# NAPADI NA KRIPTOGRAFSKE SISTEME

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

**Izvleček**

V prispevku smo predstavili najpogostejše vrste kriptografskih napadov na simetrične in asimetrične kriptografske sisteme. Izbor vrste napada je odvisen od napadalcu razpoložljivih sestavnih delov kriptografskega sistema ter drugih informacij.

Primerjali smo odpornost simetričnih in asimetričnih kriptografskih sistemov, glede na dolžino uporabljenega ključa, obširneje pa smo predstavili napad z grobo silo. Navedli smo povprečni čas, ki ga posamezni napadalec ali skupine potrebujejo za preiskavo polovice vseh možnih ključev. V najslabšem primeru je lahko povprečni čas dvakrat daljši.

Opisali smo tudi napad na kriptografski sistem DES, v katerega je bilo leta 1999 z distribuiranim iskanjem tajnega ključa vlomljeno v rekordno hitrem času.

***Abstract***

***Attacks against Cryptographic Systems***

*In this article we describe most frequently used crypto attacks against conventional or symmetric and public-key or asymmetric cryptographic systems. Type of attack selection depends on availability of cryptographic system components and other information to attacker.*

*Resistance of symmetric and asymmetric cryptographic systems is compared due to used key length. Brute force attack is circumstantially presented and average time needed to search half of the symmetric key-space is stated. Worst-case scenario could be twice as long.*

*We also describe a year 1999 attack against DES, in which cipher was broken in record time using distributed key search.*

■ ■ ■

## 1. Uvod

**Zagotavljanje tajnosti podatkov je zopet postalo aktualno, ko so se po internetu začela pošiljati zaupna sporočila. Vsako poslovanje prek interneta zahteva tajnost, celovitost in avtentičnost sporočil. Internet omogoča zelo hiter prenos velikega števila sporočil, vendar tudi zelo enostavno prestrezanje sporočil. Kot odgovor na ta problem so nastali razni širfirni in dešifrirni sistemi, ki jim pravimo tudi kriptografski sistemi. Njihova osnovna naloga je zagotavljanje tajnosti prenašanega sporočila. Z določenimi dodatnimi postopki lahko zagotovimo tudi celovitost in avtentičnost sporočil ter preprečitev utaje avtorstva in sprejema sporočila. Nepooblaščeno osebo, ki se želi dokopati do vsebine sporočila ali ga spremeniti, bomo poimenovali napadalec. Prva naloga napadalca je, da se dokoplje do sporočila. Če je le-to šifrirano, potem ima na razpolago dve možnosti. Prva je, da z analizo šifriranega sporočila razvozla vsebino. Temu postopku pravimo kriptoanaliza. Drug pristop je kraja ključa, s katerim lahko sporočilo dešifrira.**

Pri kriptoanalizi nastopata dve konfliktni zahtevi. Prva je ta, da naj bodo kriptografski sistemi čim bolj varni, čim cenejši in vsakomur dostopni. Mnogo ljudi si želi popolno tajnost poslanih sporočil. Organizacije, ki se borijo proti kriminalu in protiobveščevalne organizacije pa tega vedno ne želijo, saj dobri kriptografski sistemi otežujejo njihovo delo. Te dileme ne bomo obravnavali v tem prispevku, ampak se bomo posvetili predvsem opisu raznih vrst napadov na kriptografske sisteme. Najprej bodo na kratko opisane tiste lastnosti kriptografskih sistemov, ki jih bomo v nadaljevanju potrebovali (podrobnejši opis glej v (Pavešić 1997). Obravnavane bodo splošne značilnosti napadov in primerjava med kriptografskimi sistemi glede njihove varnosti. Nato bo sledil kratek opis najpogostejših napadov.

## 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. Sisteme, ki omogočajo šifriranje in dešifriranje sporočil, imenujemo *kriptografski sistemi*.

Pri šifriranju gre za transformacijo *odprtega sporočila* v nerazumljivo *šifrirano sporočilo* ali *tajnopis*. Tovrstna transformacija, ki se običajno izvaja kar z računalnikom,

poteka v skladu s *transformacijskimi tabelami* ali *šifrirnimi algoritmi*. Šifrirni postopek mora biti reverzibilen, saj je le v tem primeru tajnopis mogoče dešifrirati, to je pretvoriti 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 in dešifrirnega algoritma. Če za šifriranje in dešifriranje uporabljamo enak ključ, potem takemu sistemu pravimo simetričen kriptografski sistem[1]. Pri asimetričnih sistemih[2] imamo poseben ključ za šifriranje, ki je javen. Le s privatnim ključem lahko tajnopis dešifriramo. Glede na dolžino podatkov, ki jih v algoritmu obdelujemo, ločimo tokovne in blokovne šifrirne sisteme. Pri tokovnih se odprta sporočila šifrirajo po bitih, pri blokovnih pa se sporočilo razdeli na več velikih blokov[3], ki se nato šifrirajo.

## 3. Splošne značilnosti napadov na informacijski kanal in na sporočila

Eden izmed pogostih napadov na informacijski kanal je onesposobitev prenosnega medija. To lahko dosežemo s fizičnim (blokiranje voda) ali programskim posegom (blokiranje strežnika). V določenih primerih je mogoče tudi prisluškovati ali spreminjati lastnosti informacijskega kanala (npr. povzročitev prekomerne obremenitve). Če pri napadu ostane sporočilo nespremenjeno, potem gre za pasiven napad. Med pasivne napade štejemo prisluškovanje (prestrezanje) in analizo prometa sporočil:

- **Prisluškovanje:** To je direkten napad na zasebnost, ki je izvedljiv, če ima napadalec dostop do informacijskega kanala. Če prisluškovanja fizično ni mogoče preprečiti, potem moramo sporočila ustrezno šifrirati.
- **Analiza prometa:** Napadalec skuša z analizo prometa in z analizo značilnosti sporočil ugotoviti določene podatke o pošiljatelju in prejemniku (npr. identiteto).

Ker pri pasivnih napadih običajno ne ostane nobena sled za napadalcem, je tak napad težko opaziti. Zelo enostavna in popolnoma neopazna sta prisluškovanje in analiza prometa v mejah lokalnega omrežja. Za napad na sporočila, ki se prenašajo po drugih omrežjih, je treba najprej vdreti v enega izmed strežnikov, ki so vključeni v določeno lokalno omrežje.

Aktivni napadi povzročajo modifikacijo sporočila (podatkovnega toka) ali pa ustvarjajo lažno sporočilo (podatkovni tok). Ker gre za spremenjena sporočila, lahko zaznamo prisotnost aktivnih napadov. Razdelimo jih v tri kategorije:

- **Spreminjanje:** gre za napad na celovitost sporočila, zaradi katerega je lahko sporočilo spremenjeno ali zakasnjeno. Primer takšnega napada je sporočilo "Dovoli **Maji**, da dostopa do bančnega računa" spremenjeno v "Dovoli **Branku**, da dostopa do bančnega računa".
- **Ponovno pošiljanje:** napadalec prekopira sporočilo in ga kasneje (ob neprimernem času) ponovno pošlje (npr. naročilo za nakup delnic, ukaz za umik brigade).
- **Spreminjanje lastnosti informacijskega kanala:** napadalec v celoti preprečuje, spreminja ali ovira normalno komuniciranje. Npr. napadalec zaustavi vsa sporočila namenjena določenemu cilju. Drugi primer je prekomerna obremenitev omrežja s sporočili, kar privede do njegovega zloma.
- **Pretvarjanje:** napadalec se pretvarja za pooblaščeno osebo in izkorišča njene privilegije. Primer pretvarjanja je zajetje gesla, s katerim se napadalec lažno identificira in s tem pridobi določene privilegije.

## 4. Napadi in vdori v kriptografski sistem

Kakor hitro je iz tajnopisa mogoče izločiti originalno, odprto sporočilo, govorimo o vdoru v kriptografski sistem. Vdor je posledica uspešnega kriptoanalitičnega napada ali pa kraje ključa. V splošnem je odpornost kriptografskega sistema odvisna od vrste napada, njegov izbor pa od: zasnove šifrirnega sistema, ključa (dolžine ključa, njegovega distribuiranja) in napadalcu razpoložljivih informacij. Odpornost kriptografskih sistemov lahko z vidika napadalca predstavimo s količino napora, ki ga je treba vložiti za vdora.

Pred napadom mora napadalec oceniti ali je izbrani sistem sploh smiselno napasti in kakšna je najprimernejša vrsta napada. Kriptografski sistem je *računsko varen* (Stallings 1999), če so stroški vdora (dešifriranja) večji od koristi dešifriranega sporočila. Ker vrednost sporočila s časom pada, mora napadalec oceniti tudi čas, potreben za vdor.

Temelj varnosti vsakega kriptografskega sistema je ustrezen algoritem. Kljub temu, da je odpornost algoritma možno oceniti, se pogosto izkaže, da je dejanska odpornost nižja od ocenjene. Vzrok za zmanjšanje

1 *Tipičen predstavnik simetričnih kriptografskih sistemov je sistem DES (Data Encryption Standard).*
2 *Najbolj znan asimetrični kriptografski sistem je sistem RSA, poimenovan po svojih avtorjih (Ronald Rivest, Adi Shamir, Leonard Adleman).*
3 *64 in več bitna beseda.*

odpornosti je v raznih napakah, ki so nastale pri implementaciji. Posledice napak se kažejo v raznih hibah programske in strojne opreme. Poznavanje teh hib lahko zelo zmanjša varnost kriptografskega sistema. Prisotnost hib ugotavljamo z raznimi postopki preverjanja (npr. testiranje, formalno dokazovanje, itd.) (Dogša 1993). Ker so stroški testiranja zelo visoki, je zelo malo kriptografskih sistemov, ki bi bili izredno dobro preverjeni. Problem visokih stroškov testiranja izdelovalci kriptografskih sistemov rešujejo z distribuiranim testiranjem. V javnosti objavijo nekaj tipičnih informacij, ki so običajno napadalcu znane (npr. tajnopis, del odprtega sporočila in šifrirni algoritem[4]) in nato razpišejo visoko nagrado za vdor[5]. Pogosto mora napadalec tudi pojasniti svojo metodo, če želi prejeti nagrado. Z odpravljanjem najdenih napak, se veča varnost kriptografskega sistema. Mnogi so mnenja, da so zadovoljivo preverjeni le sistemi, ki so bili podvrženi distribuiranemu testiranju.

Tabela 1 prikazuje zanimivo primerjavo med odpornostjo simetričnih in asimetričnih kriptografskih sistemov, glede na dolžino uporabljenega ključa. Vidimo lahko, da je potreben za enako odpornost za simetrične šifrirne sisteme bistveno krajši ključ kot za asimetrične.

Vsaka informacija o kriptografskem sistemu in sporočilu pomaga napadalcu. Vrsta napada je odvisna od količine in vrste napadalcu razpoložljivih sporočil, njegovega znanja in računalniške podpore. Napadalcu lahko pomagajo zlasti naslednje informacije: vrsta algoritma, vsebina sporočila, vrsta sporočila (besedilo, slika, program itd.), jezik, v katerem je napisano sporočilo, statistične lastnosti jezika. S prikrivanjem teh informacij lahko dvigujemo varnost kriptografskega sistema. Napadalcu pri napadu koristita poznavanje določenih informacij in posedovanje sestavnih delov ali celotnega kriptografskega sistema:

- **skrivalni algoritem:** napadalec sumi, da je v množici sporočil skrit[6] tudi tajnopis. Npr. v eni izmed 100 slik je skrito sporočilo. Brez poznavanja skrivalnega algoritma napadalec ne more odkriti skritega sporočila, ki je lahko odprto ali šifrirano (Johnson, Jajodia 1998).
- **en tajnopis:** napadalec ima na razpolago samo tajnopis brez pripadajočega odprtega sporočila. Napadi, ki temeljijo samo na enem tajnopisu, so zelo redko uspešni. Eden izmed napadov, ki ga je možno izvesti tudi z delom tajnopisa, je napad z grobo silo[7], pri katerem napadalec poskuša vdreti sistematično - s preskušanjem vseh možnih ključev.
- **segmente odprtega sporočila in pripadajoče tajnopise.** Npr. v razpisu za napad na kriptografski sistem DES je bil znan tajnopis in začetek sporočila. Tudi v tem primeru je možno uporabiti napad z grobo silo.
- **šifrirni sistem,** s katerim lahko napadalec generira tajnopise, vendar ne pozna ključa, ker je le-ta npr. vgrajen v sistem. Napadalec lahko tvori poljubno število odprtih sporočil in tajnopisov in uporabi diferencialno analizo, kjer s premišljeno izbranimi sporočili[8] sklepa o pravilnosti ključa.
- **končno število tajnopisov in dešifrirni sistem,** vendar ne pozna ključa. Na podlagi analize tajnopisa in dešifriranega sporočila sklepa o uspešnosti napada. Napadi s tovrstnimi informacijami so običajni za asimetrične kriptografske sisteme.
- **celotni kriptografski sistem,** vendar ne pozna tajnega ključa. Napad lahko izvede s pomočjo izbranih odprtih sporočil in pripadajočih tajnopisov, ima pa tudi možnost izbire tajnopisov in pripadajočih dešifriranih sporočil. Na osnovi tega sklepa o pravilnosti izbranega ključa. Ta primer zelo redko nastopa.

V navedenih kategorijah količina informacij, katere napadalec pozna, narašča. Če napadalec uspe vdreti le s poznavanjem samo enega tajnopisa, potem velja, da je kriptografski sistem slab. Za vdor v večino dobrih šifrirnih sistemov je potrebnih več informacij.

| Simetrični šifrirni sistem | ASIMETRIČNI šifrirni sistem | |
|---|---|---|
| | RSA | ECC (Elliptic Curve Cryptosystem) |
| 40 bitov | 274 bitov | 57 bitov |
| 56 bitov | 384 bitov | 80 bitov |
| 64 bitov | 512 bitov | 106 bitov |
| 80 bitov | 768 bitov | 132 bitov |
| 96 bitov | 1024 bitov | 160 bitov |
| 112 bitov | 1792 bitov | 185 bitov |
| 120 bitov | 2048 bitov | 211 bitov |
| 128 bitov | 2304 bitov | 237 bitov |

**Tabela 1:**
**Primerjava med dolžinami ključev potrebnih za enako stopnjo odpornosti v simetričnih in asimetričnih sistemih (Moscaritolo 1999).**

4 *Izvršljivo kodo.*
5 *Primer: poziv, ki ga je razpisal laboratorij RSA za napad na kriptografski sistem DES - DES Challenge III: http://www.rsa.com/rsalabs/des3/*
6 *Veda, ki se ukvarja metodo skrivanja podatkov, se imenuje steganografija.*
7 *Angl.: brute force attack – exhaustive search.*
8 *Sorodna sporočila z določenimi razpoznavnimi vzorci.*

Kriptografski napadi se delijo (slika 1) glede na strukturo kriptografskega sistema, napadalcu razpoložljivih informacij in sestavnih delov kriptografskega sistema.

## 4.1 Najpomembnejši napadi na blokovne simetrične kriptografske sisteme

Za blokovne kriptografske sisteme je značilno, da šifrirajo naenkrat velik blok podatkov. Takšen princip varuje pred različnimi statističnimi analizami, s pomočjo katerih je mogoče sklepati o vrsti odprtega sporočila in informacijah, ki jih vsebuje. Kljub temu pa obstaja nekaj vrst napadov, ki so pri tovrstnih kriptografskih sistemih lahko zelo uspešni.

### 4.1.1 Napad z grobo silo - obširno iskanje tajnega ključa

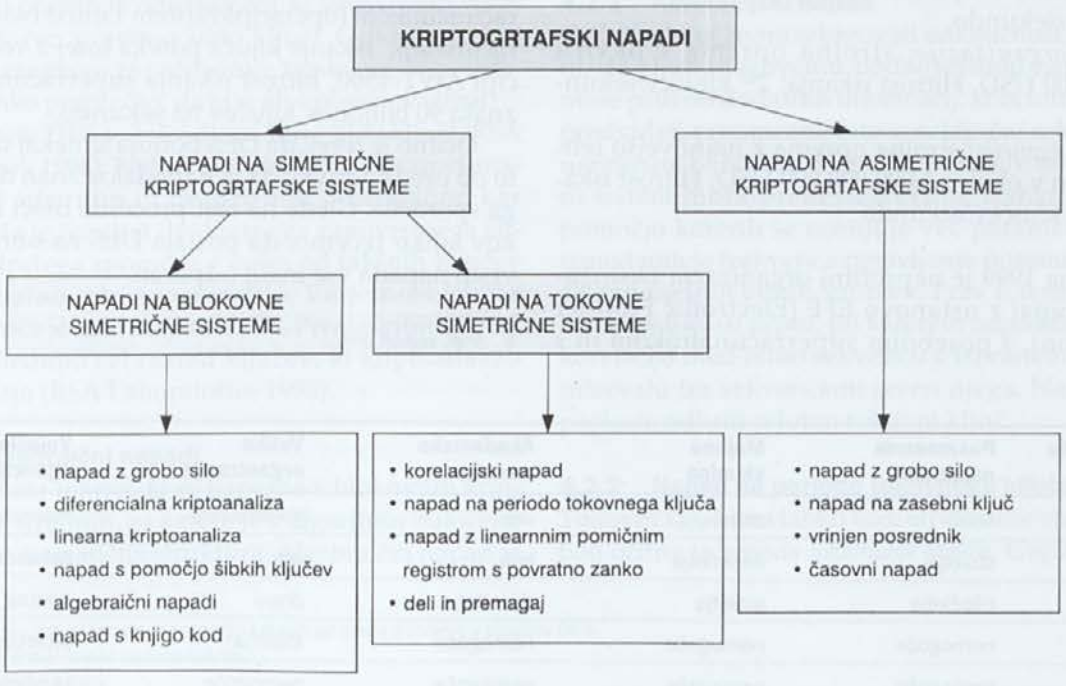
Obširno iskanje ključa, znano kot napad z grobo silo, je najpreprostejša kriptoanalitična tehnika, ki omogoča identifikacijo pravilnega tajnega ključa na osnovi poskusov z vsemi možnimi ključi. Pogoj za izvedbo tega napada je, da napadalec pozna:

- majhen del odprtega sporočila in pripadajoči tajnopis ali
- samo tajnopis, pri čemer mora imeti odprto sporočilo določene prepoznavne karakteristike.

Sam postopek je sestavljen samo iz treh korakov: izbor ključa, poskusno dešifriranje in ugotavljanje uspešnosti. Prva dva koraka je možno enostavno avtomatizirati, medtem ko lahko tretji v nekaterih primerih pomeni velik problem. Uspešnost, to je pravilnost ključa se kaže v tem, da je dešifrirano sporočilo smiselno. Če je znan vsaj del odprtega sporočila, potem je ugotavljanje ključa zelo hitro in enostavno. V kolikor napadalec dela odprtega sporočila ne pozna, lahko o njem ugiba, npr. mnogi dopisi se začnejo s »Spoštovani«. Če nima nobenih podatkov o sporočilu, je ugotavljanje uspešnosti ključa najdolgotrajnejši korak. Če ne pozna niti jezika, v katerem je napisano sporočilo, ali če gre za digitalno sliko, potem je napad z grobo silo največkrat neuspešen.

Napad z grobo silo je mogoče izvesti s strojno ali programsko opremo. Primeren je za odkrivanje tajnih ključev konstantne dolžine v simetričnih in asimetričnih kriptografskih sistemih. Ker je zelo obširen, zahteva ogromno časa in uporabo izjemno hitrih računalnikov. Napad na DES s 56-bitnim ključem bi namreč kljub uporabi danes najhitrejšega računalnika lahko trajal več sto let. Večjo računalniško moč je možno doseči z distribuirano kriptoanalizo. Iskanje ključa je razdeljeno na večje število računalnikov, ki so povezani v mrežo. Pri distribuiranem iskanju ključa vsak računalnik obravnava le del množice možnih ključev.

Tabela 2 prikazuje povprečni čas, potreben za vdor v simetričen kriptografski sistem. Uporabljena sta dva parametra: velikost ključa in hitrost preizkušanja. Če je hitrost 1 ključ/ms, pomeni, da mora računalnik v eni




**Slika 1: Vrste kriptografskih napadov.**

| Velikost ključa | Število vseh možnih ključev | Čas za preiskavo polovice vseh možnih ključev: Hitrost dekodiranja: 1 ključ/μs | Čas za preiskavo polovice vseh možnih ključev: Hitrost dekodiranja: $10^7$ ključev/μs |
|---|---|---|---|
| 32 bitov | $2^{32} = 4.3 \cdot 10^9$ | $2^{31}$ μs = 35.8 min | 2.15 ms |
| 56 bitov | $2^{56} = 7.2 \cdot 10^{16}$ | $2^{55}$ μs = 1142 let | 10.01 ur |
| 128 bitov | $2^{128} = 3.4 \cdot 10^{38}$ | $2^{127}$ μs = $5.4 \cdot 10^{24}$ let | $5.4 \cdot 10^{18}$ let |

**Tabela 2: Povprečni čas potreben za napad z grobo silo pri dveh različnih hitrostih iskanja (Stallings 1999).**

mikrosekundi generirati ključ, izvesti poskusno dešifriranje in ugotoviti uspešnost ključa. Tabela 3 prikazuje povprečni čas, ki ga potrebujejo posamezni napadalec ali skupine za preiskavo polovice vseh možnih ključev. V najslabšem primeru se seveda ti časi podvojijo.

Tabela 3 temelji na predpostavkah iz leta 1997:

- *posamezni napadalec:* samostojen računalnik z ustrezno programsko opremo. Hitrost iskanja: $2^{17}$-$2^{24}$ ključev/sekundo.
- *majhna skupina*: 16 računalnikov z ustrezno programsko opremo. Hitrost iskanja: $2^{21}$-$2^{24}$ ključev/sekundo.
- *akademsko omrežje*: 256 računalnikov z ustrezno programsko opremo. Hitrost iskanja: $2^{25}$-$2^{28}$ ključev/sekundo.
- *velike organizacije*: strojna oprema v okviru 1.000,000 USD. Hitrost iskanja: $2^{43}$ ključev/sekundo.
- *vojaške agencije*: strojna oprema z najnovejšo tehnologijo v okviru 1.000.000,000 USD. Hitrost iskanja: $2^{55}$ ključev/sekundo.

19. januarja 1999 je neprofitni organizaciji *Distributed.net*, skupaj z ustanovo EFF (Electronic Frontier Foundation), s posebnim superračunalnikom in s približno 100.000 osebnimi računalniki povezanih prek Interneta, uspelo postaviti hitrostni rekord v odkrivanju 56-bitnega DES-ovega ključa. Znan je bil tajnopis in začetek odprtega sporočila *"See you in Rome (second AES Conference, March 22-23, 1999)"*. Med 72,057,594,037,927,936 možnimi ključi jim je z akcijo *DES III Deep Crack* uspelo odkriti pravega v 22 urah in 15 minutah. Superračunalnik so zgradili na osnovi strogo namenskega čipa AWT-4500 Deep Crack, ki ga je izdelala firma AWT (Advanced Wireless Technologies). Čip se sestoji iz 24. identičnih iskalnih enot[9], ki delujejo z uro frekvence 40MHz in zmore testirati 60 milijonov ključev na sekundo (Kocher 1998). 64 takšnih čipov sestavlja, skupaj z ustrezno logiko za upravljanje, posebno matično ploščo. 29 takšnih plošč predstavlja šest računalnikov, ki skupaj s krmilnim PC računalnikom (operacijski sistem Linux) tvorijo superračunalnik. Iskanje ključa poteka torej z več kot 1800 čipi AWT-4500, hitrost iskanja superračunalnika pa znaša 90 bilijonov ključev na sekundo.

Očitno je torej, da DES ponuja le nekaj urno zaščito ob predpostavki, da je napadalcu znan del odprtega sporočila. Glede na rast procesne moči računalnikov lahko rečemo, da postaja DES na obravnavano vrsto napada vse manj odporen.

9 *Angl. search unit.*

| Dolžina ključa | Posameznik napadalec | Majhna skupina | Akademsko omrežje | Velike organizacije | Vojaške agencije |
|---|---|---|---|---|---|
| 40 bitov | tedni | dnevi | ure | milisekunde | mikrosekunde |
| 56 bitov | stoletja | desetletja | leta | ure | sekunde |
| 64 bitov | tišočletja | stoletja | desetletja | dnevi | minute |
| 80 bitov | nemogoče | nemogoče | nemogoče | stoletja | stoletja |
| 128 bitov | nemogoče | nemogoče | nemogoče | nemogoče | tisočletja |

**Tabela 3: Povprečni čas, ki ga porabi posameznik ali skupina za preiskavo polovice vseh možnih ključev (Moscaritolo 1999).**

#### 4.1.2 Diferencialna kriptoanaliza

Gre za zahteven in kompleksen napad, pri katerem ima napadalec šifrirni sistem, vendar ne pozna ključa (Ritter 2001). Šifrirni sistem napade tako, da izbira dve sorodni odprti sporočili in analizira dobljena tajnopisa. Pri tem pričakuje, da bo tudi v pripadajočih tajnopisih mogoče zaslediti podobnost, na osnovi katere bi lahko sklepal o ključu. S skrbno iterativno analizo dobljenih podatkov določi verjetnosti možnih ključev. Z najbolj verjetnim poskusi dešifrirati enega izmed tajnopisov.

#### 4.1.3 Linearna kriptoanaliza

To je napad, pri katerem napadalec razpolaga z odprtimi sporočili, ki jih sam ne more poljubno izbirati, ter pripadajočimi tajnopisi (Ritter 2001). Do posameznih informacij o ključu pride na osnovi zadostnega števila parov odprtih sporočil in pripadajočih tajnopisov. Večje število takšnih parov poveča verjetnost uspešnega napada. Linearna kriptoanaliza sistema DES poteka tako, da poskuša napadalec na osnovi razpoložljivih parov vzpostaviti statistično linearno povezavo med vhodnimi in izhodnimi biti posamezne S-škatle[10].

Elementi diferencialne in linearne kriptoanalize so združeni v novi obliki napada, imenovani *diferencialno-linearna kriptoanaliza*[11].

#### 4.1.4 Napad s pomočjo šibkih ključev

Znano je, da je varnost nekaterih kriptografskih sistemov odvisna tudi od vrednosti izbranega ključa. Pri nekaterih vrednostih se kriptografski sistem odzove z določenim pravilnim obnašanjem, ki lahko olajša vdor. Takim ključen pravimo šibki ključi. Odkritje šibkih ključev je zanimivo za načrtovalce kriptografskega sistema, saj lahko preprečijo, da bi si jih uporabnik izbral.

Za sistem DES so bili odkriti štirje šibki ključi (RSA Laboratories 1998). Njihov slučajni izbor povzroči enakost med šifrirnim in dešifrirnim postopkom, kar pomeni, da je rezultat dvakratnega zapovrstnega šifriranja odprtega sporočila z enim od takšnih ključev kar originalno odprto sporočilo. Verjetnost izbora takega ključa je zelo majhna ($2^{-52}$). Pri algoritmu IDEA lahko zasledimo cel razred ključev, ki kriptoanalizo zelo olajšajo (RSA Laboratories 1998).

#### 4.1.5 Algebraični napadi

To je skupina tehnik, ki so uspešne v blokovnih kriptografskih sistemih, za katere je v algoritmu določena značilna matematična struktura. Algebraični napad je lahko zelo uspešen v primeru kriptografskega sistema, ki ga je mogoče razdeliti na posamezne podstrukture. Napadalec napada posamezno podstrukturo in na ta način poskuša vdreti v celotni sistem. Pojavi pa se vprašanje, ali je neki šifrirni sistem sploh mogoče predstaviti s podstrukturami. Za DES je znano, da to ni mogoče.

#### 4.1.6 Napad s knjigo kod[12]

Napadalec zbira odprta sporočila s pripadajočimi tajnopisi, tvorjenimi z istim ključem. Ko zasledi tajnopis, ki ga ima v svoji knjigi kod, odkrije njemu pripadajoče odprto sporočilo. Tovrstni napad je primeren za napad na blokovne šifrirne sisteme, saj je le v tem primeru mogoče kontrolirati njegovo kompleksnost, ki zavisi od velikosti uporabljenih blokov in s tem števila elementov v knjigi kod.

### 4.2 Najpomembnejši napadi na tokovne simetrične kriptografske sisteme

Najobičajnejša varianta šifriranja s tokovnim kriptografskim sistemom je kombinacija tokovnega ključa[13] in odprtega sporočila. Tokovni ključ se generira na osnovi tajnega ključa. To je naključna sekvenca bitov, ki se na bitnem nivoju kombinira[14] z biti odprtega sporočila. Večina napadov na tovrstne sisteme je *ad hoc*, sicer pa so znani (RSA Laboratories 1998, 1995): korelacijski napad, napad na periodo tokovnega ključa, napad z linearnim pomičnim registrom s povratno zanko[15], deli in premagaj.

#### 4.2.1 Korelacijski napad

Tokovni ključ mora izkazovati naključnost, kar pomeni, da kljub njegovemu podaljševanju napadalec ne more priti do dodatnih informacij, ki bi mu omogočile predvideti posamezne bite v naključni sekvenci - generiranem tajnopisu. Varen in zanesljiv tokovni šifrirni sistem mora prenesti številne *statistične teste*, s pomočjo katerih se ocenjuje več parametrov. Eden izmed njih je frekvenca pojavljanja posameznih bitov ali zaporednih bitnih vzorcev. Prav ti testi so osnova za t.i. *korelacijski napad*, pri katerem napadalec preverja korelacijo med bitno sekvenco v izbranem časovnem intervalu ter sekvencami izven njega. Na tej osnovi poskuša odkriti celoten tokovni ključ.

#### 4.2.2 Napad na periodo tokovnega ključa

Tokovni ključ ima lahko tudi strukturne slabosti. Najbolj očitna je *perioda tokovnega ključa*. Gre za primere,

10 Angl. S-box – gre za tabele, s pomočjo katerih se izvaja šifriranje v sistemu DES.
11 Angl. differential-linear cryptoanalysis.
12 Angl. codebook attack.
13 Angl.keystream.
14 Običajno se izvaja logična operacija XOR.
15 Angl. linear feedback shift register.

pri katerih prihaja do prehitrih ponovitev določenega število bitov v tokovnem ključu. Razlog za to je prekratek tokovni ključ. Napadalec poskuša odkriti določen del tokovnega ključa - periodo, ki bi mu omogočil dešifrirati določene dele tajnopisa. Tovrstni napad opozarja, da je pri načrtovanju tokovnih šifrirnih sistemov treba paziti na minimalno periodo tokovnega ključa ali izbrati ustrezno vrednost njene spodnje meje.

#### 4.2.3 Napad z linearnim pomičnim registrom s povratno zanko

Določene strukturne slabosti so lahko celo tako velike, da ponujajo napadalcu možnosti iskanja alternativnih poti za generiranje dela tokovnega ključa ali tokovnega ključa v celoti. Vodilni tovrstni pristop, ki omogoča reprodukcijo (izdelavo kopij) tokovnih ključev, je uporaba *linearnega pomičnega registra s povratno zanko*. Ta deluje tako, da na svojem vhodu prebere končno sekvenco bitov, na izhodu pa to sekvenco ponovno generira. Pri tem je pomembna dolžina registra, od katere zavisi dolžina prebrane ter kasneje ponovno generirane sekvence.

Varnost šifrirnega sistema se meri na osnovi *linearne kompleksnosti* sekvence, ki je določena z velikostjo linearnega pomičnega registra s povratno zanko, potrebnega za reprodukcijo te iste sekvence. Tokovni šifrirni sistem mora imeti torej čim večjo linearno kompleksnost.

#### 4.2.4 Deli in premagaj

Razen iskanja ključa s pomočjo napada z grobo silo je znan tudi razred napadov, ki jih lahko opišemo z izrazom *deli in premagaj*[16]. V primeru tokovnih šifrirnih sistemov gre za napad na tokovni ključ, ki se generira na osnovi izbranega tajnega ključa. Napadalec uspe zajeti del tokovnega ključa in na osnovi tega prične z ugotavljanjem celotnega tajnega ključa. Z grobo silo napada posamezne dele tajnega ključa, pri čemer poskuša identificirati tisti del, ki ima zelo očiten in neposreden učinek na generiran tokovni ključ. Napad je tem uspešnejši, čim bolj se napadalcev tokovni ključ ujema z dejansko prisotnim tokovnim ključem. Rezultati napada *deli in premagaj* so lahko v pomoč tudi pri izvajanju zelo hitrih in učinkovitih korelacijskih napadov.

### 4.3 Najpomembnejši napadi na asimetrične kriptografske sisteme

Nekateri najpomembnejši napadi na asimetrične kriptografske sisteme so: napad z grobo silo, napad na zasebni ključ, vrinjeni posrednik[17] (MITM), časovni napad[18].

#### 4.3.1 Napad z grobo silo

Podobno kot simetrične je tudi asimetrične kriptografske sisteme možno učinkovito napasti z grobo silo. Protiukrep je tudi tukaj enak: uporabiti je treba čim daljše ključe. Sistemi z javnimi ključi temeljijo na inverznih matematičnih funkcijah, katerih računska kompleksnost ne narašča linearno z dolžino ključa, ampak običajno precej hitreje. Ključ mora biti dovolj dolg, da napad z grobo silo ni praktičen, po drugi strani pa dovolj kratek, da sta šifriranje in dešifriranje dovolj hitra.

#### 4.3.2 Napad na zasebni ključ

Napadalec poskuša na osnovi znanega javnega ključa generirati pripadajoči zasebni ključ. Ta napad je izredno zahteven, saj je povezava med javnim in zasebnim ključem zelo zapletena. Pri sistemu RSA temelji tovrstna povezava na faktoriranju velikih praštevil, kar je izredno dolgotrajen postopek.

#### 4.3.3 Vrinjeni posrednik

To je napad, kjer se napadalec (oseba C) pojavlja kot posrednik (man-in-the middle) med pošiljateljem (oseba A) in prejemnikom (oseba B). Če želi zavzeti vlogo posrednika, mora imeti možnost prestrezanja sporočila, ki je namenjeno osebi B. Princip napada je naslednji: napadalec objavi svoj javni ključ in se pri tem izdaja za osebo B. Kadar želi oseba A poslati šifrirano sporočilo osebi B, uporabi njen javni ključ, ki pa je dejansko ključ napadalca - osebe C. Na ta način napadalec sprejema šifrirana sporočila, ki jih lahko brez težav dešifrira s svojim zasebnim ključem. Ko prebere sporočilo, ga šifrira s pravim javnim ključem osebe B in ji ga pošlje. Tovrstni napad se preprečuje s t.i. *potrditvijo* javnega ključa.

#### 4.3.4 Časovni napad

Gre za zelo sodoben, računsko nezahteven in precej neopazen napad. Šifriranje različnih sporočil običajno traja različno dolgo. Če lahko napadalec meri čas, potreben za izvajanje šifrirne operacije, lahko pride na osnovi ponovljivih meritev in z uporabo verjetnosti in statistike, do pomembnih informacij o tajnem ključu, s katerimi se opravljajo šifrirni izračuni. Časovni napad je posebej nevarna oblika napada, saj zahteva le tajnopis. Deluje dobro tudi, če meritve niso posebej natančne. Uporablja se pri napadih na RSA, Diffie-Hellmanovo metodo in metode, ki temeljijo na

16 Angl. *divide and conquer.*
17 Angl. *man-in-the middle*
18 Angl. *timing attack.*

eliptičnih funkcijah. Proti časovnim napadom na RSA sta predlagana dva načina obrambe: dodajanje naključnih zakasnitev v računski del algoritma in dodatno predhodno šifriranje z nekim drugim algoritmom.

## 5. Sklep

Za absolutno preprečitev napadov bi bilo treba zagotoviti stalno fizično zaščito celotnega komunikacijskega sistema, kar pa je večinoma nemogoče (npr. internet, telefonsko omrežje,...). Dejavnosti, ki jih lahko uporabimo za reševanje opisane problematike, lahko razdelimo v naslednje kategorije: fizična preprečitev dostopa, odkrivanje napada, onemogočanje napada. Z zaščitnimi strežniki lahko zavarujemo lokalni del omrežja pred zunanjimi napadalci. Če smo zaznali napad in imamo tudi varnostne kopije sporočil, potem je možna tudi njihova rekonstrukcija.

Vsaka informacija o kriptografskem sistemu in sporočilu pomaga napadalcu. Vrsta napada je odvisna od količine in vrste napadalcu razpoložljivih sporočil, njegovega znanja in računalniške podpore. S prikrivanjem nekaterih podatkov o kriptografskem sistemu in sporočilu lahko povečujemo varnost kriptografskega sistema. Praviloma bo do napada prišlo, ko bo napadalec ocenil, da so stroški vdora (dešifriranja) manjši od koristi dešifriranega sporočila. Ker vrednost sporočila s časom pada, mora oceniti tudi, koliko časa potrebuje.

Ker se bosta kriptoanaliza in hitrost računalnikov neprestano dvigovala na višjo raven, bo treba tudi neprestano vzdrževanje kriptografskih sistemov, če želimo ohranjati potrebno varnost.

## LITERATURA


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

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

[3] T. Dogša (1993): *Verifikacija in validacija programske opreme*, Tehniška fakulteta Maribor

[4] Vinnie Moscaritolo (1999): *http//www.vmeng.com/vinnie/crypto.html*

[5] N. F. Johnson, S. Jajodia (1998): *Exploring Steganography: Seeing the Unseen*, IEEE Computer, februar 1998, str.26-34

[6] Paul C. Kocher (1998): *Breaking DES*, RSA Laboratories' CryptoBytes vol. 4, Number 2, Winter 1998

[7] Terry Ritter (2001): *Research Comments from Ciphers By Ritter: http://www.ciphersbyritter.com/*

[8] RSA Laboratories (1998): *Frequently asked Question About Todays Cryptography* v4.0

[9] RSA Laboratories (1995): Technical Report TR-701: *Stream Ciphers*, July 1995


◆


*Matej Šalamon je diplomiral leta 1994 in magistriral leta 1999 na Fakulteti za elektrotehniko, računalništvo in informatiko v Mariboru, kjer je tudi zaposlen kot asistent za področje elektronike. 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 predvsem s preverjanjem programske opreme.*