HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

IDEA algoritam

CCERT-PUBDOC-2003-06-25

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.lss.hr - laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

IDEA (International Data Encryption Algorithm) se u konačnom obliku pojavio 1992. godine. Algoritam se bazira na impresivnim teoretskim temeljima, i kao takav se pokazuje vrlo otpornim na sve vrste napada. Stručnjaci ga procjenjuju jednim od najsigurnijih simetričnih algoritama koji se danas koriste.

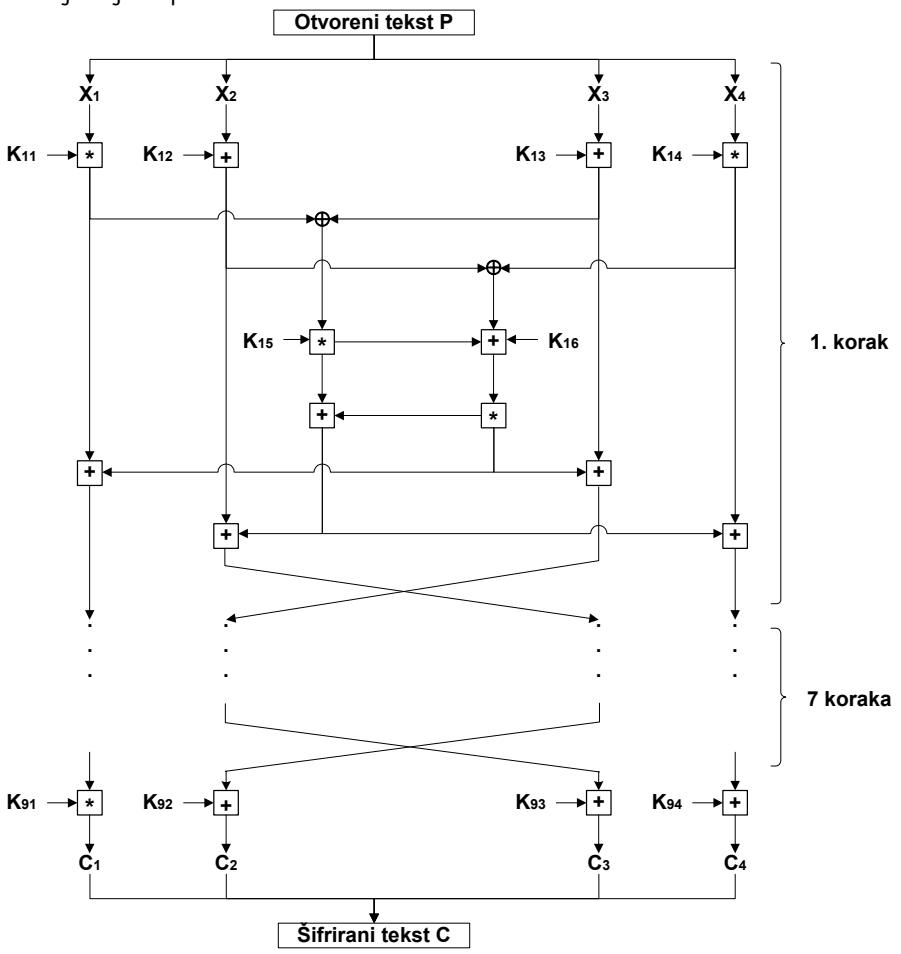
Još jedna od prednosti IDEA algoritma u odnosu na DES jest to da prilikom razvoja algoritma nije bilo miješanja nekih državnih institucija, tako da se ne sumnja u postojanje bilo kakvog *backdoora* (za razliku od DES-a, u čijem je razvoju određeni utjecaj imala i NSA).

U ovom trenutku u komercijalnoj primjeni DES još uvijek ima primat, djelomično i zato pošto je IDEA patentirana te je za komercijalnu upotrebu potrebna odgovarajuća licenca. Najpoznatija i najraširenija uporaba IDEA algoritma vezana je uz PGP, koji ga koristi kao simetrični algoritam.

2. Način rada

Slično kao i priličan broj drugih simetričnih algoritama (između ostalog i DES), IDEA šifrira otvoreni tekst u 64-bitnim blokovima. Ključ za šifriranje je duljine 128 bita, a šifriranje i dešifriranje se provodi na isti način. Osnova algoritma su tri algebarske operacije; XOR, zbrajanje modulo 2^{16}, te multiplikacija modulo $2^{16}+1$. Svaku od tih operacija jednostavno je implementirati sklopovski ili programski, što ubrzava sam postupak šifriranja/dešifriranja.

Slika 1 daje shematski prikaz algoritma. Algoritam se sastoji od 8 koraka koji su funkcijski identični. U svakom koraku kao ulaz se koriste četiri 16-bitna bloka koji su generirani u prethodnom koraku, dok su rezultat funkcije koja se provodi u svakom koraku također četiri 16-bitna izlazna bloka.



Slika 1: Shematski prikaz IDEA algoritma

Postupak šifriranja se provodi tako da se 64-bitni blok podataka dijeli u četiri 16-bitna podbloka: X_1, X_2, X_3, X_4. Ta četiri bloka predstavljaju ulazne parametre prvog od osam koraka algoritma. U svakom od koraka na podblokovima se izvodi XOR operacija, zatim modulo zbrajanje, te na kraju modulo multiplikacija međusobno i sa šest 16-bitnih podključeva. Između svakog od koraka algoritma drugi i treći podblok se zamjenjuju. Konačno, četiri podbloka se kombiniraju sa četiri podključa dajući tako konačnu transformaciju.
Algoritam izgleda ovako:

```
početak
  P = P1P2P3P4
  X1 = P1
  X2 = P2
  X3 = P3
  X4 = P4
  za i=1 do i=8 radi
        izračunaj R1 = X1 * Ki1
        izračunaj R2 = X2 + Ki2
        izračunaj R3 = X3 + Ki3
        izračunaj R4 = X4 * Ki4
        izračunaj R5 = R1 + R3
        izračunaj R6 = R2 ⊕ R4
        izračunaj R7 = R5 * Ki5
        izračunaj R8 = R6 + R7
        izračunaj R9 = R8 * Ki6
        izračunaj R10 = R7 + R9
        izračunaj Y1 = R1 ⊕ R9
        izračunaj Y2 = R3 ⊕ R9
        izračunaj Y3 = R2 ⊕ R10
        izračunaj Y4 = R4 ⊕ R10
        ako je i=8 onda
              X1 = Y1
              X2 = Y3
              X3 = Y2
              X4 = Y4
        inače
              X1 = Y1
              X2 = Y2
              X3 = Y3
              X4 = Y4
  kraj
  izračunaj C1 = X1 * S91
  izračunaj C2 = X2 + S92
  izračunaj C3 = X3 + S93
  izračunaj C4 = X4 * S94
  C = C1C2C3C4
kraj
```

2.1. Generiranje ključeva

Podključevi (ukupno 52 16-bitna ključa) koji se koriste u algoritmu generiraju se od 128-bitnog ključa na sljedeći način: ključ se dijeli na osam 16-bitnih ključeva koji se koriste kao podključevi za prvu iteraciju i prva dva ključa druge iteracije. Zatim se ključ rotira 25 bitova u lijevo, te se generira sljedećih osam ključeva koji se zatim koriste kao preostala četiri podključa druge iteracije i četiri podključa treće iteracije itd.

2.2. Dešifriranje

Algoritam za dešifriranje je potpuno identičan, osim što se podključevi generiraju na malo drugačiji način. Podključevi koji se koriste za dešifriranje primjenjuju se obrnutim redoslijedom, te su aditivno ili multiplikativno inverzni ključevima za šifriranje. Točan postupak generiranja podključeva za dešifriranje je sljedeći:

```
početak
  za i=1 do i=8 radi
        Kdi1 = K(10-i)1^-1
        Kdi1 = -K(10-i)2
        Kdi3 = -K(10-i)3
        Kdi4 = -K(10-i)4^-1
        Kdi5 = K(9-i)5
        Kdi6 = K(9-i)6
  kraj
  Kd91 = K11^-1
  Kd92 = -K12
  Kd93 = -K13
  Kd94 = -K14^-1
kraj
```

3. Inačice IDEA-e

IDEA može funkcionirati u svim načinima rada. Standardni način je šifriranje blokova (engl. *ECB - electronic codebook*), a također je moguće i ulančavanje blokova (engl. *CBC – cipher block chaining*). Isto tako IDEA može funkcionirati za šifriranje tokova podataka, npr. za CFB (engl. *cipher feedback*) način rada.
Slično kao i DES, u slučaju korištenja dvostrukog šifriranja, IDEA bi bila ranjiva na *man-in-the-middle* napade, no 128-bitni ključ osigurava dovoljnu razinu sigurnosti da bi pokušaj takvog napada bio nepraktičan. Ukoliko se želi postići još viša razina sigurnosti moguće je korištenje trostruke IDEA implementacije, kod koje se šifriranje provodi na sljedeći način:

$$C=E_{K3}(D_{K2}(E_{K1}(P)))$$

Dešifriranje je u tom slučaju točna inverzija postupka šifriranja:

$$P=D_{K3}(E_{K2}(D_{K1}(P)))$$

Na taj način postiže se efektivna duljina ključa od 384 bita.
Također, ukoliko se koriste odgovarajući alati za upravljanje ključevima, moguća je implementacija IDEA algoritma s nezavisnim podključevima. IDEA koristi 52 16-bitna ključa, što znači da bi ukupna duljina ključa bila 832 bita. Ova inačica IDEA-e je sigurnija, ali nije točno procijenjeno koliko je to unaprjeđenje sigurnosti.

4. Sigurnost

IDEA, iako prilično nov algoritam, pokazao se prilično sigurnim u odnosu na druge simetrične algoritme. Napad primjenom čiste sile (engl. *brute force attack*) u ovom trenutku i s trenutno dostupnom tehnologijom zbog 128-bitne duljine ključa nije moguć.
Primjenom kriptoanalize algoritma do sada nisu pronađene određene slabosti ili nedostaci, koji bi u značajnijoj mjeri utjecali na sigurnost i pouzdanost algoritma, no algoritam je prilično nov, tako da postoji mogućnost da će se u budućnosti pronaći metode diferencijalne ili linearne kriptoanalize koje bi mogle pojednostaviti napade na algoritam. U ovom trenutku to nije slučaj.
Jedini do sad pronađeni uvjetni nedostatak jest klasa slabih ključeva. Ukoliko se koristi jedan od ključeva oblika:

0000, 0000, 0x000, 0000, 0000, 000x, xxxx, 0x000

gdje je "x" bilo koji heksadecimalni broj, moguće je takav ključ identificirati kroz napad korištenjem odabranog otvorenog teksta (engl. *chosen plaintext attack*). To je moguće jer izvođenje XOR operacije nad određenim parovima otvorenog teksta garantira isti rezultat izvođenja XOR operacije nad odgovarajućim šifriranim tekstom. Ukoliko se koristi generator pseudoslučajnih brojeva, vjerojatnost pojavljivanja ovakvog ključa je vrlo mala ($1/2^{96}$), no ukoliko se želi eliminirati i ta mala mogućnost dovoljno je za svaki podključ izvesti XOR operaciju s vrijednosti 0x0dae.
U ovom trenutku razina sigurnosti koju pruža standardni IDEA algoritam sa 128-bitnim ključem smatra se više nego zadovoljavajućom. Ukoliko ni to nije dovoljno, razinu sigurnosti može se povećati korištenjem modifikacija IDEA algoritma opisanih u prethodnom poglavlju (trostruki IDEA algoritam, korištenje nezavisnih podključeva).

5. Zaključak

Obzirom da u ovom trenutku nisu poznate metode kriptoanalize koje bi olakšale napad na algoritam, a napad primjenom čiste sile uopće nije izvediv, IDEA se može smatrati vrlo sigurnim simetričnim algoritmom za šifriranje podataka.
Algoritam je relativno nov, pa se ne isključuje mogućnost da u budućnosti budu pronađene kriptoanalitičke metode koje bi olakšale napade na algoritam, no, u svakom slučaju, u današnje vrijeme takve metode ne postoje.
Ograničenje za korištenje algoritma u komercijalne svrhe predstavlja to što je algoritam patentiran i za njegovu komercijalnu uporabu potrebno je licenciranje.
U ovom trenutku zbog tih razloga uporaba algoritma ograničena je na određene primjene. Svakako najpoznatija od njih je PGP (Pretty Good Privacy) paket, namijenjen inicijalno za šifriranje i autentikaciju poruka elektroničke pošte, koji danas osim sigurne razmjene tih poruka može poslužiti i za zaštitu drugih podataka (datoteka, diskova itd.).