Da li je algoritam DES neprobojan?

DRAGAN PLESKONJIĆ, dipl. ing.

U prethodna dva broja Mog mikra objavljeni su članci o kriptozaštiti podataka. Ovim tekstom tu malu seriju nastavljamo. Do sada je bilo reči o starijim kriptografskim metodama i o jednom savremenom algoritmu (RSA). U ovom broju biće reči o DES algoritmu. Pre toga recimo nešto o značaju kriptografije u savremenom računarstvu.

Značaj zaštite tajnosti podataka

Danas skoro da nema oblasti ljudske delatnosti u kojoj se ne primenjuju računari. Na računarima i računarskoj opremi se čuvaju i obrađuju, a komunikacijskim linijama prenose podaci koji su često od životnog značaja za funkcionisanje različitih sistema, organizacija i institucija. Narušavanje integriteta podataka, neovlašteno čitanje, modifikacija ili brisanje mogu naneti vrlo velike štete vlasniku podataka ili onome na koga se odnose.

Uzmimo nekoliko primera koji ilustruju **potrebu zaštite**:

– podatak o trenutnoj likvidnosti preduzeća ili neka poslovna tajna, ako »procure« u javnost mogu naneti dosta štete toj firmi

– provala u bazu podataka (recimo sa ocenama studenata) može omogućiti izmenu podataka, što je nedopustivo

– mnoge firme čuvaju na računaru personalne podatke o svojim zaposlenim; neovlaštena izmena ili ponekad sam neovlašteni uvid u te podatke može izazvati negativne posledice

– neovlašteni uvid u stanje na računima banaka, ili još gore, lažni nalog za izvršenje novčane transakcije je nedopustiv

– podaci koji se skupljaju u zdravstvu takođe imaju određeni nivo tajnosti koji se mora osigurati

– novi programi (tj. izvorni kodovi) se moraju čuvati zbog mogućnosti krađe još u toku razvoja

– razna naučna, tehnička i tehnološka dostignuća i inovacije zahtevaju zaštitu od krađe podataka

– lična prepiska, različiti popisi, podsetnici, tekstovi i sl. koje uređujete i čuvate na vašem računaru takođe mogu zahtevati zaštitu.

Tako se može navesti još dosta situacija u kojima je zaštita nužna. Možemo reći da je kod nas dosta nizak nivo zaštitne kulture, uključujući i ljude na određenim nivoima rukovođenja koji su odgovorni za sigurnost i tajnost podataka u interesu preduzeća i pojedinaca. Imajući to u vidu, mogu se uskoro i kod nas očekivati senzacionalne novinske vesti o »oticanju« podataka o pojedincima i preduzećima, različitim malverzacijama, možda proneverama i sl. Dakle, sve ono što smo dosad čitali o slučajevima u inostranstvu.

Da se takve situacije ne bi dešavale nužna je zaštita. Već se donose zakoni koji regulišu koji se podaci mogu skupljati, ko ih može skupljati, ko ima pravo uvida u podatke i na koji način treba biti obezbeđena njihova sigurnost. To je u interesu onoga ko podatke skuplja i onoga na koga se oni odnose.

U zapadnim zemljama su ovi mehanizmi (zakonski okviri i stvarna briga za sigurnost) već razvijeni. Na tržištu računarske opreme se već prodaje određena hardverska i softverska oprema koja se koristi za zaštitu.

Kriptografske metode zaštite, o kojima je reč u ovoj maloj seriji napisa, su jedna grupa metoda zaštite uz organizacione, tehničke i programske metode zaštite.

Kriptografija (grčki »skriveno pisanje«) podrazumeva, kao što je ranije pisano, prevođenje podataka u oblik koji je nerazumljiv svima onima koji nisu ovlašteni imati uvid u podatke. U takvom obliku podaci su sigurni od neovlaštenog čitanja. Modifikacija ovih podataka je skoro nemoguća, a da se to ne otkrije. Ovim je donekle zaštićen i integritet podataka jer će zlonamerni teško prepoznati podatke na koje žele destruktivno delovati (npr. izbrisati ih). Naravno, sve će ovo biti ispunjeno tek uz dobro izabrani kriptografski algoritam.

U prošlom broju je opisan predstavnik sistema sa javnim ključevima – RSA algoritam. Taj algoritam spada u asimetrične algoritme jer se kod njega jedan ključ koristi za šifrovanje, a drugi za dešifrovanje. U ovom broju biće prikazan DES algoritam koji je predstavnik simetričnih algoritama (isti ključ se koristi za šifrovanje i dešifrovanje).

DES algoritam

DES (**D**ata **E**ncryption **S**tandard) je federalni standard za šifrovanje podataka SAD, koji se koristi tamo gde je kriptografija neophodna, kao u prenosu neklasificiranih podataka za potrebe vlade i vladinih agencija SAD. Sistem na kom je algoritam baziran razvio je IBM, a usvojio Nacionalni biro za standarde (ANSI) i javno ga proglasio federalnim standardom za obradu informacija. DES je preporučen za upotrebu i od strane američkog bankarskog udruženja (ABA – American Bankers Association). Detaljna specifikacija kompletnog algoritma je već odavno dostupna.

Izrađuju se uređaji specijalne namene za šifrovanje po ovom algoritmu, koji su raspoloživi na tržištu kompjuterske opreme. Ovakva hardverska izvedba je dosta pogodna i daje zadovoljavajuće rezultate u pogledu brzine šifrovanja. Programske implementacije su moguće, ali su nepogodne zbog male brzine.

Algoritam šifrovanja podataka. Algoritam je projektovan za šifrovanje i dešifrovanje blokova podataka koji se sastoje od 64 bita pod kontrolom 64-bitnog ključa (ovo je u suštini 56-bitni ključ, a ostalih 8 bita su paritetni). Dešifrovanje se obavlja istim ključem kao i šifrovanje, s tim što se podključevi uzimaju u obrnutom redosledu tako da postupci šifrovanja i dešifrovanja budu inverzni. Postupak šifrovanja (i dešifrovanja) se obavlja u 16 iteracija. Logička struktura DES algoritma prikazana je na slici 1, a dijagram toka algoritma na slici 2.

Blok koji će biti šifrovan, podvrgnut je inicijalnoj transformaciji IP, a potom složenom računanju zavisnom od ključa i konačno permutaciji koja je inverzna inicijalnoj permutaciji IP–1. Računanje, zavisno od ključa, može jednostavno biti definisano pomoću funkcije F zvane funkcija šifrovanja i funkcije KS koja određuje izbor podključa od osnovnog ključa.

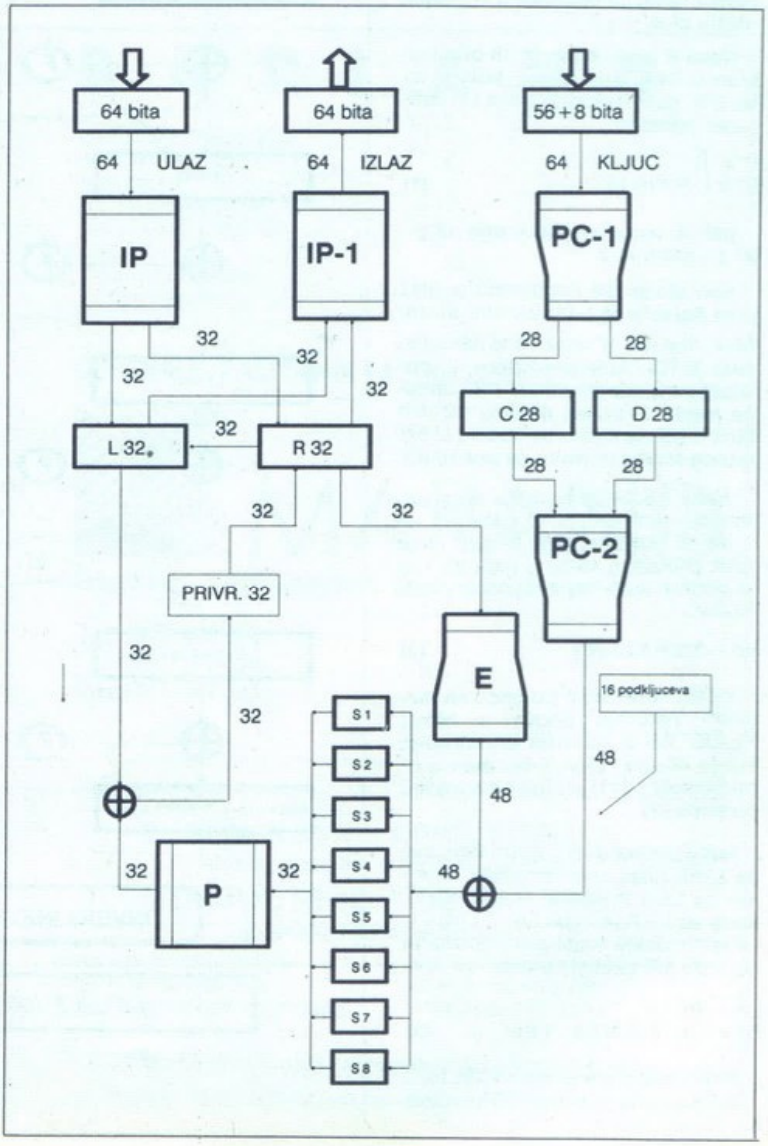
Ovde će ukratko biti prikazan algoritam šifrovanja (i dešifrovanja) podataka.

Neka je na ulazu blok od 64 bita. Sastoji se od dva jednaka podbloka, L i R (levog i desnog). LR označava da se blok sastoji od bitova L koje slede bitovi od R. 64 bita ulaznog bloka prvo se podvrgavaju sledećoj transformaciji zvanoj inicijalna transformacija (oznaka IP).

IP

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Sl.1. Logicka struktura DES algoritma



Znači da permutovani izlaz ima 58. bit ulaza kao prvi izlazni bit, 50. bit ulaza kao drugi bit itd. do 7. bita ulaza kao poslednjeg. Tako dobijeni izlazni blok ove permutacije je ulaz za složeno računanje, zavisno od ključa, što je opisano kasnije.

Izlaz iz računanja se podvrgava permutaciji koja je inverz inicijalne permutacije (oznaka IP−1).

IP−1

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

Tako izlaz iz algoritma ima 40. bit bloka koji je izlaz iz računanja, kao prvi bit; 8. bit kao drugi bit, sve do 25. bita, koji je zadnji bit izlaza iz algoritma.

Računanje koje se vrši nakon IP, a pre IP−1, sastoji se od 16 iteracija. Ovde će taj proces biti opisan u obliku funkcije F koja operiše sa dva bloka, jednim od 32 bita i jednim od 48 bita, i proizvodi blok od 32 bita.

Uzmimo da se 64 bita ulaznog bloka sastoje od 32-bitnog bloka L iza koga sledi 32-bitni blok R. Koristeći notaciju definisanu u uvodu, ulazni blok je LR.

Neka K bude blok od 48 bita izabran iz 64-bitnog ključa, tada je izlaz L'R' nakon obrade ulaza LR definisan pomoću:

$$L' = R$$
$$R' = L \oplus F(R,K) \qquad (1)$$

gde ⊕ označava sabiranje bit po bit po modulu 2.

Kao što je pre napomenuto, ulaz prve iteracije je permutovani ulazni blok. Ako je L'R' izlaz 16-te iteracije, tada je R'L' blok predizlaza, tj. pre izlazne transformacije L' i R' zamene mesta. U svakoj iteraciji različiti blok K bitova ključa se izabira iz 64-bitnog ključa (formira se podključ).

Neka KS bude funkcija koja uzima prirodni broj n iz intervala od 1 do 16 i 64-bitni blok KLJUČ i kao izlaz proizvodi 48-bitni blok Kn koji je permutovani izbor bitova iz bloka KLJUČ.

$$Kn = KS(n,KLJUČ) \qquad (2)$$

sa Kn određenim pomoću 48 različitih položaja bitova u bloku KLJUČ. KS je funkcija određivanja ključa. Naime, blok K korišten u n-toj iteraciji od **(1)** je blok Kn određen pomoću **(2)**.

Neka permutovani ulazni blok bude L0R0 (ulaz prve iteracije). Uzmimo da Ln i Rn budu L' i R' u **(1)**. Kada su L i R jednaki Ln−1 i Rn−1, i K je Kn; dakle, kada je n u području od 1 do 16, tada **(1)** prelazi u:

$$Ln = Rn-1$$
$$Rn = Ln-1 \oplus F(Rn-1,Kn) \qquad (3)$$

Blok predizlaza je tada R16L16.

Funkcija KS proizvodi 16 ključeva Kn koji su potrebni za algoritam.

Dešifrovanje. Permutacija IP−1 primenjena na blok predizlaz je inverz inicijalne permutacije primenjene na ulaz. Dakle, iz **(1)** sledi:

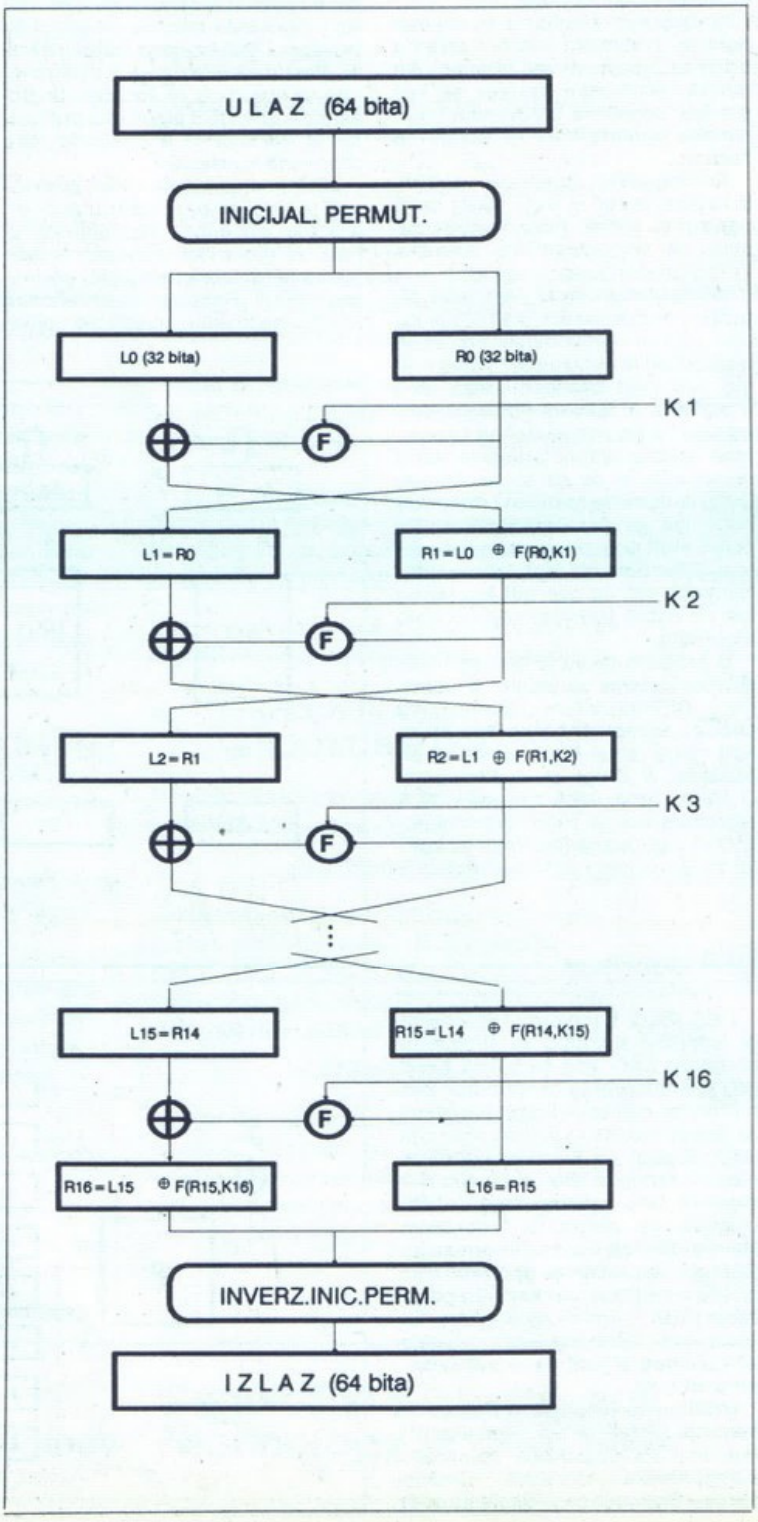
$$R = L'$$
$$L = R' \oplus F(L',K) \qquad (4)$$

Za dešifrovanje je samo potrebno primeniti potpuno isti algoritam kao i za šifrovanje bloka poruka, pazeći pri tome da se pri svakoj iteraciji u dešifrovanju koristi isti blok K (tj. podključ) kao i u šifrovanju. Dešifrovanje se može opisati pomoću sledeće jednakosti:

$$Rn-1 = Ln$$
$$Ln-1 = Rn \oplus F(Ln,Kn) \qquad (5)$$

gde je sada R16L16 permutovani ulazni blok za dešifrovanje i L0R0 je blok predizlaza. Tako se, kod dešifrovanja, K16 koristi kod prve iteracije, K15 kod druge i sve tako do K1, koji se koristi u 16. iteraciji.

Sl.2. Dijagram toka algoritma



Funkcija šifre F(R,K). Prikaz funkcije F(R,K) dat je na slici 3. Uzmimo da E označava funkciju koja uzima blok od 32 bita kao ulaz i proizvodi blok od 48 bita kao izlaz. Neka E bude takav da 48 bita svog izlaza daje kao 8 blokova od po 6 bita biranjem bitova sa svog ulaza oslanjajući se na tabelu E.

E

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

Tako su prva tri bita od E(R) bitovi na pozicijama 32, 1 i 2 u R, dok su poslednja dva bita u E(R) bitovi na pozicijama 32 i 1.

Svaka od funkcija S1, S2..., S8 uzima 6-bitni blok kao ulaz i proizvodi 4-bitni blok kao izlaz što je ilustrovano korišćenjem tabele S1.

S1

broj vrste	broj kolone															
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
	1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
	2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
	3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

Ako je S1 funkcija definisana u ovoj tabeli i blok od 6 bita, tada se S1(B) određuje ovako:

Prvi i poslednji bit od B predstavljaju, u bazi 2, brojeve od 0−3. Uzmimo da je taj broj i. Srednja 4 bita iz B predstavljaju, takođe u bazi 2, broj između 0 i 15. Uzmimo da je taj broj jednak j. Ako u tabeli nađemo itu vrstu i j-tu kolonu, u preseku se nalazi broj između 0 i 15. Treba ga predstaviti u bazi 2 i to je S1(B) iz S1 za ulaz B. Na primer, za ulaz 011011, vrsta je 01, a kolona 1101 (kolona 13). U vrsti 1 i koloni 13 nalazi se 5, tako da je izlaz 0101.

Funkcije izbora S2, S3..., S8 ovde neće biti navedene jer je postupak isti, jedino se brojevi u tablici razlikuju, što neće uticati na daljnje razmatranje DES algoritma.

Permutaciona funkcija P proizvodi 32-bitni izlaz iz 32-bitnog ulaza permutovanjem bitova ulaznog bloka. Ta funkcija je određena pomoću sledeće tabele:

P

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

Izlaz P(L) za funkciju P dobiven pomoću ove tabele je dobiven iz izlaza L uzimanjem 16-og bita iz L kao prvog bita u P(L), 7-og bita kao drugog bita u P(L) i tako sve do 25-og bita iz L koji je uzet kao 32-i bit u P(L).

Da bismo definisali F(R,K) prvo definišemo B1, B2 ..., B8 kao blokove od po 6 bita za koje vredi:

$$B1B2 \ldots B8 = K \oplus E(R) \quad (6)$$

Blok F(R,K) je tada definisan kao:
P(S1(B1)S2(B2) ... S8(B8)) **(7)**

Dakle, $K \oplus E(R)$ je najpre podeljeno u 8 blokova, kao što je pokazano u **(6)**. Tada je svaki blok uzet kao ulaz u Si i 8 blokova S1(B1), S2(B2),..., S8(B8), po 4 bita svaki, su spojeni u jedan blok od 32 bita koji čini ulaz u P. Izlaz **(7)** je tada izlaz iz funkcije F za ulaz R i K.

Nakon računanja po funkciji F(R,K) rezultat se smešta u privremeni registar. Prethodni sadržaj registra R se prebaci u L, a tek onda sadržaj privremenog registra (rezultat računanja) ide u R. Nakon ovoga može početi sledeća iteracija.

Izbor ključa. DES ima 64-bitni ključ. Ključ, u suštini, ima 56 osnovnih i 8 paritetnih bita. S obzirom da paritetni biti zavise od osnovnih, onda je to, sa stanovišta sigurnosti, 56-bitni ključ. Taj se ključ, na početku šifrovanja bloka, permutovanim izborom svodi na 56 bita (2 podbloka ključa po 28 bita). Ovaj izbor određen je tabelom koja se obično obeležava sa PC−1 (engl. permuted choice 1), koju ovde nećemo navoditi. Ključ se tada podeli na dva dela po 28 bita. Potom se, pri svakoj iteraciji, pravi pomak (shift) bita ključa prema sledećoj tabeli:

broj iteracije	broj pomaka
1,2,9,16	1
3−8, 10−15	2

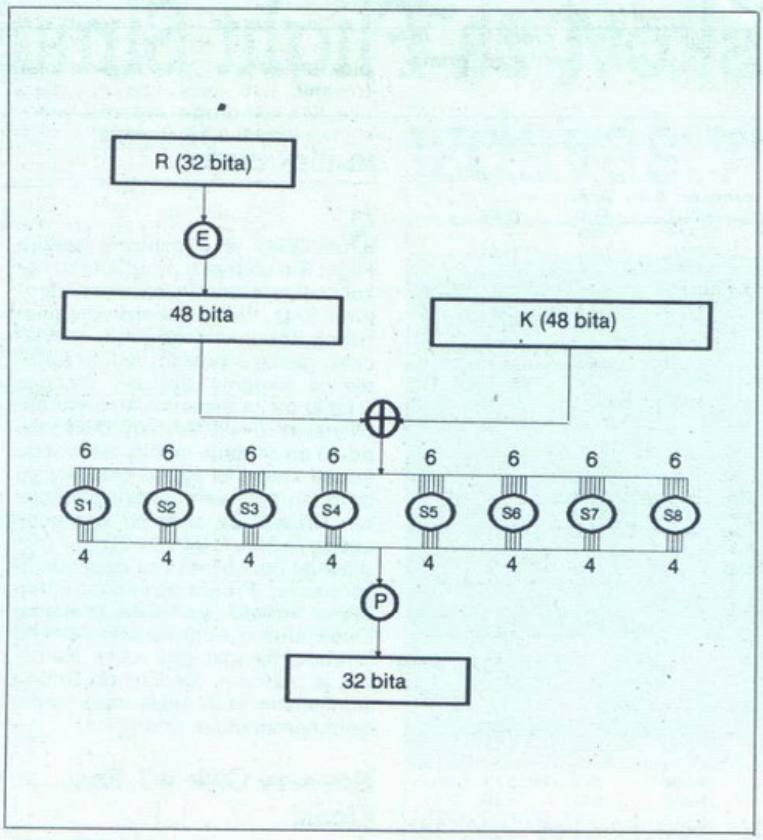
Zatim se, prema drugoj permutacionoj tabeli, PC−2 od 56 bita odabire 48 bita koji ulaze u daljnji proces šifrovanja.

Poboljšane verzije DES algoritma. Često se sreću modifikovane verzije DES algoritma koje poboljšavaju karakteristike algoritma i neutrališu neke uočene nedostatke.

To su:
- šifrovanje tokom (stream cipher mode)
- šifrovanje povratnom vezom (cipher feedback mode)
- šifrovanje ulančavanjem blokova (block chaining mode).

Ocena DES algoritma. Ovaj algoritam je praktično prvi standard u ovom području. Javno je publikovan čime je na neki način svet bio izazvan da ga »razbije«. To nikom dosad nije pošlo za rukom, odnosno nije objavljeno da je nekom uspelo da algoritam razbije. Poznati kriptografi mu nalaze dosta zamerki, ali izgleda sve ostaje na zamerkama. Algoritam je i dalje vrlo siguran i verovatno će biti još dosta dugo primenjivan. Na ruku mu ide dosta dobra brzina šifrovanja u hardverskim realizacijama koje imaju i prihvatljive cene. Primena je dosta jednostavna što je olakšavajuće za krajnjeg korisnika koji ne mora biti stručnjak u području kriptografije. Ovaj algoritam se puno primenjuje u SAD. Ipak, široka primena izaziva brojne kriptoanalitičare i one koji bi želeli ostvariti korist razbijanjem DES algoritma, pa to treba imati u vidu. Problem je i upravljanje ključevima (key management), tj. dojava 64-bitnog ključa ako više udaljenih učesnika ima šifrovanu komunikaciju, a iz razloga sigurnosti se ključ često menja. U takvim situacijama je možda bolje koristiti neki drugi manje poznati algoritam ili neku modifikaciju DES algoritma.

Na kraju se može reći da, za većinu uobičajenih zahteva, DES algoritam možemo uspešno primeniti, dok se za specijalne namene mogu kreirati vlastiti (poželjno je tajni) algoritmi.



Sl. 3. Prikaz funkcije F(R,K)

Drugi algoritmi

Navedimo i neke od drugih svetski poznatih algoritama kriptozaštite o kojima dosad nismo govorili:

1. B-Crypt je implementacija simetričnog kriptoalgoritma zvanog B152 (potiče od British Telecoma). Ovaj algoritam spada u simetrične algoritme. Šifruje se 64-bitni blok uz 64-bitni ključ (64 bita = 58 bita podataka + 8 paritetnih bita) i 64-bitni inicijalizacioni vektor za generator pseudoslučajnih brojeva. Nisu objavljeni principi rada ovog algoritma.

2. FEAL-1 (Fast data enciphering algorithm) je japanski algoritam za »brzo« šifrovanje. To je simetrični algoritam koji šifruje 64-bitni blok koristeći 64-bitni ključ. Šifrovanje se obavlja u svega 4 iteracije, pa je algoritam brži od DES algoritma. Nema (prema našim saznanjima) generalnih publikacija o sigurnosti ovog algoritma.

Postoje brojni drugi algoritmi za šifrovanje podataka. U ovoj maloj seriji napisa prikazani su neki od najpoznatijih. Stalno se kreiraju novi algoritmi prema različitim zahtevima (sigurnost, brzina, cena, praktična primenjivost itd.). Može se reći da je još u toku borba između kriptografa koji šifarske algoritme stvaraju i kriptoanalitičara koji ih »razbijaju«. To je borba koja je davno počela i kojoj se kraj ne nazire. Apsolutno sigurni sistem ne postoji i može se samo težiti za postizanjem što veće sigurnosti.