SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

Seminarski rad

Simetrični algoritmi kriptiranja

KOLEGIJ: ***Sustavi za praćenje i vođenje procesa***

AUTOR: ***Neven Parat***
0036368647

ZAGREB, svibanj 2005.

Sadržaj :

1. Uvod

Sigurnost računalnih sustava postaje sve važnija, jer sve više korisnika na sve više načina koristi sve više informacija u računalnom svijetu. U takvom sustavu postoji i sve veća opasnost od neovlaštene uporabe informacija, podmetanja krivih informacija ili uništavanja informacija. U računalnim sustavima informacije se prenose raznovrsnim otvorenim i nesigurnim komunikacijskim putevima. Pristup do tih puteva ne može se fizički zaštititi pa svaki neprijateljski nastrojen napadač može narušiti sigurnost sustava. Zbog toga zaštitni komunikacijski mehanizmi nad nesigurnim komunikacijskim kanalom postaju najvažniji oblik ostvarenja sigurnosti. Pokazuje se da je najdjelotvornija zaštita poruka njihovo kriptiranje.

Kako današnji računalni sustavi teže što većoj otvorenosti, tako se uvode standardi u svim područjima korištenja računala. Prema tome, samo je bilo pitanje vremena kada će doći do standarda u kriptiranju, što se ostvarilo 1976. godine pojavom DES-a (engl. *Data Encryption Standard*). S vremenom je DES prestao udovoljavati teškim kriterijima pa je i zamijenjen 1998. godine novim standardom, AES-om (engl. *Advanced Encryption Standard*) za koji se vjeruje da je dovoljno siguran.

2. Osnovni termini

Kriptografija je znanost "tajnog pisanja", tj. znanost pohrane informacija u onoj formi koja će biti čitljiva samo onima kojima je informacija namijenjena dok će za ostale biti neupotrebljiva. Usporedo sa razvojem kriptografije razvila se i znanost kojoj je cilj analizom kriptirane poruke odgonetnuti njen sadržaj. Ta znanost se naziva **kriptoanaliza**.

Pored gore navedenog, valja spomenuti jednu bitnu razliku između termina **kriptografija** i termina **kriptologija**. *Kriptografija* je znanost koja se bavi svim aspektima sigurnosnog transporta podataka kao što su na primjer autentifikacija (web, lokalne mreže i sl.), digitalni potpisi, razmjena elektroničkog novca. *Kriptologija*, je za razliku grana matematike koja se bavi matematičkim načelima, te matematičkom implementacijom kriptografskih metoda.

Originalna poruka koju je *pošiljaoc će slati* u daljnjem razmatranju će se zvati **čisti tekst** ili **original**. Zatim, *kodiranje* poruke tj. postupak pretvaranja originala (čistog teksta) u nečitljiv oblik ćemo nazvati **enkripcija**. Tako enkriptiran tekst ima engleski termin *ciphertext*, a mi ćemo je jednostavno nazvati **kodiranom porukom**. Nadalje, postupak *dekodiranja* poruke, tj. vraćanja poruke iz njenog enkriptiranog oblika u originalni (*čisti tekst*) oblik naziva se **dekripcija**.

Vrlo važan termin u kriptografiji je **ključ**. Ključ ima veliku ulogu u enkripciji i dekripciji poruke i detaljnije će biti objašnjen kasnije.

3. Osnovni kriptografski algoritmi

Nekada, prije nego što su računala ušla u široku uporabu, tj. prije nego su se dovoljno razvila, većina kriptografskih metoda šifriranja se bazirala na tajnosti **šifre**. No, tako bazirani algortimi su se pokazali dosta nepouzdani, te su se morale pronaći neke druge metode šifriranja. Današnje metode šifriranja zasnivaju se na uporabi **ključa**. Ključ je najvažniji dio u pravilnom enkriptiranju i dekriptiranju poruka.
Upravo ovisno o načinu korištenja ključa, razvile su se dvije klase algoritama. Jedna je **simetrična**, a druga **asimetrična** klasa. Drugim riječima, postoje simetrični algoritmi kriptiranja i asimetrični algoritmi kriptiranja. Osnovna razlika je u tome da simetrični algoritmi koriste isti ključ za enkripciju i dekripciju neke poruke (ili se ključ za dekripciju može lako proizvesti iz originalnog ključa za enkripciju), dok asimetrični algoritmi koriste različite ključeve za enkripciju i dekripciju iste. Svaki od načina kriptiranja će se nešto detaljnije objasniti.

- **Simetrični algoritmi:**

  Ove algoritme dijelimo u dvije grupe: **stream šifriranje** i **blok šifriranje** Stream šifriranje radi tako da se enkripcija poruke (originala) vrši bit po bit, dok se kod blok šifriranja enkripcija vrši po blokovima podataka, tj. uzimaju se blokovi od više bitova (64, 128, 196, 256 ...), te se enkriptiraju kao cjelina. Dekripcija se najčešće vrši *inverznim enkriptiranjem*, tj. algoritam je isti, ali se podključevi enkripcije koriste obrnutim redoslijedom.

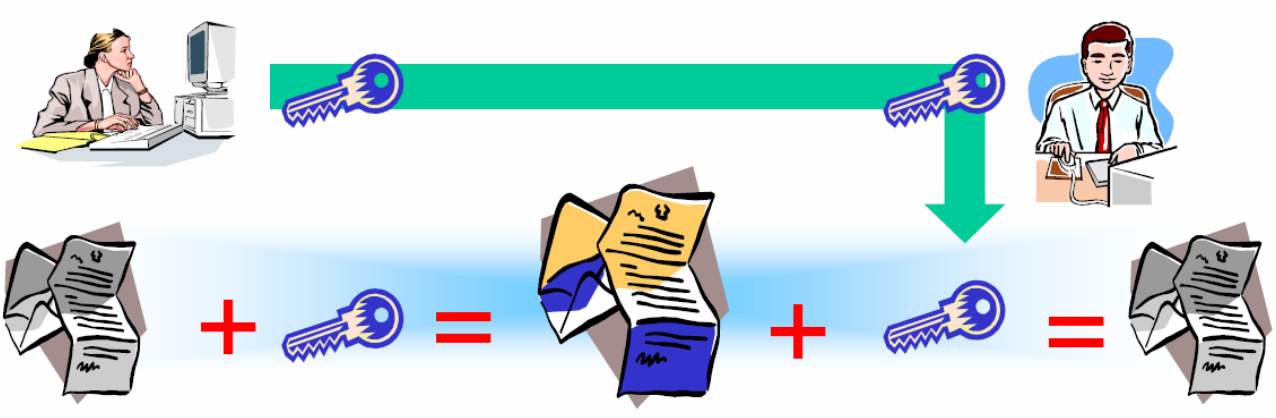
- **Asimetrični algoritmi:**

  Ove algoritme nazivamo još i **public-key algorithms,** tj. algoritmi s **javnim ključem**. Razlog ovakvom nazivu je taj što je dozvoljeno da se *jedan od ključeva* potreban za enkripciju/dekripciju objavi javno (npr. Internet, novine). Ovdje treba obratiti pažnju na riječi *"jedan od ključeva".* Ono što je specifično za ovaj tip algoritma je to da se koriste **dva** ključa za enkripciju/dekripciju poruke (originala). Ideja je sljedeća: osoba **A** objavi svoj **javni ključ** preko nekog medija (npr. Internet). Osoba **B**, koja osobi **A** želi poslati tajnu poruku enkriptira tu svoju poruku s ključem koju je osoba **A** javno objavila te joj takvu poruku pošalje (recimo preko e-mail servisa). Jedino osoba **A** sa svojim **privatnim (tajnim)** ključem može dekriptirati poruku poslanu od osobe **B** i nitko drugi.

Uglavnom, simetrični algoritmi su po svojoj prirodi brži, tj. implementacija na računalu se brže odvija od implementacije asimetričnih algoritama. No, zbog nekih prednosti asimetričnih algoritama u praksi se obje vrste algoritama isprepleću u cilju bolje zaštite poruka. Obično se asimetrični algoritmi koriste za enkripciju *slučajno generiranog broja* koji služi kao ključ za enkripciju originalne poruke metodama simetričnih algoritama. Ovo se naziva **hibridna enkripcija**.

4. Simetrična kriptografija

- Za šifriranje i dešifriranje koristi se isti ključ – tajni ključ
- Dužina ključa naznačuje koliko će trebati da se napadom razbije šifra
- Mora se osigurati razmjena ključa preko nesigurnog komunikacijskog kanala
- Dobre strane: brzina šifriranja velikih količina podataka
- Mane:
    - s porastom broja korisnika raste broj ključeva, npr. 5 korisnika – 10 ključeva,
    - N korisnika – N * (N-1) /2 ključeva,
    - ne mogu se koristiti za digitalno potpisivanje.



5. Simetrični algoritmi

5.1. Popis simetričnih algoritama

DES prethodnici i sljdbenici:

Lucifer
DES
DESX
3-DES
Blowfish
DEAL
FEAL
ICE
IDEA
Khufu
MacGuffin
NewDES
RC2
RC5
Akelarre
SHARK

AES kandidati:

AES (Rijndael)
FROG
LOKI97-sim LOKI91 -sim
MARS
RC6
Magenta
Serpent
Twofish

Jednostavni:

3-Way
ENIGMA
Solitaire
TEA

Kriptiranje toka podataka:

A-5
Helix
Pike, Pike
RC4
SEAL
SOBER
WAKE

Višenamjenski:

Panama
Sapphire

Ostali:
CAST
CMEA
E2
GOST
Hasty Pudding
Misty
SAFER++
SEA
Skipjack
Square
Turtle
ARC4
BBC
CRAB
Crypt
Crypton
Damond2
DFC
Khafre
LOKI89, 91
MDC
MMB
MPJ
NSEA
ORYX
Q128
Quadibloc*
Rainbow
REDOC
S1
Scop
Yarro

5.2. Podaci o važnijim simetričnim algoritmima

Lucifer

Lucifer je prvi simetrični algoritam za kriptiranje kojeg je osmislio Horst Fiestel, razvijen od strane IBM – a u ranim sedamdesetima. Prethodnik je DES – a i mnogo je jednostavniji od njega.

Činjenice:

- prvi simetrični algoritam s blok šifriranjem
- prethodnik DES-a
- enkriptira blok veličine 128 bita
- koristi ključ veličine 128 bita
- 16 podključeva dužine 72 bita
- koristi 16 'Feistel runda' (iteracije) kod enkriptiranja
- dekripcija se vrši inverznom enkripcijom

Slabosti:

- slabosti u korištenju ključa (key scheduling)
- slab je na napade diferencijalne kriptoanalize

Danas se smatra nesigurnim, no zbog dužine ključa, te brzine enkriptiranja može se koristiti za enkriptiranje u kombinaciji s nekim dobrim simetričnim algoritmom kao što je DES.

DES

- Donedavno standardni algoritam za enkripciju.

Činjenice:

- nastao od LUCIFER-a, (NBS,IBM,NSA)
- enkriptira blok veličine 64 bita
- koristi ključ dužine 64 bita (56 efektivno)
- broj rundi varijabilan (ovisi o dužini ključa i dužini bloka)
- koristi 16 podključa dužine 48 bita
- koriste se Feistel runde

Najčešće korišten simetrični algoritam.
Polako će ga zamijeniti puno sigurniji i napredniji algoritam Rijndael koji je nazvan AES (Advanced Encryption Standard).

Zanimljivost vezana uz DES: pokazano je da kad bi umjesto 16 podključeva deriviranih iz početnog 64-bitnog ključa K koristili 16 različito zadanih ključeva, ne bi dobili puno na sigurnosti. U biti rezultat bi bio jednak korištenju regularnog DES kriptiranja sa 65-bitnim ključem K.

Druga zanimljivost vezana uz DES je na žalost i njegova slabost. Naime, zbog načina na koji DES kreira podključeve, postoje 4 ključa za koje je dekripcija jednaka enkricpiji. To znači da ako s tim ključem želimo enkriptirati poruku dvaput, dobili bi smo kao rezultat originalnu poruku. No, vjerovatnost enkriptiranja baš tim ključevima je jako mala pa ne utječe značajno na sigurnost.

Probijanje DES-a

DES je nastao početkom 70-ih godina, a odobren je 1977. Može se reći da je kao enkripcijski standard zadovoljio ciljeve (sigurnost) i predviđen vijek trajanja (20-25 godina), no krajem 90-ih (1997), RSA Laboratories obznanjuje **RSA Secret Key Challenge**. Cilj izazova bio je probijanje nekih od najkorištenijih algoritama enkripcije u to doba. Također, pored samog dokaza o ranjivosti današnjih algoritama (DES, RC5), očekivala su se i neka dodatna saznanja koja bi se stekla kroz izazov.
Izazov se u početku sastojao od 13 zadataka. Dvanaest od njih su se sastojala od probijanja RC5 algoritma i to različitih duljina ključeva (od 40-128 bitova), dok je jedan zadatak bio probijanje DES-a. Niže je kronološki slijed probijanja algoritama:

- siječanj, 1997. - RSA izdaje **RSA Secret Key Challenge** ($10,000)
- listopad, 1997. - razbijen 56-bitni **RC5**
    - nakon 250 dana *brutte-force (exhaustive key search)* napada sa 10,000 računala. Projekt se zvao **Bovine RC5 Effort**, grupa koja je vodila projekt zvala se *Distributed.net group*, a korištena metoda povezivanja računala zove se distribuirano mrežno računarstvo. Dosta važan podatak vezan za ovaj način obrade podataka je to da je korišteno samo *idle* vrijeme procesora, tj. koristilo se ono vrijeme dok je procesor bio nezaposlen. Kada bi se posvetilo potpuno vrijeme svih korištenih

računala samo ovm zadatku, vrijeme probijanja ključa bilo bi puno kraće.

- 1997. - razbijen 56-bitni **DES**
  - za razbijanje *brutte-force* metodom, bilo je potrebno **96 dana**. Grupa se zvala **Deschall** i korišteno također je distribuirano mrežno računarstvo s 15,000-20,000 računala.
- siječanj, 1998. - RSA izdaje **DES challenge II** izazov
  - cilj RSA je bio da dvaput na godinu izda novi izazov za razbijanje DES-a. Po njihovim procjenama, svakom novom uspjelom pokušaju trebalo bi znatno manje vremena za razbijanje.
- veljača, 1998. - razbijen 56-bitni **DES**
  - grupa *Distributed.net* u puno kraćem roku probija DES (**41 dan**). I ovaj put se koristilo *distribuirano mrežno računarstvo* uz ukupno 50,000 procesora. Projekt je nazvan **Monarch** i pretraženo je ukupno 85% 56-bitnog prostora ključa.
- srpanj, 1998. - razbijen 56-bitni **DES**
  - drugi u nizu izazova te godine (**DES challenge II-2**) je dobijen od Electronic Frontier Foundation (EFF) organizacije. EFF je kreirala posebno projektirano računalo nazvano **DES Cracker** koje je koštalo $220,000 i koje je probilo DES za **56 sati**. Brzina pretraživanja ovog *custom-made* računala bila je 90 biliona ključeva/sekundi.
- siječanj, 1999. - razbijen 56-bitni **DES**
  - na izazov **DES challenge III** odazvali su se opet EFF i Distributed.net grupa, samo ovaj put su ujednili snage. **DES Cracker**, sada uz pomoć distribuiranog mrežnog računarstva koje je objedinjavalo 100,000 PC računala na Internetu, probilo je poruku kodiranu 56-bitnim DES ključem za **22 sata i 15 minuta**. To je bio ujedno i novi rekord u probijanju DES šifre. Brzina pretraživanja DES prostora je bila 245 biliona ključeva/sekundi.

Važno je napomenuti da osim brutte-force napada, postoje još neke slabosti u DES-u za koje se sumnja da su namjerno uvedene.

- kompletna specifikacija S-kutija je ostala tajna (način izvedbe) od strane NIST-a (bivšeg NBS-a)
- iako se S-kutije DES-a smatraju za jako dobre (pogotovo s obzirom da su konstruirane sredinom '70-ih godina), one nisu optimizirane protiv linearne kriptoanalize - sumnja se na backdoor za NSA.

Triple DES i 2-Key 3DES

- "Triple data" enkripcijski standard koji pojačava standardnu DES enkripciju.

To je DES bazirani algoritam, ali koristi 2 ili 3 različita DES ključa. Prvi ključ se koristi za enkriptiranje bloka podataka izvorne poruke. Tako enkriptirana poruka se dekriptira drugim ključem. Normalno je da se dekripcijom sa ovim ključem neće dobiti originalna poruka, već nova šifrirana poruka. Na kraju se razultat dekripcije opet enkriptira, ovaj put ili trećim ključem ili opet prvim. Time se povećao broj kombinacija koje bi eventualni napadač morao probati da bi pronašao ključ. Broj kombinacija se penje (za 2 različita ključa) na 2112, dok za 3 različita ključa čak na 2168 kombinacija.

3-DES (kako ga još nazivaju) rješava problem dužine ključa običnog DES-a, no sa sobom unosi novi problem. Puno je sporiji od običnog DES-a (barem dvaput). To je i jedan od razloga zašto je raspisan natječaj za AES.

Preporučen od RSA Security-a.

IDEA

- blok šifriranje

Činjenice:

- enkriptira blok veličine 64 bita
- koristi ključ dužine 128 bita
- 52 podključeva dužine 16 bita
- koristi jedan par podključeva po rundi *
- koristi 8 cross-footed runda (iteracije) kod enkriptiranja
- nema S-kutija, niti drugih lookup tabela
- dekripcija se vrši inverznom enkripcijom

Prednosti:

- do sada je izdržao 'napadima' akademske zajednice **

* IDEA koristi 52 podključa svaki dužine 16 bitova te, ima 8 rundi (8.5) enkripcija poruke. Po dva podključa se koriste u svakoj rundi (16), zatim, četiri podključa se koriste prije svake runde (32), te se zadnja četiri podključa koriste nakon zadnje runde (4) -> 16+32+4=52.
Podključevi se dobiju tako da se 128 bitni ključ razdijeli u prvih 8 podključeva (K1-K8) svaki veličine 16 bita. Zatim se sljedećih 8 podključeva dobije tako da se 25 puta napravi kružni lijevi pomak svakog od prethodno napravljenih podključeva. Postupak se radi dok se ne kreiraju svi podključevi.

** Iako je generiranje ključeva pravilno, što bi ukazalo na slabost algoritma, do sada je ovaj algoritam izdržao sva nastojanja akademskih ustanova u njegovom razbijanju.

Do sada najbolji napadi na algoritam su uspjeli probiti 4.5 runde od ukupnih 8.5 (napad nemoguća diferencijalna ideja - impossible differential idea od Biham-a, Shamir-a i Biryukov-a).

Što se tiče same poruke, blok dužine od 64 bita se razdijeli na četiri dijela od po 16 bita. Sada se koriste tri operacije nad 16 bitnim dijelovima (16-bitni ključ i 16-bitna poruka): zbrajanje, XOR operacija, te množenje.

Ovo je jedan od najpoznatijih simetričnih blok algoritama.

Također, smatra se jako sigurnim. IDEA je najpoznatija u primjeni kod PGP-a.

Internacionalni enkripcijski algoritam razvijen u Švicarskoj od strane ETH-a. Autor: Xuejia Lai te Prof. J. Massey početkom 90'-tih.

Slobodan za nekomercijalnu uporabu. Patentiran u USA i nekim Europskim državama. Vlasnik patenta je firma Ascom Systec no licencu izdaje iT_Security Ltd

Blowfish

- Simetrično blok šifriranje

Činjenice:

- enkriptira blok veličine 64 bita
- koristi ključ varijabilne dužine (od 32-448 bita)
- 18 podključeva dužine 72 bita
- koristi 16 'Feistel runda' (iteracije) kod enkriptiranja
- 4 S-kutije, sa 256 32-bitne vrijednosti
- dekripcija se vrši inverznom enkripcijom

Prednosti:

- korištenje ključa (key scheduling)

Blowfish je poznat po svojoj organizaciji ključeva, tj. key-schedulingu. Sve svoje podključeve, te sadržaje S-kutija ovaj algoritam kreira tako da višestruko iterira zadanu blok šifru (ključ). Ovo ga čini, čak i za male ključeve, jako otpornim na brutte-force napade, jer se sa svakom iteracijom (novim podključem) povećava broj kombinacija (svih ključeva zajedno).

Može se koristiti kao zamjena za DES ili IDEA.

Razvijen od Bruce Schneier-a.

Slobodan za uporabu. Nije patentiran.

AES

AES (Advanced Encryption Standard) je novi algoritam enkripcije koji će zamjeniti DES kao standardni algoritam enkripcije u svijetu.

Zašto AES?

Razlog je jednostavan. Naglim razvojem informacijske tehnologije algoritmi koji su nastali prije deset, dvadeset i više godina su zastarjeli u smislu da više ne pružaju dovoljnu sigurnost. Naime, zadnjih dvadeset godina kriptoanaliza (kao i kriptografija) je također profitirala od razvoja računarske moći. Algoritmi kao DES za koje se nekad smatralo da su neprobojni, danas je moguće kompromitirati.

Tijek natječaja za AES

Kako je DES prestao udovoljavati sigurnosnim zahtjevima bilo je nužno uvesti novi standard. Početnu ideju za rad na novom kriptografskom standardu nazvanom **AES** (engl. ***Advanced Encryption Standard***) NIST (engl. *The National Institute of Standards and Technology*) objavljuje 2. siječnja 1997. godine, da bi 12. rujna iste godine i službeno otvorio javni natječaj. 3DES (engl. *Triple DES*) je označen kao privremeni standard do kraja natječaja. Na natječaj se mogu prijaviti samo algoritmi sa sljedećim svojstvima:

- simetrični blokovski algoritmi sa javnim kodom,
- podržavanje veličine bloka od minimalno 128 bita i
- podržavanje veličine ključa od 128, 192 i 256 bita.

Na prvoj AES konferenciji (nazvanoj *AES1*) 20. kolovoza 1998. NIST objavljuje prihvaćanje u natječaj 15 kandidata: CAST-256, CRYPTON, DEAL, DFC, E2, FROG, HPC, LOKI97, MAGENTA, MARS, RC6™, Rijndael, SAFER+, Serpent te Twofish.
Na istoj konferenciji NIST traži javne komentare na pristigle algoritme i u tu svrhu otvara i službene stranice te forum gdje ljudi iz cijeloga svijeta mogu vidjeti kodove algoritama i sudjelovati u javnim raspravama i analizama algoritama.
Svi pristigli komentari su diskutirani i analizirani na drugoj konferenciji (*AES2*) održanoj u ožujku 1999. Na temelju komentara, kritika i analiza 20. kolovoza 1999. odabrano je pet finalista: **MARS**, **RC6™**, **Rijndael**, **Serpent** te **Twofish**.
Na trećoj AES konferenciji (*AES3*) održanoj u travnju 2000. nastavlja se sa javnom analizom finalista sve do 15. ožujka 2000. godine, kada se za novi standard odabire **Rijndael**.

Rijndael

Rijndael je simetrični blok algoritam predložen za AES od strane Joan Daemen-a i Vincent Rijmen-a iz Belgije. Krajem 2000. godine je i izabran za novi AES.

Osnovne karakteristike su mu sljedeće:

- Veličina bloka enkripcije je varijabilna i može biti 128, 192 ili 256 bita.

- Dužina ključa mu je također varijabilna i može biti 128, 192 i 256 bita (pa i više ili manje, samo da je dužina djeljiva sa 4 - u tom slučaju mijenja se i broj rundi).

- Broj rundi je varijabilan. Naime, broj rundi ovisi o dužini ključa i veličini bloka (oboje vraijabilno). Zato, ne brojeći zadnju ekstra rundu, imamo:

    - 9 rundi ako su i blok i ključ 128 bita dužine,
    - 11 rundi ako je bilo blok, bilo ključ 192 bita dužine,
    - 13 rundi ako je bilo blok, bilo ključ 256 bita dužine.

Već iz ovih karakteristika može se naslutiti da je algoritam otporniji na brutte-force napad od DES-a (veća dužina ključa).

CAST-256

- Blok šifriranje

Činjenice:

- enkriptira blok veličine 128 bita
- koristi ključ varijabilne veličine (do 256) bita
- 18 podključeva dužine 72 bita
- koristi jedan par podključeva po rundi
- koristi 48 runda (iteracije) kod enkriptiranja
- 4 S-kutije, sa 256 32-bitne vrijednosti
- dekripcija se vrši inverznom enkripcijom

Prednosti:

- otporan na diferencijalnu linearnu kriptoanalizu
- otporan na analize ključa (related-key)
- korištenje ključa (key scheduling)
- posjeduje općenito dobre kriptografske osobine

Koristi F-funkciju koja ima 32-bitni ulaz, te 32-bitni izlaz (za razliku od DES-a koji koristi za ulaz jedan 32-bitni i 48 bitni podatak). Runde (iteracije) su organizirane u četvorke (quadrons) kojih je ukupno 12 (48 rundi).

Što se tiče samog naziva, moguće je u literaturi naići na termin CAST6. Kao i kod CAST-128 (CAST5) algoritma, termin CAST6 se koristi u kombinaciji sa dužinom ključa CAST-256 algoritma. Ako je dužina ključa 192 bita, tada se koristi termin CAST6-192. Termin CAST-256 se koristi samo kada je dužina korištenog ključa 256 bita.

Bivši AES kandidat.

Razvijen od Carlisle Adams-a & Stafford Tavares-a.

6. Zaključak

U odabiru za AES sudjelovali su kandidati sa gotovo jednakim predispozicijama za pobjedu. To sugerira da nam u slučaju zakazivanja jednog kandidata uvijek ostaje dovoljan broj jednako dobrih zamjena. Sudeći po dosadašnjim zbivanjima, vrlo brzo slijedit će lavina pokušaja probijanja Rijndaela, no čini se da ovaj put to ipak neće biti tako lako. Pri konstrukciji DES-a nije se raspolagalo današnjim znanjima (a i namjerno je malo oslabljen) pa je s vremenom prestao udovoljavati zahtjevima. Što se tiče duljine ključa, sada konačno više nema potrebe za strahom, a isto vrijedi i za sve dosada poznate napade. No, nitko ne zna što budućnost donosi, a da i u budućnosti stoji na raspolaganju dovoljno pouzdan algoritam, potrebno je učestalo razrađivanje poznatih algoritama, spajanje metoda iz poznatih algoritama ili smišljanje potpuno novih.

Iako je kod DES-a bio javno objavljen još 1976. godine, učinkovitiji napadi pojavljuju se tek početkom devedesetih. Ti napadi nisu došli s ubrzanim razvojem tehnologije ,već su matematičke i statističke prirode, što znači da su bili izvedivi od samog početka. Unatoč tome sustav je korišten kao standard kroz dugi niz godina, a da nitko (ili ipak – velika većina) nije znao za njegove slabosti. Takav razvoj događaja ipak stvara određenu dozu straha i kod novog kriptografskog sustava.

Općenito je vrlo teško dati objektivnu i realnu ocjenu kvalitete nekog algoritma. Ta je činjenica uvelike otežala natječaj za AES gdje je postavljen zadatak da se međusobno usporede konkretni algoritmi, te da se na koncu uzme jedan od njih i da se pred cijelim svijetom ustvrdi da je baš on najbolji. Ali najbolji ne postoji. Postoje samo bolje ili lošije osobine pojedinog algoritma u nekim konkretnim okolnostima.

Brzina je samo jedna od mnogih osobina pojedinog algoritma. Ipak, brzina algoritma se ističe među ostalim osobinama po tome što ima konkretnu vrijednost pa je pogodna pri usporedbi algoritama. Sudeći po mjerenjima može se zaključiti da su svi finalisti zadovoljavajuće brzi. Iako su se pokazali daleko najbržima RC6 i MARS, niti jedan od njih nije postao standardom. Od pet finalista po brzini je Rijndael tek četvrti, no to ga nije spriječilo da pobijedi na natječaju.

Čini se da su ključne ipak bile neke druge Rijndaelove osobine: odlične performanse na različitim platformama, dobra sigurnosna razina, pogodnost za pametne kartice, brzo generiranje ključeva, dobra podrška paralelnom izvođenju...

7. Terminologija

Feistel runde — Iteracije u kojima se blok ulaznog podatka dijeli na dva dijela. Jedan dio se mijenja u funkciji runde (koja za DES ima 4 koraka), a drugi dio ostaje nepromijenjen. Za DES jedna Feistel runda izgleda ovako.:

ekspanzija polovice bloka,
XOR bloka sa podključem,
zamijena bitova sa podacima iz S-kutija,
permutacija P izlaza S-kutija.

Nakon toga, podblokovi podataka zamjenjuju strane, tako da se kroz 16 rundi (za DES) svaki podblok mijenja jednak broj puta (8). Ono što Feistel funkcije čini posebno dobrim za kriptiranje (simetrični algoritmi) je to da sama funkcija runde ne mora biti invertibilna, no finalna funkcija bloka je uvijek invertibilna. Zato se dekripcija vrši brzo i jednostavno, te s istim ključem kao i enkripcija.

Key-scheduling — Organiziranje ključeva. Postupak pripreme ključeva za daljnji postupak enkripcije. Kod algoritama koji koriste princip Feistel rundi, to je postupak ekspanzije ključa na rk bita, gdje je r broj rundi, a k broj bita ključa enkripcije.

S-boxes, S-tablice, kutije — Tablice kojima se polja adresiraju sa n bita. Svako polje sadrži vrijednost od m bita, pa je to praktički tablica pretvorbe n bitne informacije u m bitnu. S stoji za substitucijske.

S-tablice su važna karika kod mnogih simetričnih algoritama (npr. DES, Serpent ...). Jako je važno da one budu otporne na kriptoanalizu. Postoji više načina izrade S-tablica. Jedan način je korištenje matematičkih funkcija za koje je moguće dokazati otpornost na određene napade. S druge strane, neki algoritmi koriste S-tablice kreirane korištenjem heuristike. Za te se tablice ne može eksplicitno matematički dokazati da su sigurne, no one imaju neke dodatne prednosti koje matematički kreirane S-tablice nemaju.

S-tablice su u nekim algoritmima jedini izvor nelinearnosti, pa otpornost algoritma uvelike pada na njih. DES spada u takve algoritme. Njegove tablice se smatraju tako dobre da su ih neki algoritmi implementirali u svoj kod (Serpent-0). To možda i nije najbolja ideja, jer je DES-ove S-tablice kreirala NSA koja nikada nije izdala njihove potpune specifikacije (sumnja se da u DES-ovim tablicama postoji neki backdoor za NSA).

NBS	*National Bureau of Standards*	Nacionalni biro za standarde (američki); kasnije preimenovan u NIST
NIST	*The National Institute of Standards and Technologies*	Nacionalni institut standarda i tehnologija (američki)
NSA	*National Security Agency*	Agencija za nacionalnu sigurnost (američka)

8. Literatura

1. Internet stranice Zavoda za telekomunikacije Fakulteta elektrotehnike i računarstva: www.tel.fer.hr

2. Internet stranice o računalnoj sigurnosti Zavoda za elektroniku, mikroelektroniku, računalne i inteligentne sustave Fakulteta elektrotehnike i računarstva: http://sigurnost.zemris.fer.hr

3. AES home page: http://www.nist.gov/aes

4. Internet stranice Fakulteta Organizacije i Informatike: http://www.student.foi.hr/nastava/OS/

5. http://mapmf.pmfst.hr/~marpla/

6. http://pingvin.carnet.hr/web_dokumentacija/posluzitelji/index.htm