TEHNIČKA ŠKOLA MLADENOVAC

Vuka Karadžića 75, 11400 Mladenovac, тел.011/8231-985, [tsm@gmail.com](mailto:tsm@gmail.com)

**SIMETRIČNO ŠIFROVANJE I DEŠIFROVANJE**

**rofesor:** **Učenik:**

**Srđan Maričić Stefan Todorović IV6**

**Uvod**

Kod simetrične enkripcije koriste se isti ključ i za šifrovanje i za dešifrovanje. Baš zbog toga je raznovrsnost, a samim tim i sigurnost algoritama ovakve enkripcije je velika. Bitan faktor je i brzina - simetrična enkripcija je veoma brza. Pored svih prednosti koje ima na polju sigurnosti i brzine algoritma, postoji i jedan veliki nedostatak. Kako preneti tajni ključ? Problem je u tome, što ako se tajni ključ presretne, poruka se može pročitati. Zato se ovaj tip enkripcije najčešće koristi prilikom zaštite podataka koje ne delimo sa drugima (šifru znate samo vi i nju nije potrebno slati drugome).

Klod Šenon (Claude Shannon) je definisao uslove savršene tajnosti, polazeći od sledećih osnovnih pretpostavki:

* Tajni ključ se koristi samo jednom.
* Kriptoanalitičar ima pristup samo kriptogramu.

Šifarski sistem ispunjava uslove savršene tajnosti ako je otvoreni tekst X statistički nezavisan od kriptograma Y, što se može matematički izraziti na sledeći način:

**P(X = x|Y = y) = P(X = x)**

za sve moguće otvorene tekstove **x=(x1,x2…..xm)** {\displaystyle x=(x\_{1},x\_{2},...x\_{m})} i sve moguće kriptograme **y=(y1,y2…..yn)** {\displaystyle x=(x\_{1},x\_{2},...x\_{m})}  {\displaystyle y=(y\_{1},y\_{2},...y\_{n})}; drugim rečima, verovatnoća da slučajna promenljiva X ima vrednost x jednaka je sa ili bez poznavanja vrednosti slučajne promenljive Y. Zbog toga kriptoanalitičar ne može bolje proceniti vrednost X poznavajući vrednost Y od procene bez njenog poznavanja, nezavisno od raspoloživog vremena i računarskih resursa kojima raspolaže. Koristeći pojam entropije iz teorije informacija Šenon je odredio minimalnu veličinu ključa potrebnu da bi bili ispunjeni uslovi savršene tajnosti. dužina ključa K mora biti najmanje jednaka dužini otvorenog teksta M:

**K ≥ M**

**Vrste algoritama simetričnih ključeva**

Postoje dve vrste algoritama simetričnih ključeva: šifre toka i blok šifre. Šifre toka šifruju poruku kao tok bitova jedan po jedan. Blok šifre uzimaju blokove bita, šifruju ih kao jednu celinu. Blokovi od 64 bita se često koriste, iako moderno šifrovanje poput AES-a (Advanced Encryption Standard) koristi blokove od 128 bita.Neki od poznatih simetričnih algoritma su:

* DES (Data Encryption Standard) – ključ je dužine 56 bita.
* Triple DES, DESX, GDES, RDES – ključ je dužine 168 bita.
* (Rivest) RC2, RC4, RC5, RC6 – promenljiva dužina ključa do 2048 bita.
* IDEA – osnovni algoritam za PGP – ključ je dužine 128 bita.
* Blowfish – promenljiva dužina ključa do 448 bita.
* AES (Advanced Encryption Standard) - radi sa blokovima od po 128 bita i koristi ključeve dužine 128, 192 i 256 bita.

**DES**

**Data Encryption Standard** (DES) – DES algoritam je najviše korišćen algoritam za kriptovanje na svetu. Dugo godina, DES je među ljudima bio sinonim za sigurno šifrovanje. Razvijan je od strane brojnih organizacija za kriptovanje poruka i podataka pa je postao najrasprostranjeniji komercijalni algoritam. DES je blok šifra što znači da algoritam kriptuje podatke u 64-bitna bloka i koristi 64-bitni ključ. U realnosti, samo 56 bitova se koristi za kriptovanje/dekriptovanje podataka gde preostalih 8 bitova rade kao analogni. Upotreba 56 bita omogućava veliki prostor za ključ. Potencijalne mogućnosti za ključ čine razbijanje ovog koda teškim kada su u pitanju brutalni napadi

**Triple DES i 2-Key 3DES**

**Triple DES** algoritam - U poslednjih nekoliko godina zabeležen je veliki broj probijanja DES algoritma razbijanjem ključa za kriptovanje. Vlada Sjedinjenih Američkih Država ne priznaje više DES kao standard pa su mnoge organizacije prešle na trostruki DES algoritam. Trostruki DES koristi tri ključa za kriptovanje podataka što povećava veličinu ključa na 168 bita. Postoji više metoda trostrukog DES algoritma:

1. Prvi metod: podaci se kriptuju tri puta sa tri odvojena ključa.
2. Drugi metod: podaci se kriptuju prvim ključem, dekriptuju drugim i ponovo se kriptuje trećim ključem.
3. Treći metod: sličan je sa prethodna dva, sa tim što se isti ključ  koristi u prvoj i trećoj operaciji.

**3-DES** rešava 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**

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 generisanje 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.

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

**AES**

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

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) je takođe profitirala od razvoja računarske moći. Algoritmi kao DES za koje se nekad smatralo da su neprobojni, danas je moguće kompromitirati.

Početnu ideju za rad na novom kriptografskom standardu nazvanom AES (engl. Advanced Encryption Standard) NIST (engl. The National Institute of Standards and Technology) objavljuje 1997. godine, da bi iste godine i službeno otvorio javni konkurs. 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) 1998. NIST objavljuje prihvaćanje u takmičenje 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 ucestvovati u javnim raspravama i analizama algoritama. Svi pristigli komentari su analizirani na drugoj konferenciji (AES2). Na temelju komentara, kritika i analiza. odabrano je pet finalista: MARS, RC6™, Rijndael, Serpent te Twofish. Na trećoj AES konferenciji (AES3) održanoj 2000. nastavlja se sa javnom analizom finalista sve do 15. marta 2000. godine, kada se za novi standard odabira Rijndael.

**Blowfish**

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 brutteforce 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 upotrebu.

**Generacija ključa**

Kasa se koristi sa asimetričnim šifrovanjem za transfer ključa, pseudonasumični generatori ključeva se skoro uvek koriste za generisanje simetričnih ključeva. Međutim, nedostatak nasumičnosti u tim generatorima ili u njihovim inicijalizacijskim vektorima je užasna i dovela je do kriptoanalitičkih pucanja u prošlosti. Zato je od suštinske važnosti da implementacija koristi izvor velike entropije za svoju inicijalizaciju