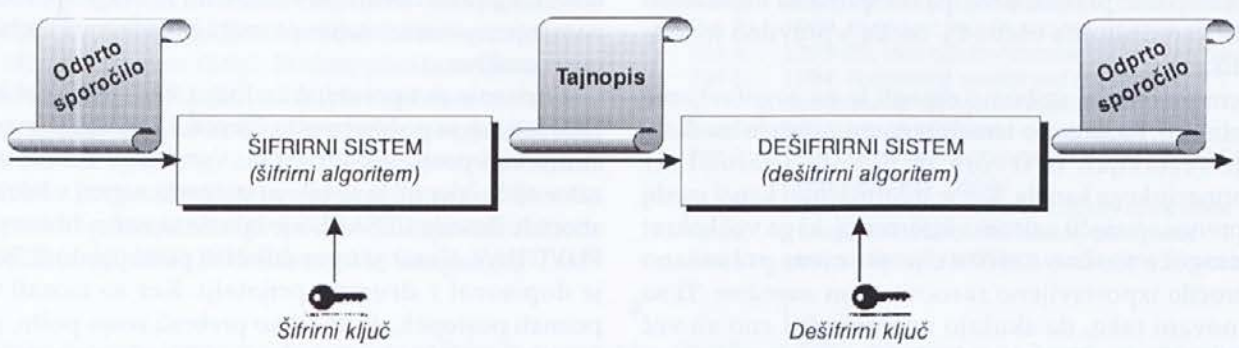
Kriptografske sisteme lahko klasificiramo (slika 2) po treh kriterijih [2]:

1. ***Število uporabljenih ključev.*** V primeru, da pošiljatelj in prejemnik uporabljata en sam ključ, govorimo o *simetričnem, enoključnem* ali *konvencionalnem šifriranju* (angl. symetric, single-key, secret key - conventional cipher), če pa uporabljata dva različna ključa, gre za *asimetrično, dvoključno šifriranje* ali *šifriranje z javnim ključem* (angl. asymetric, two-key, public key cipher).
2. ***Metoda šifriranja.*** Šifriranje sporočil se izvaja z različnimi metodami. Medtem, ko sta pri simetričnih sistemih uveljavljena predvsem principa *zamenjave* in *premeščanja*, se v asimetričnih sistemih šifriranje izvaja s posebnimi matematičnimi transformacijami. Pri zamenjavi se vsak element (bit, znak, skupina bitov ali znakov) v odprtem sporočilu preslika v drugi element, pri premeščanju pa se elementi odprtega sporočila prerazporejajo. Večina sistemov vsebuje več stopenj zamenjave in premeščanj.
3. **Velikost vhodnega bloka, ki ga uporablja šifrirna metoda.** Kriptografski sistem lahko šifrira ali dešifrira odprto sporočilo po blokih določene dolžine - v tem primeru govorimo o blokovnih šifrirnih sistemih (angl. Block cipher), obstajajo pa sistemi, ki odprto sporočilo šifrirajo ali dešifrirajo bit za bitom - tokovni šifrirni sistemi (angl. Stream cipher). Tovrstni shemi zasledimo v primeru simetričnih kriptografskih sistemov.

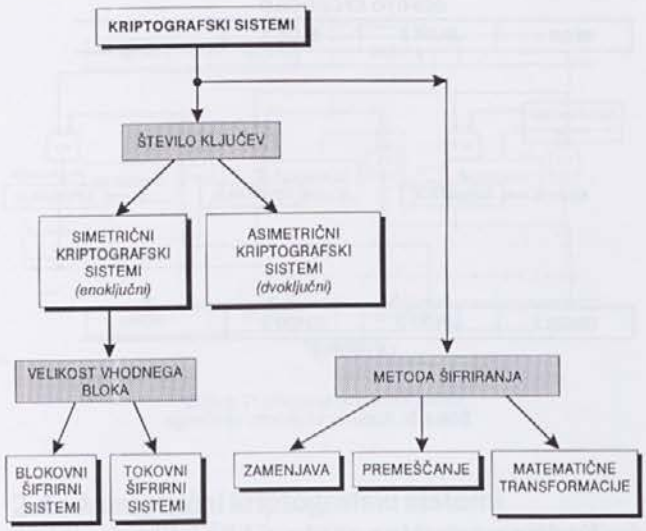
## 2.3 Simetrični kriptografski sistemi

Slika 3 prikazuje preprost model simetričnega kriptografskega sistema. Proces šifriranja poteka na osnovi šifrirnega algoritma in enega samega *tajnega ključa* (angl. Secret key). Izhod šifrirnega algoritma - tajnopis je po sprejemu potrebno transformirati nazaj v originalno odprto sporočilo, kar se izvede z dešifrirnim algoritmom in enakim ključem, kot je bil uporabljen pri šifriranju.

1 *Uporabljajo se tudi izrazi prikrito sporočilo, šifropis, ali kriptogram.*




**Slika 1:**
Kriptografski sistem sestavljata šifrirni in dešifrirni sistem. Tajnopis je mogoče uspešno dešifrirati samo v primeru poznanega dešifrirnega ključa.

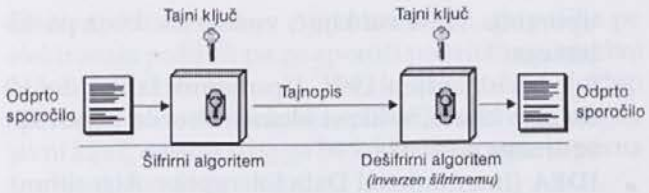



**Slika 2:** Splošna klasifikacija kriptografskih sistemov

Šifriranje in dešifriranje s simetričnimi algoritmi je običajno hitro, pojavi pa se problem varne izmenjave ključa med pošiljateljem in prejemnikom.

Oglejmo si pomembne elemente simetričnih kriptografskih sistemov nekoliko natančneje (slika 4). Šifrirni algoritem ima dva vhoda. Prvi je povezan z izvorom, ki tvori odprto sporočilo $M$, sestavljeno iz končne množice znakov - abecede[2]. Na drugem vhodu je ključ $K$, ki ga je potrebno po varnem kanalu distribuirati na ciljno stran - ponor. Za varno distribucijo ključa poskrbi pošiljatelj, obstaja pa možnost, da ključ izdela tretja oseba in ga pošlje na obe strani - izvor in ponor.

[2] *Danes se najpogosteje uporablja binarna abeceda [0, 1]*




**Slika 3:** Preprost model simetričnega kriptografskega sistema

Na osnovi odprtega sporočila $M$ in tajnega ključa $K$ šifrirni algoritem $E$ tvori tajnopis $C$:

$$C = E(M, K). \tag{1}$$

Tajnopis se po šifriranju odpošlje. Njegov prejemnik ga nato, s pomočjo dešifrirnega algoritma $D$, pretvori nazaj v odprto sporočilo $M$:

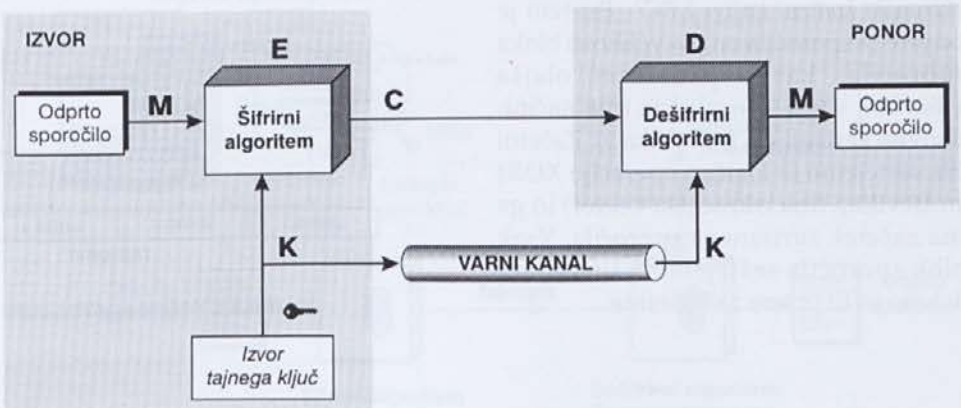
$$M = D(C, K) = D(E(M, K), K) \tag{2}$$

Najbolj znani simetrični kriptografski sistemi so [4]:

- **DES (Data Encryption Standard)** ali DEA (Data Encryption Algorithm), ki sta ga razvila NIST (National Institute of Standards and Technology) ter IBM.
- **RC2, RC4, RC5** - je razvil Ronald Rivest.

*RC2* se vgrajuje v nekatere programe (npr. Outlook Express), namenjene za delo z elektronsko pošto. Uporabljamo lahko ključe dolžine 1 do 2048 bitov razen za verzije, ki so namenjene uporabnikom zunaj ZDA. Za te verzije je ameriška vlada izdala zakon, s katerim je omejila ključ na največ 40 bitov.

*RC4* je tekoč šifrirni algoritem z spremenljivo dolžino ključa do 2048 bitov. Vgrajen je v Netscape-ov brkljalnik kot del protokola SSL. Ameriška verzija




**Slika 4:** Podrobnejši model simetričnega kriptografskega sistema

uporablja 128-bitni ključ, verzija za izvoz pa 40-bitnega.

*RC5* je bil objavljen 1994. Uporabnik lahko določi dolžino ključa, velikost bloka in število ponovitev šifrirnega postopka.

- **IDEA** (International Data Encryption Algorithm): razvila sta ga James L.Massey in Xuejia Lai v Zürichu in objavila leta 1990. Uporablja 128 bitov dolg ključ na 64 bitov dolgih blokih. Patent zanj ima Ascom-Tech iz Švice. Izven ZDA ga lahko uporabljamo brez plačila licenčnine. Če DES uporabljamo s trojnim ključem, je počasnejši od IDEA.
- **Skipjack:** algoritem, ki ga je razvila NSA (National Security Agency), je strogo zaščiten. Uporabljen je v šifrirnem čipu Clipper. Ključ je 80-biten. Vsak čip ima svoj ključ, katerega polovici sta shranjeni v različnih agencijah (key escrow agency).

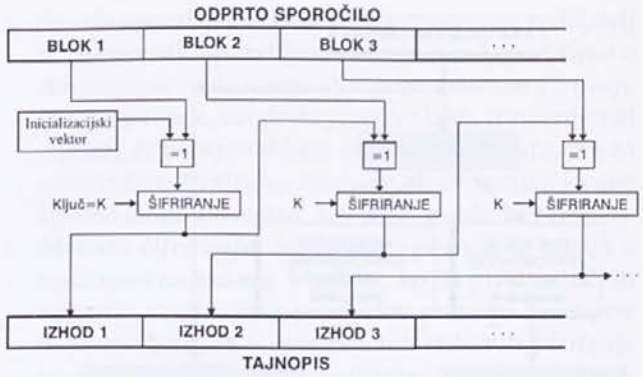
### 2.3.1 Tokovni in blokovni simetrični šifrirni sistemi

Pri *tokovnem* načinu šifriranja se sporočilo šifrira bit za bitom tako, da se kombinira bit ključa in bit sporočila - običajno je to kar logična operacija XOR. Če je uporabljen kratek, ponavljajoči ključ, postopek ni varen - s kombiniranjem šifriranega sporočila je razmeroma lahko ugotoviti najprej dolžino ključa, potem vrednost ključa in nato sporočilo dešifrirati. Nasprotno pa je sistem kriptografsko zelo robusten, če se ključ ne ponavlja in je povsem naključen niz bitov.

Večina algoritmov, ki se danes uporabljajo v civilnih organizacijah, je *blokovnih*: sporočilo se razbije na tako dolge bloke, kot zahteva algoritem, nato pa se vsak blok preoblikuje in kombinira s ključem. Permutacije, substitucije in kombinacije s ključem (npr. DES) morajo zagotoviti, da so v izhodnem bloku zabrisani vsi vzorci iz vhodnega bloka - skratka, da izgleda kot naključen niz bitov. Za vse simetrične algoritme velja, da se šifriranega sporočila ne da zgostiti za več kot nekaj odstotkov.

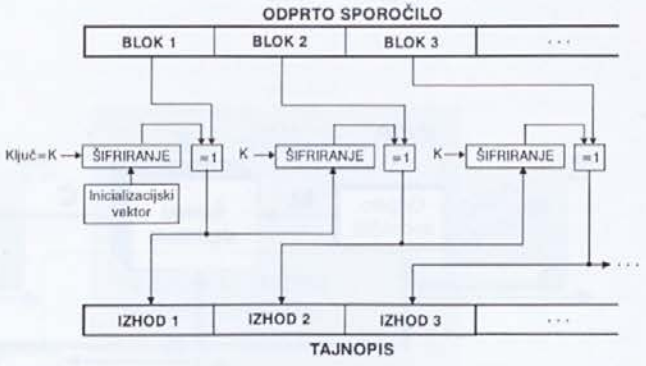
Pri blokovnih algoritmih je pomemben tudi način povezovanje blokov [5]. Če se šifrira vsak blok posebej, govorimo o *elektronski kodirni knjigi EBC*[3]. Pri tem je velikost bloka odprtega sporočila enaka velikosti bloka šifriranega sporočila, kar napadalcem olajša dešifriranje. Veliko bolj varni so naslednji trije načini:

- **Kodirno blokovno veriženje CBC**[4] (slika 5): Začetni blok sporočila seštejemo (z logično operacijo XOR) z naključnim številom (inicializacijski vektor) in ga postavimo na začetek šifriranega sporočila. Vsak naslednji blok sporočila seštejemo s šifriranim prejšnjim blokom in to potem zašifriramo.



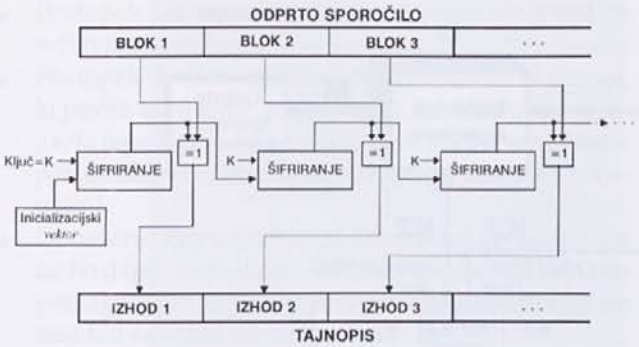

**Slika 5:** Kodirno blokovno veriženje

- **Kodirna povratna zanka CFB**[5] (slika 6): inicializacijski vektor zašifriramo s ključem in rezultat seštejemo (z logično operacijo XOR) s prvim blokom sporočila. Tako dobimo prvi šifrirani blok. To vsoto zašifriramo s ključem in tako dobimo začasni ključ. Temu prištejemo drugi blok sporočila... Vidimo, da pri tem načinu s šifriranjem pravzaprav spreminjamo ključ.
- **Izhodna povratna zanka OFB**[6] (slika 7): šifriranje je podobno prejšnjemu načinu. Inicializacijski vektor zašifriramo s ključem. Ta rezultat (recimo mu R1) seštejemo (z logično operacijo XOR) s prvim blokom sporočila in to je prvi šifrirani blok sporočila. Potem dobimo ključ za šifriranje naslednjega bloka tako, da R1 zašifriramo s prvotnim ključem... Od prejšnjega načina se razlikuje v tem, da začasni ključ, tvorjen s šifriranjem predhodnega ključa, ni odvisen od sporočila.




**Slika 6:** Kodirna povratna zanka

3 *Angl. Electronic Code Book*
4 *Angl. Cipher Block Chaining*
5 *Angl. Cipher Feedback*
6 *Angl. Output Feedback*




**Slika 7:** Izhodna povratna zanka

## 2.4 Asimetrični kriptografski sistemi

Problem varne izmenjave tajnega ključa pri simetričnih kriptografskih sistemih so rešili šele z uvedbo *asimetričnih kriptografskih sistemov* oziroma *kriptografskih sistemov z javnim*. Njihova prva predstavitev[7] leta 1976 je povzročila radikalne spremembe v dotedanjih kriptografskih sistemih. Za razliko od simetričnih sistemov, pri katerih se šifriranje/dešifriranje izvaja na osnovi zamenjav in transpozicij, temeljijo asimetrični sistemi na posebnih matematičnih funkcijah. Njihovo delovanje ni vezano le na enega, temveč na dva ločena ključa, s pomočjo katerih je mogoče zagotoviti ne le zasebnosti sporočil[8] temveč tudi verodostojnost in celovitost.

Pri kriptografskih sistemih z javnim ključem uporabnik kreira na svojem računalniku dva ključa: *zasebnega*[9] in *javnega*[10]. Javni ključ javno objavi na katerem od strežnikov z javnimi ključi, ga pošilja po elektronski pošti ali pa ga sporoči po telefonu, zasebni ključ pa drži v tajnosti. Vsi, ki mu hočejo poslati sporočilo, bodo za šifriranje sporočila uporabili njegov javni ključ, dešifriral pa ga bo lahko le on sam, ki pozna še svoj skriti zasebni ključ.

Na sliki 8 je prikazan preprost model kriptografskega sistema z javnim ključem, kjer pošiljatelj pošilja sporočilo prejemniku - Andreju. Sporočilo šifrira z Andrejevim javnim ključem, ki je v prostem dostopu na strežniku z javnimi ključi. Odposlan tajnopis bo lahko dešifriral samo Andrej, ki pozna svoj zasebni ključ.

S pomočjo slike 9 si oglejmo nekatere podrobnosti. Ponor B tvori par ključev: javnega *KJ* in zasebnega *KZ*. Medtem, ko je zasebni ključ *KZ* znan samo ponoru B, je ključ *KJ* javno objavljen kar pomeni, da je dostopen tudi izvoru A. Izvor A, ki namerava šifrirati odprto sporočilo *M* in ga poslati ponoru B, uporabi za šifriranje javni ključ *KJ* in šifrirni algoritem *E*. Odprto sporočilo *M* tako pretvori v tajnopis *C*:

$$C = E(M, KJ) \tag{3}$$

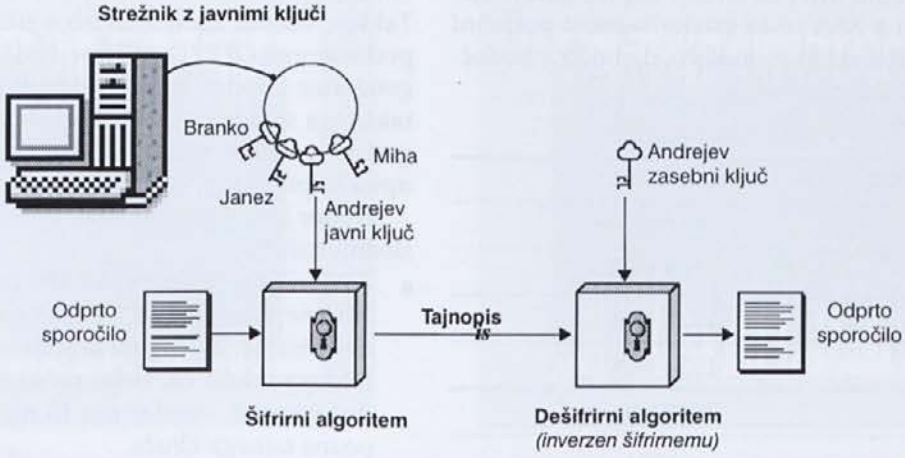
Ponor B tajnopis sprejme in ga s pomočjo dešifrirnega algoritma *D* in zasebnega ključa *KZ* pretvori nazaj v odprto sporočilo *M*:

$$M = D(C, KZ) = D(E(M, KJ), KZ) \tag{4}$$

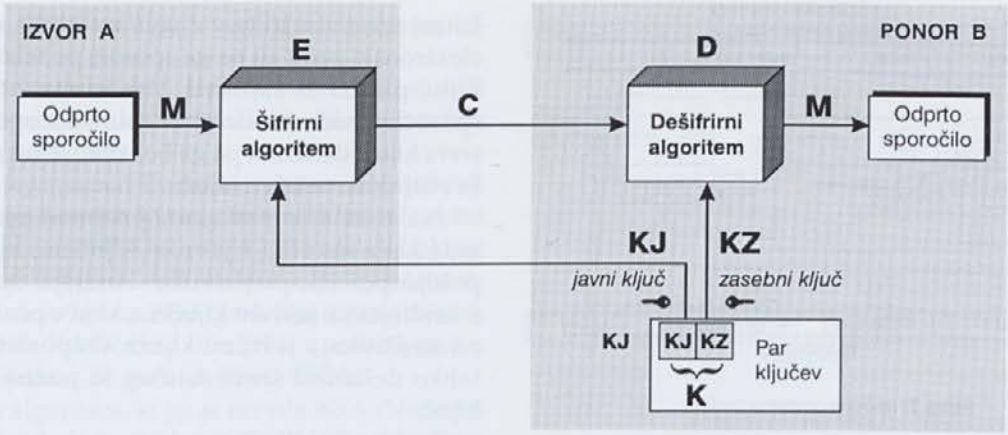
Šifrirni in dešifrirni algoritmi temeljijo na uporabi *navideznih enosmernih funkcij*[11], t.j. *enosmernih funkcij z vgrajeno pastjo*, za katere je značilno:

1. posamezna funkcijska vrednost $C=f(M,K)$ ima unikatni inverz $M=f^{-1}(C, K)$;
2. izračun funkcijske vrednosti $C=f(M,K)$ je enostaven, če sta *M* in *K* znana;

[7] *Predstavila sta ga W. Diffie in M. Hellman.*
[8] *Simetrični kriptografski sistemi v splošnem poskrbijo le za zasebnost sporočil.*
[9] *Angl. Private key*
[10] *Angl. Public key*
[11] *Angl. Trap-door one-way function.*




**Slika 8:** Preprost model asimetričnega kriptografskega sistema




**Slika 9:** Podrobnejši model asimetričnega kriptografskega sistema

3. izračun inverzne vrednosti $M=f^{-1}(C, K)$ je enostaven, če sta $C$ in $K$ znana;
4. inverzno vrednost $M=f^{-1}(C, K)$ je nemogoče izračunati, če je $C$ in $K$ neznan, kar pomeni, da enosmerne pasti ne moremo odpreti brez poznavanja ključa $K$.

Najbolj znana algoritma z javnim ključem sta [4]:

- algoritem **RSA**, poimenovan po svojih avtorjih (Ronald Rivest, Adi Shamir, Leonard Adleman) in patentiran v ZDA. Metoda temelji na zahtevni nalogi faktorizacije števila, ki je zmnožek dveh velikih praštevil.

  Na voljo je veliko komercialnih izvedb RSA (tako programskih kot strojnih). Uporabljajo se ključi daljši od 512 bitov. Za ameriške firme velja omejitev za izvoz: dobiti morajo dovoljenje vlade, ta pa običajno ne dovoli izvoziti programa, ki uporablja daljši ključ od 512 bitov. RSA Laboratories priporoča ključ 768 bitov za osebno uporabo, 1024 bitov za uporabo v organizacijah in 2048 bitov za ključe v izredno pomembnih operacijah.
- **ECC** (Elliptic Curve Cryptosystems) je algoritem, katerega matematična osnova so eliptične funkcije. V primerjavi z RSA so za enako varnost potrebni krajši ključi (tabela 1), zato kaže, da bodo v bodočnosti ti algoritmi prevladali.

| dolžina ključa ECC | dolžina ključa RSA |
|---|---|
| 106 bitov | 512 bitov |
| 132 bitov | 768 bitov |
| 160 bitov | 1024 bitov |
| 191 bitov | 1536 bitov |
| 211 bitov | 2048 bitov |

**Tabela 1:** Primerjava med dolžinami ključev, potrebnih za enako stopnjo varnosti pri RSA in ECC [4].

Leta 1990 so se razširile govorice, da ameriška vlada na predlog FBI in NSA pripravlja zakon, ki bo zelo omejil uporabo kriptografskih algoritmov [4]. Phil Zimmermann[12], računalniški strokovnjak, je kot odgovor na to napisal programski paket **PGP (Pretty Good Privacy)**, ki je brezplačen in uporablja simetrične in asimetrične algoritme, zgostitvene funkcije in vse, kar je potrebno za pošiljanje šifriranih sporočil po elektronski pošti. Poleg avtorja so ga dopolnjevali uporabniki po vsem svetu. Od verzije 5 naprej je možno izbirati med algoritmi RSA, Diffie-Hellman, IDEA in drugimi simetričnimi algoritmi.

## 2.5 Splošne lastnosti kriptografskih sistemov

Namen načrtovalcev kriptografskih sistemov je izdelati dober oziroma kakovosten kriptografski sistem. Kakovost se ocenjuje na osnovi njegovih lastnosti, ki so: varnost, hitrost, zanesljivost, enostavnost, cenenost, vzdrževalnost.

Ena izmed najpomembnejših lastnosti kriptografskih sistemov je njihova varnost. O popolni varnosti bi lahko govorili samo v primeru, če bi razpolagali z vsaj toliko ključi, kolikor odprtih sporočil želimo šifrirati [1]. Takšen, vendar zgolj teoretičen šifrirni sistem, je znan pod imenom *OTP* (One-Time-Pad). Njegova osnova je generator popolnoma naključnih števil. Ker v praksi takšnega sistema ni mogoče realizirati, velja kriptografski sistem za varnega, če se že dolgo časa uspešno upira kriptoanalizi svetovne strokovne javnosti.

Dober kriptografski sistem mora izpolnjevati naslednje zahteve:

- Zasebnost sporočil ne sme sloneti na tajnosti samega šifrirnega postopka temveč na tajnosti ključa za dešifriranje. Z drugimi besedami to pomeni, da ima lahko vsakdo na voljo računalniški program za dešifriranje, vendar mu to nič ne pomaga, če ne pozna tajnega ključa.

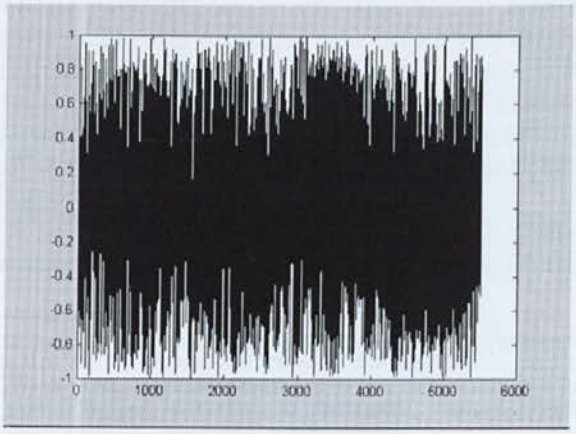
[12] *http://www.nai.com/products/security/phil/phil.asp*

- Postopek šifriranja in dešifriranja mora biti izvedljiv v čim krajšem času.
- Postopek dešifriranja mora biti enostaven za tistega, ki pozna tajni ključ, in praktično neizvedljiv za tistega, ki tega ključa ne pozna, četudi pozna sam postopek dešifriranja in ima na razpolago zmogljiv računalnik.
- Obnašanje kriptografskega sistema naj bo takšno, da ne bo dajalo napadalcu nobenih informacij, ki bi mu pomagale pri dešifriranju (npr. hitrost šifriranja ne sme biti odvisna od velikosti ključa).
- Vsi tajnopisi, ki jih tvori kripografski sistem, morajo imeti enake statistične lastnosti. Samo zamenjava vrstnega reda črk v tekstu temu ne ustreza, saj lahko napadalec s statistično analizo ugotovi, da je znak, ki se najbolj pogosto pojavlja, črka E (velja za slovenščino). Slika 10 prikazuje rezultate šifriranja dveh različnih tipov odprtih sporočil s kaotičnim kriptografskim sistemom, ki uporablja kaotično digitalno sito [6]. Izgled tajnopisov kaže, da se njune statistične lastnosti nekoliko razlikujejo.

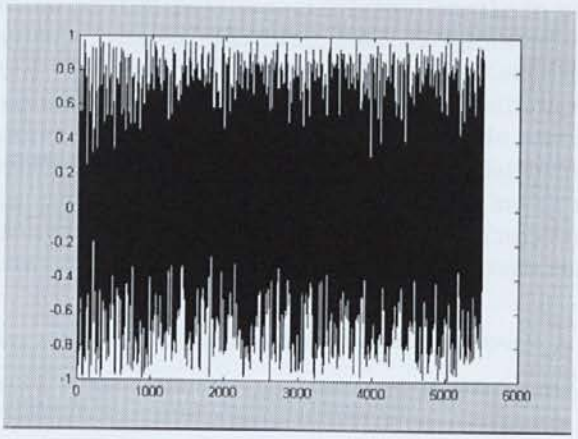
Na varnost kriptografskih sistemov vplivajo:

- *časovna zahtevnost šifrirnih in dešifrirnih algoritmov*: zasnova sodobnih kriptografskih sistemov je takšna, da prevede dešifriranje tajnopisa brez poznavanja ključa na zelo zahtevno računsko nalogo, ki zahteva za svoje reševanje zelo veliko časa. Zahtevnost algoritmov za šifriranje in dešifriranje je povezana z računsko zahtevnostjo [1], ki se ovrednoti glede na število osnovnih računskih operacij kot so npr. seštevanje, odštevanje, množenje, deljenje, primerjanje, itd.
  Problem, ki ga rešuje algoritem, je preprost, če je rešljiv v *polinomskem času* kar pomeni, da je pri $n$-bitnem vhodu v algoritem, čas za izračun izhodne vrednosti proporcionalen vrednosti $n^a$, pri čemer je $a$ konstanta [2]. Za takšne algoritme pravimo, da pripadajo razredu **P** - *polinomski*. Obstajajo pa še varnejši algoritmi, ki so povezani s precej zahtevnejšimi koncepti. To so algoritmi, ki pripadajo razredu **NP** - *nedeterministični polinomski razred* in se vgrajujejo v sodobne kriptografske sisteme (RSA). Njihova časovna zahtevnost je sorazmerna vrednosti $c^n$, kjer je c pozitivna konstanta, $n$ pa število bitov vhoda.
- *zasnova - struktura*: Stuktura blokovnih sistemov, ki uporablja dodatne načine povezovanja blokov (CBC, CFB ali OFB), se izkaže za precej varnejšo kot navadna struktura, ki šifrira vsak blok posebej (EBC). Struktura RSA sistema temelji na računsko zelo zahtevni operaciji faktoriziranja števil. Za tovrstno operacijo je bilo predstavljenih precej različnih algoritmov, za katere je značilno, da so izredno dolgotrajni. Razbijanje takšnih sistemov je zaradi tega zelo naporno oziroma nesmiselno.
- *dolžina uporabljenega ključa* in njegovo *distribuiranje*: daljši ključ pomeni večjo varnost. V mnogih primerih se z dolžino ključa veča tudi čas šifriranja in dešifriranja. Distribucija tajnega ključa med pošiljateljem in prejemnikom mora biti varna.
- *kakovost implementacije*: pomembno je, da so kriptografski sistemi pravilno implementirani z neokrnjenimi in kriptografsko analiziranimi verzijami šifrirnih in dešifrirnih algoritmov. Še tako dober algoritem ni varen, če ni pravilno implementiran.

Tudi hitrost šifriranja in dešifriranja vpliva na kakovost kriptografskega sistema. Delovanje kriptografskega sistema v realnem času v večini primerov zahteva aparaturno izvedbo. Primerjava hitrosti asimetričnih in simetričnih algoritmov kaže, da so asimetrični algoritmi neuporabni za masovno šifriranje podatkov, saj so precej počasnejši od simetričnih. Algoritem RSA je namreč 1000-5000 krat počasnejši od algoritma DES.




**a)** Šifriran sinusni signal




**b)** Šifrirana tekstovna datoteka

**Slika 10:** Primer šifriranja sinusnega signala in datoteke z istim ključem. Statistične lastnosti obeh tajnopisov niso povsem enake.

Vzdrževalnost kriptografskega sistema je odvisna od njegove zasnove in implementacije. Zelo priporočljivo je, da obstaja možnost enostavne spremembe:

- ključa in njegove dolžine
- dolžine vhodnih blokov (odprto sporočilo)
- šifrirnega in dešifrirnega algoritma (v primeru kasneje odkritih pomanjkljivosti).

Tovrstne spremembe naj ne bodo pogojene z zahtevnimi posegi v strojno opremo ali celo načrtovanjem nove, pač pa naj bo omogočeno programsko spreminjanje.

## 3. Zaključek

Kriptografski sistemi so imeli že v preteklosti pomembno vlogo, ki pa je bila omejena predvsem na vojaško področje. Ker je v računalniških omrežjih relativno enostavno prisluškovati, se je že zelo zgodaj pojavila potreba po kriptografskih sistemih. V prispevku smo prikazali koncepte najpomembnejših kriptograskih sistemov, ki se uporabljajo predvsem na področju računalniških komunikacij.

Noben kriptografski sistem ne zagotavlja popolne zasebnosti. Njihova kakovost je odvisna od vrste algoritma in kakovostne implementacije. Vsak napadalec se za napad odloči šele takrat, ko se stroški (napor) vloženi v napad povrnejo z vrednostjo prebrane informacije. Na podlagi te ugotovitve so zasnovani vsi kriptografski sistemi.

## Literatura


[1] N. Pavešić: *Informacija in kodi*, Univerza v Ljubljani, 1997.

[2] W. Stallings: *Cryptography and Network Security: Principles and Practice*, Second Edition, Prentice-Hall, 1999.

[3] S. Tomažič, M. Umek : *Varne komunikacije preko Interneta*, Zbornik posvetovanja Dnevi slovenske informatike, Portorož, 17.-20. april 1996. - Ljubljana: Slovensko društvo Informatika, 1996 - str. 214-222.

[4] Center vlade za informatiko: *http://www.sigov.si/tecaj/kripto/index.htm*, marec 1999.

[5] Eli Biham, Lars R. Knudsen, RSA Laboratories' CryptoBytes: *DES, Triple-DES and AES*, vol. 4, Number 1, Summer 1998.

[6] M. Šalamon, T. Dogša: *Kaos v digitalnem situ drugega reda*, Zbornik sedme Elektrotehniške in računalniške konference ERK '98, 24. - 26. september 1998, Portorož, - Ljubljana, Zv. A, str. 65-68.


◆


*Matej Šalamon je diplomiral leta 1994 na Fakulteti za elektrotehniko, računalništvo in informatiko v Mariboru, kjer je tudi zaposlen kot asistent za področje elektronskih vezij. Na raziskovalnem področju se ukvarja predvsem s kaotičnimi in kriptografskimi sistemi.*

*Tomaž Dogša je docent na mariborski Fakulteti za elektrotehniko, računalništvo in informatiko, kjer predava na dodiplomski in podiplomski stopnji in vodi Center za verifikacijo in validacijo sistemov. Na raziskovalnem področju se ukvarja s kriptografskimi sistemi in s preverjanjem programske opreme.*


◆