Diferencijalna kriptoanaliza

Gašpar, Leonora

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Leonora Gašpar

DIFERENCIJALNA KRIPTOANALIZA

Diplomski rad

Voditelj rada:
prof. dr.sc. Andrej Dujella

Zagreb, srpanj, 2016.

Ovaj diplomski rad obranjen je dana _____ pred ispitnim povjerenstvom u sastavu:

1. _____, predsjednik
2. _____, član
3. _____, član

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Sadržaj

Uvod

Suvišno je pričati o značaju kriptografije u današnjem društvu, u doba kada se većina novčanih transakcija odvija digitalnim putem, gdje razne institucije imaju velike količine podataka koji bi mogli načiniti veliku štetu dođu li u krive ruke. Zbog toga matematičari, kriptografi, rade na razvoju što boljih kriptosustava. Naravno, javlja se i potreba za njihovim testiranjem, otkrivanjem mogućih mana koje bi mogle dovesti do njihovog razbijanja. Kriptoanaliza je znanstvena disciplina koja se bavi proučavanjem postupaka za čitanje skrivenih poruka bez poznavanja ključa.
Diferencijalna kriptoanaliza jedan je od moćnih napada kojeg su prvi javno opisali Biham i Shamir. Primjenjiva je na bilo koji simetrični blokovni kriptosustav. Diferencijalna kriptoanaliza analizira učinak određenih razlika u parovima šifrata na razlike rezultirajućih parova šifrata. Te razlike mogu se upotrijebiti za pronalazak najvjerojatnijeg ključa. U ovom radu obrađujemo tu metodu na nekim varijantama DES-a i na FEAL.
DES (Data Encryption Standard) je bio korišten kao standardni algoritam za šifriranje u SAD-u od sredine sedamdesetih pa sve do 2002. Spada u blokovne kriptosustave te je na njega moguće primjeniti metodu diferencijalne kriptoanalize. Međutim, ustvrdilo se da je ta metoda bila poznata još 1974. te da su je konstruktori DES-a imali u vidu kod dizajna S-kutija i permutacije P.
Važno je napomenuti da na kraju diferencijalna kriptoanaliza nije razbila DES. Godine 1998. konstruirano je računalo "DES Cracker" koje je moglo razbiti DES u 56 sati i to tako da pretražuje čitav prostor ključeva od DES-a veličine 2^{56}.

Poglavlje 1

Uvod u diferencijalnu kriptoanalizu

U ovom poglavlju uvodimo terminologiju, predstavljamo ideju iza diferencijalne kriptoanalize, te definiramo pojmove koje ćemo koristiti u kasnijim poglavljima.

Diferencijalna kriptoanaliza jedan je od najmoćnijih napada na blok-kriptosustave. Prvi su je javno opisali izraelski kriptoanalitičari Eli Biham i Adi Shamir kasnih 1980ih, no bila je poznata i više od 10 godina ranije tvorcima kriptografskog algoritma Data Encryption Standard (DES).

1.1 Oznake i definicije

Poruka koju želimo šifrirati zove se otvoreni tekst. Postupak transformiracije otvorenog teksta koristeći unaprijed dogovoreni ključ zove se šifriranje. Šifriranjem otvorenog teksta dobije se šifrat.
Kriptoanaliza ili dekriptiranje je znanstvena disciplina koja se bavi proučavanjem postupaka za čitanje skrivenih poruka bez poznavanja ključa.
Kriptografski algoritam ili šifra je matematička funkcija koja se koristi za šifriranje i dešifriranje. Općenito, radi se o dvije funkcije, jednoj za šifriranje, a drugoj za dešifriranje. Te funkcije preslikavaju osnovne elemente otvorenog teksta (najčešće su to slova, bitovi, grupe slova ili bitova) u osnovne elemente šifrata, i obratno.
Kriptosustav se sastoji od kriptografskog algoritma, te svih mogućih otvorenih tekstova, šifrata i ključeva. Iterativni kriptosustavi su obitelj kriptološki jakih funkcija koje se temelje na iteriranju slabije funkcije n puta. Svaka iteracija zove se *runda* i kriptosustav se zove n-rundni kriptosustav. Funkcija runde je funkcija čiji je input output prethodne runde i potključ. Obično se zadaje tablicama (supstitucijskim tablicama ili S-kutijama), aritmetičkim operacijama, bitovnim operacijama ili operacijom ekskluzivno ILI (XOR).

Potključ je vrijednost koja ovisi o ključu i računa se pomoću posebnog algoritma - algoritma dodjeljivanja ključa (en. key scheduling algorithm).

Razlikujemo četiri osnovna nivoa kriptoanalitičkih napada: samo šifrat, poznat otvoren tekst, odabrani otvoreni tekst, odabrani šifrat. Diferencijalna kriptoanaliza spada u metodu "odabrani otvoreni tekst", što znači da kriptoanalitičar ima mogućnost odabira teksta koji će biti šifriran, te može dobiti njegov šifrat.

Predstavimo sada ideju diferencijalne kriptoanalize na jednostavnom kriptosustavu. Neka su m, c i k nizovi binarnih brojeva duljine b, gdje m predstavlja otvoreni tekst, c šifrat i k tajni ključ, a $\oplus$ operacija XOR po bitovima.
Šifriramo poruku m na sljedeći način:

$$c = m \oplus k$$

Ako je ključ k nasumično odabran i koristi se samo jednom, kriptoanalitičar ne može dobiti nikakve informacije o m promatrajući šifrat c. No što se dogodi ako koristimo isti ključ dvaput? Pretpostavimo da smo koristili ključ k za šifriranje poruka m_0 i m_1 da bi dobili c_0 i c_1. Tada napadač koji presretne oba šifrata može izračunati:

$$c_0 \oplus c_1 = (m_0 \oplus k) \oplus (m_1 \oplus k) = m_1 \oplus m_1$$

Drugim riječima, kriptoanalitičar može izračunati XOR dva otvorena teksta izravno iz presretnutih šifrata. Ako poruke sadrže redundaciju, na primjer ako predstavljaju tekst iz prirodnog jezika, tada napadač može doći do zaključaka o otvorenom tekstu pomoću XOR-a šifrata.

Definicija 1.1.1. *Neka je $\pi_S : \{0,1\}^m \to \{0,1\}^n$ S-kutija, i neka je (x, x^*) uređeni par nizova bitova duljine m. Kažemo da je input XOR x' S-kutije $x' = x \oplus x^*$, a output XOR y' je $y' = \pi_S(x) \oplus \pi_S(x^*)$. Za $x' \in \{0,1\}^m$, definiramo $\Delta(x')$ kao skup svih uređenih parova (x, x^*) za koje je input XOR jednak x'.*

Iz $x' = x \oplus x^*$ vrijedi i : $x^* = x \oplus x'$. Prema tome $\Delta(x')$ možemo zapisati na sljedeći način:

$$\Delta(x') = \{(x, x \oplus x') : x \in \{0,1\}^m\}.$$

Dakle, skup $\Delta(x')$ sadrži 2^m parova.
Za svaki par u $\Delta(x')$ možemo izračunati output XOR S-kutije. Zatim možemo tabulirati dobivenu distribuciju output XOR-a. Postoji 2^m output XOR-a koji su distribuirani kroz 2^n

mogućih vrijednosti. Neuniformna distribucija outputa biti će temelj za uspješan kriptoanalitički napad.

Ne možemo dobiti puno informacija razmatrajući jednu poruku i šifrat, ali možemo dobiti puno više uzmemo li parove poruka i šifrata. U našem jednostavnom primjeru manipulacijom šifrata eliminirali smo uporabu tajnog ključa.
U stvarnosti će sama metoda biti puno kompliciranija, ali promatranje razlika između parova otvorenog teksta kako su šifrirani i odabir razlike koja nam dozvoljava da zanemarimo uporabu ključa (barem prilikom analize) čine glavnu ideju iza diferencijalne kriptoanalize.

Primjer 1.1.2. *Pretpostavimo da $n = m = N_r = 4$, gdje je N_r broj rundi, a n i m kao iz definicije. Neka je π_S definiran na sljedeći način:* $0 \leftrightarrow (0,0,0,0), 1 \leftrightarrow (0,0,0,1), \cdots, 9 \leftrightarrow (1,0,0,1), A \leftrightarrow (1,0,1,0), \cdots, F \leftrightarrow (1,1,1,1)$ *gdje su input z i output $\pi_S(z)$ zapisani u heksadecimalnom formatu.*

z	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$\pi_S(z)$	E	4	D	1	2	F	B	8	3	A	6	C	5	9	0	7

Tablica 1.1: S-kutija za primjer **??**

Uzmimo da je input XOR para dva inputa $x' = 1011$.
Tada: $\Delta(1011) = \{(0000, 1011), (0001, 1010), \cdots, (1111, 0100)\}$.
Za svaki uređeni par skupa $\Delta(1011)$ *računamo output XOR od* π_S. *Za svaki redak Tablice* **??** *vrijedi:* $x \oplus x^* = 1011$ *i* $y' = y \oplus y^*$ *(uz oznake* $y = \pi_S(x)$, $y^* = \pi_S(x^*)$*).*

x	x^*	y	y^*	y'
0000	1011	1110	1100	0010
0001	1010	0100	0110	0010
0010	1001	1101	1010	0111
0011	1000	0001	0011	0010
0100	1111	0010	0111	0101
0101	1110	1111	0000	1111
0110	1101	1011	1001	0010
0111	1100	1000	0101	1101
1000	0011	0011	0001	0010
1001	0010	1010	1101	0111
1010	0001	0110	0100	0010
1011	0000	1100	1110	0010
1100	0111	0101	1000	1101
1101	0110	1001	1011	0010
1110	0101	0000	1111	1111
1111	0100	0111	0010	0101

Tablica 1.2:

Prebrojimo li koliko puta se ponavlja svaki od nizova bitova u zadnjem stupcu Tablice **??***, dobivamo sljedeće distribucije output XOR-a:*

niz bitova	0000	0001	0010	0011	0100	0101	0110	0111
broj ponavljanja	0	0	8	0	0	2	0	2

niz bitova	1000	1001	1010	1011	1100	1101	1110	1111
broj ponavljanja	0	0	0	0	0	2	0	2

Tablica 1.3:

1.2 Tablica distribucije razlika

Definicija 1.2.1. *Tablica koja prikazuje distribuciju input XOR-ova i output XOR-ova svih mogućih parova S-kutija naziva se tablica distribucije razlika (en. difference distribution table) S-kutije.*

U toj tablici svaki redak odgovara određenom input XOR-u, svaki stupac odgovara određenom output XOR-u, a sami elementi tablice predstavljaju broj mogućih parova s određenim input XOR-om i output XOR-om. U našem primjeru samo 5 od 16 mogućih XOR-a se zapravo pojavljuju. Taj primjer ima jako neuniformnu distribuciju.

Primjer 1.2.2. *Tablica distribucije razlika za Primjer* **??***:*

output	input XOR															
XOR	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	2	0	0	0	2	0	2	4	0	4	2	0	0
2	0	0	0	2	0	6	2	2	0	2	0	0	0	0	2	0
3	0	0	2	0	2	0	0	0	0	4	2	0	2	0	0	4
4	0	0	0	2	0	0	6	0	0	2	0	4	2	0	0	0
5	0	4	0	0	0	2	2	0	0	0	4	0	2	0	0	2
6	0	0	0	4	0	4	0	0	0	0	0	0	2	2	2	2
7	0	0	2	2	2	0	2	0	0	2	2	0	0	0	0	4
8	0	0	0	0	0	0	2	2	0	0	0	4	0	4	2	2
9	0	2	0	0	2	0	0	4	2	0	2	2	2	0	0	0
A	0	2	2	0	0	0	0	0	6	0	0	2	0	0	4	0
B	0	0	8	0	0	2	0	2	0	0	0	0	0	2	0	2
C	0	2	0	0	2	2	2	0	0	0	0	2	0	6	0	0
D	0	4	0	0	0	0	0	4	2	0	2	0	2	0	2	0
E	0	0	2	4	2	0	0	0	6	0	0	0	0	0	2	0
F	0	2	0	0	6	0	0	0	0	4	0	2	0	0	2	0

Tablica 1.4:

U stupcima i retcima tablice zapisali smo output i input XOR-eve u heksadecimalnom obliku. Podaci iz Tablice **??** *nalaze se u retku B jer* $(B)_{16} = (1011)_2$

Sljedeće definicije vezane su za tablice distribucije razlika :

Definicija 1.2.3. *Neka su X i Y dvije vrijednosti koje predstavljaju potencijalne input i output XOR-eve neke S-kutije, tim redom. Kažemo da X može uzrokovati Y preko S-kutije ako postoji par u kojem je input XOR S-kutije jednak X i output XOR S-kutije jednak Y.*
To označavamo sa : $X \rightarrow Y$*, odnosno u suprotnom* $X \nrightarrow Y$

Primjer 1.2.4. *Uzmimo input XOR S1'*$_I = 34_x$ *(bro*j_x *znači da je bro j u heksadecimalnom zapisu) On ima samo 8 mogućih output XOR-a, dok je ostalih 8 nemoguće. Mogući output XOR-i S1'*$_O$ *su:* $1_x, 2_x, 3_x, 4_x, 7_x, 8_x, D_x, F_x$*. Prema tome, input XOR S1'*$_I = 34_x$ *može uzrokovati output XOR S1'*$_O = 1_x(34_x \rightarrow 1_x)$
Također vrijedi: $34_x \rightarrow 2_x$ *i* $34_x \rightarrow F_x$*. S druge strane,* $34_x \nrightarrow 0_x$ *i* $34_x \nrightarrow 9_x$*.*

Primjer **??** pokazuje da za fiksiran input XOR mogući output XOR-i nemaju uniformnu distribuciju.
Sljedeća definicija proširuje definiciju **??** s vjerojatnostima:

Definicija 1.2.5. *Kažemo da X može uzrokovati Y s vjerojatnošću p preko S-kutije ako je output XOR jednak Y za dio p parova u kojima je input XOR S-kutije jednak X.*

Primjer 1.2.6. $34_x \rightarrow 2_x$ *proizlazi iz 16 od 64 para od S1 (vidi tablicu 1.5 - čitamo broj u retku* 34_x*, stupcu 2), dakle s vjerojatnošću* $\frac{1}{4}$*.* $34_x \rightarrow 4_x$ *rezultira iz 2 od 64 para od S1, dakle vjerojatnost je* $\frac{1}{32}$*.*

Sljedeća definicija proširuje prethodne dvije definicije za uporabu s funkcijom F:

Definicija 1.2.7. *Neka su X i Y vrijednosti koje predstavljaju potencijalni input i output XOR za funkciju F. Kažemo da X može uzrokovati Y s vjerojatnošću p preko funkcije F ako je output XOR jednak Y za dio p svih mogućih input parova enkriptiranih pomoću svih mogućih vrijednosti podključa kod kojih je input XOR funkcije F jednak X.*
Ako vrijedi $p > 0$ *to označavamo sa:* $X \rightarrow Y$

1.3 Karakteristike

Prethodno opisani algoritam ostavlja nam problem "guranja" znanja XOR-ova parova otvorenog teksta kroz što više rundi (korak 3), a da ih pritom ne pretvorimo u nizove nula. Kad su XOR-ovi parova nula, oba teksta su jednaka, outputi su također jednaki, pa su i svi ključevi jednako vjerojatni. Osim toga, u diferencijalnoj kriptoanalizi poželjno bi bilo imati nekakve statističke informacije o razlikama u međurundama tokom enkripcije, ako znamo samo razliku otvorenog teksta. Sve to inspiracija je za uvođenje pojma karakteristike:

Input XOR	Output XOR															
	0x	1x	2x	3x	4x	5x	6x	7x	8x	9x	Ax	Bx	Cx	Dx	Ex	Fx
00x	64	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
01x	0	0	0	6	0	2	4	4	0	10	12	4	10	6	2	4
02x	0	0	0	8	0	4	4	4	0	6	8	6	12	6	4	2
03x	14	4	2	2	10	6	4	2	6	4	4	0	2	2	2	0
04x	0	0	0	6	0	10	10	6	0	4	6	4	2	8	6	2
05x	4	8	6	2	2	4	4	2	0	4	4	0	12	2	4	6
06x	0	4	2	4	8	2	6	2	8	4	4	2	4	2	0	12
07x	2	4	10	4	0	4	8	4	2	4	8	2	2	2	4	4
08x	0	0	0	12	0	8	8	4	0	6	2	8	8	2	2	4
09x	10	2	4	0	2	4	6	0	2	2	8	0	10	0	2	12
0Ax	0	8	6	2	2	8	6	0	6	4	6	0	4	0	2	10
0Bx	2	4	0	10	2	2	4	0	2	6	2	6	6	4	2	12
0Cx	0	0	0	8	0	6	6	0	0	6	6	4	6	6	14	2
0Dx	6	6	4	8	4	8	2	6	0	6	4	6	0	2	0	2
0Ex	0	4	8	8	6	6	4	0	6	6	4	0	0	4	0	8
0Fx	2	0	2	4	4	6	4	2	4	8	2	2	2	6	8	8
10x	0	0	0	0	0	0	2	14	0	6	6	12	4	6	8	6
11x	6	8	2	4	6	4	8	6	4	0	6	6	0	4	0	0
12x	0	8	4	2	6	6	4	6	6	4	2	6	6	0	4	0
13x	2	4	4	6	2	0	4	6	2	0	6	8	4	6	4	6
14x	0	8	8	0	10	0	4	2	8	2	2	4	4	8	4	0
15x	0	4	6	4	2	2	4	10	6	2	0	10	0	4	6	4
16x	0	8	10	8	0	2	2	6	10	2	0	2	0	6	2	6
17x	4	4	6	0	10	6	0	2	4	4	4	6	6	6	2	0
18x	0	6	6	0	8	4	2	2	2	4	6	8	6	6	2	2
19x	2	6	2	4	0	8	4	6	10	4	0	4	2	8	4	0
1Ax	0	6	4	0	4	6	6	6	6	2	2	0	4	4	6	8
1Bx	4	4	2	4	10	6	6	4	6	2	2	4	2	2	4	2
1Cx	0	10	10	6	6	0	0	12	6	4	0	0	2	4	4	0
1Dx	4	2	4	0	8	0	0	2	10	0	2	6	6	6	14	0
1Ex	0	2	6	0	14	2	0	0	6	4	10	8	2	2	6	2
1Fx	2	4	10	6	2	2	2	8	6	8	0	0	0	4	6	4
20x	0	0	0	10	0	12	8	2	0	6	4	4	4	2	0	12
21x	0	4	2	4	4	8	10	0	4	4	10	0	4	0	2	8
22x	10	4	6	2	2	8	2	2	2	2	6	0	4	0	4	10
23x	0	4	4	8	0	2	6	0	6	6	2	10	2	4	0	10
24x	12	0	0	2	2	2	2	0	14	14	2	0	2	6	2	4
25x	6	4	4	12	4	4	4	10	2	2	2	0	4	2	2	2
26x	0	0	4	10	10	10	2	4	0	4	6	4	4	4	2	0
27x	10	4	2	0	2	4	2	0	4	8	0	4	8	8	4	4
28x	12	2	2	8	2	6	12	0	0	2	6	0	4	0	6	2
29x	4	2	2	10	0	2	4	0	0	14	10	2	4	6	0	4
2Ax	4	2	4	6	0	2	8	2	2	14	2	6	2	6	2	2
2Bx	12	2	2	2	4	6	6	2	0	2	6	2	6	0	8	4
2Cx	4	2	2	4	0	2	10	4	2	2	4	8	8	4	2	6
2Dx	6	2	6	2	8	4	4	4	2	4	6	0	8	2	0	6
2Ex	6	6	2	2	0	2	4	6	4	0	6	2	12	2	6	4
2Fx	2	2	2	2	2	6	8	8	2	4	4	6	8	2	4	2
30x	0	4	6	0	12	6	2	2	8	2	4	4	6	2	2	4
31x	4	8	2	10	2	2	2	2	6	0	0	2	2	4	10	8
32x	4	2	6	4	4	2	2	4	6	6	4	8	2	2	8	0
33x	4	4	6	2	10	8	4	2	4	0	2	2	4	6	2	4
34x	0	8	16	6	2	0	0	12	6	0	0	0	0	8	0	6
35x	2	2	4	0	8	0	0	0	14	4	6	8	0	2	14	0
36x	2	6	2	2	8	0	2	2	4	2	6	8	6	4	10	0
37x	2	2	12	4	2	4	4	10	4	4	2	6	0	2	2	4
38x	0	6	2	2	2	0	2	2	4	6	4	4	4	6	10	10
39x	6	2	2	4	12	6	4	8	4	0	2	4	2	4	4	0
3Ax	6	4	6	4	6	8	0	6	2	2	6	2	2	6	4	0
3Bx	2	6	4	0	0	2	4	6	4	6	8	6	4	4	6	2
3Cx	0	10	4	0	12	0	4	2	6	0	4	12	4	4	2	0
3Dx	0	8	6	2	2	6	0	8	4	4	0	4	0	12	4	4
3Ex	4	8	2	2	2	4	4	14	4	2	0	2	0	8	4	4
3Fx	4	8	4	2	4	0	2	4	4	2	4	8	8	6	2	2

Tablica 1.5: Tablica distribucije razlika za S-kutiju S1 od DES-a

Definicija 1.3.1. *Neka je n prirodan broj. n-rundna karakteristika je uređena trojka oblika* $\Omega = (\Omega_P, \Omega_\Lambda, \Omega_T)$ *gdje je* Ω_P *XOR otvorenog teksta,* Ω_T *XOR šifrata i* Ω_Λ *n-torka:* $\Omega_\Lambda = (\Lambda_1, \Lambda_2..., \Lambda_n)$*, a* $\Lambda_i = (\lambda_I^i, \lambda_O^i)$ *gdje su* λ_I^i *i* λ_O^i *m/2-bitni nizovi i m je veličina bloka kriptosustava.*
Karakteristika ima sljedeća svojstva:

$$\begin{aligned}
\lambda_I^1 &= desna\ polovica\ od\ \Omega_P \\
\lambda_I^2 &= lijeva\ polovica\ od\ \Omega_P \oplus \lambda_O^1 \\
\lambda_I^n &= desna\ polovica\ od\ \Omega_T \\
\lambda_I^{n-1} &= lijeva\ polovica\ od\ \Omega_T \oplus \lambda_O^n
\end{aligned}$$

te za svaki i takav da $2 \leq i \leq n-1$*:*

$$\lambda_O^i = \lambda_I^{i-1} \lambda_I^{i+1}$$

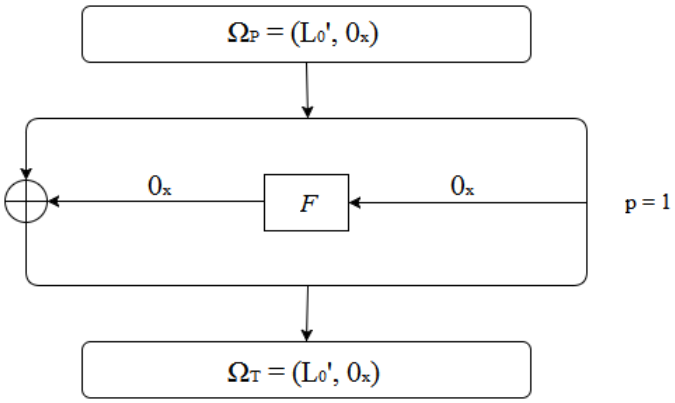
Ukratko, *n*-rundnu karakteristiku čine:

- XOR vrijednost dva otvorena teksta
- XOR vrijednost dva šifrata
- XOR vrijednosti inputa svake runde u dva izvršavanja
- XOR vrijednosti outputa svake runde u dva izvršavanja

Karakteristika ima svoju vjerojatnost *p*. *p* predstavlja vjerojatnost da su XOR odabranog otvorenog teksta nasumičnog para, runda i XOR šifrata jednaki onima iz te karakteristike. Navodimo neke primjere karakteristika, uz oznake $\Omega_P = (L_0', R_0')$, $\Omega_T = (R_1', L_1')$.

Primjer 1.3.2. *1-rundna karakteristika sa vjerojatnošću p = 1, za proizvoljan* L_0'*:*

$$R_0' = 0_x,\ L_1' = R_0' = 0_x,\ R_1' = L_0'$$



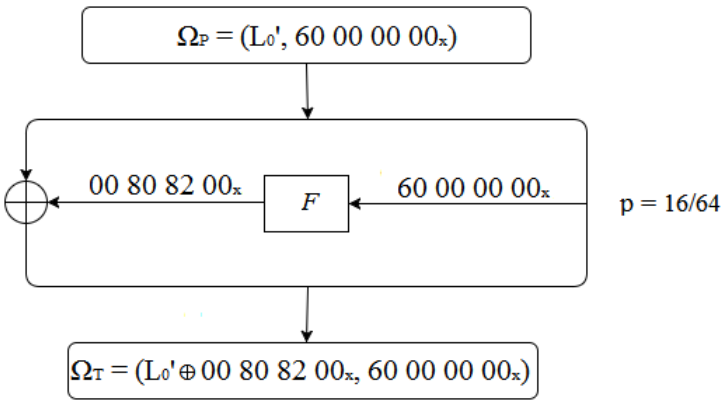
Slika 1.1: 1 - rundna karakteristika iz Primjera **??**

Taj primjer opisuje jedinu 1-rundnu karakteristiku sa vjerojatnošću većom od 0.25. Ta karakteristika je vrlo korisna i primjenjiva u bilo kojem kriptosustavu sličnom DES-u.

Primjer 1.3.3. *1-rundna karakteristika sa vjerojatnošću p = 14/64, za proizvoljan* L'_0*:*

$$R'_0 = 60000000_x$$

$$L'_1 = R'_0 = 60000000_x,\ R'_1 = L'_0 \oplus 00808200_x$$

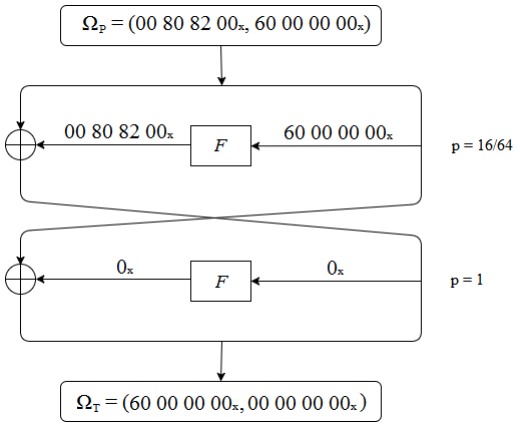


Slika 1.2: 1- rundna karakteristika iz Primjera **??**

Sljedeći primjer je 2-rundna karakteristika nastala konkatenacijom dviju 1-rundnih iz prethodna dva primjera:

Primjer 1.3.4. *2-rundna karakteristika sa vjerojatnošću p = 14/64:*

$$L'_0 = 00808200_x, R'_0 = 60000000_x$$
$$L'_1 = 60000000_x, R'_1 = 00808200 \oplus 60000000 = 00000000$$
$$L'_2 = 60000000_x, R'_2 = 60000000 \oplus 00000000 = 00000000_x$$



Slika 1.3: 2 - rundna karakteristika iz Primjera **??**

1.4 Pravi i krivi par

Primjetimo kako napadač ne može sigurno znati je li specifičan par sa zadanom razlikom zaista daje željenu razliku nakon svake runde (kao što je određeno karakteristikom). Kažemo da je pravi par svaki par koji zaista slijedi karakteristiku. Par koji odstupa od karakteristike u nekom trenutku zovemo krivi par.

Definicija 1.4.1. *Pravi par (en. right pair) u odnosu na n-rundnu karakteristiku* $\Omega = (\Omega_P, \Omega_\Lambda, \Omega_T)$ *i neovisan ključ K je par za koji vrijedi* $P' = \Omega_P$ *te za svaku rundu i prvih n runda enkripcije para koristeći neovisan ključ K, input XOR i-te runde jednak je* λ_I^i *a output XOR funkcije F jednak je* λ_O^i*. Svaki par koji nije pravi par u odnosu na karakteristiku i neovisan ključ naziva se krivi par (en. wrong pair) u odnosu na karakteristiku i neovisan ključ.*

Definicija 1.4.2. *n-rundna karakteristika* $\Omega^1 = (\Omega_P^1, \Omega_\Lambda^1, \Omega_T^1)$ *može se konkatenirati sa m-rundnom karakteristikom* $\Omega^2 = (\Omega_P^2, \Omega_\Lambda^2, \Omega_T^2)$ *ako je* Ω_T^1 *jednak* Ω_P^2 *kad mu se lijeva i desna polovica zamjene. Konkatenacija karakteristika* Ω^1 *i* Ω^2 *(ako mogu biti konkatenirane) je karakteristika* $\Omega = (\Omega_P^1, \Omega_\Lambda, \Omega_T^2)$*, gdje je* Ω_Λ *konkatenacija od* Ω_Λ^1 *i* Ω_Λ^2*.*

Sljedeće definicije bave se vjerojatnošću karakteristika:

Definicija 1.4.3. *Runda i karakteristike* Ω *ima vjerojatnost* p_i^Ω *ako vrijedi* $\lambda_I^i \rightarrow \lambda_I^i$ *sa vjerojatnošću* p_i^Ω *po funkciji F.*

Definicija 1.4.4. *n-rundna karakteristika* Ω *ima vjerojatnost* p^Ω *ako je* p^Ω *produkt vjerojatnosti svojih n runda:*

$$p^\Omega = \prod_{i=1}^{n} p_i^\Omega$$

Prema tome, vjerojatnost iz Primjera **??** mogli smo dobiti i kao produkt vjerojatnosti iz Primjera **??** i **??** jer je ta karakteristika nastala konkatenacijom karakteristika iz Primjera **??** i **??**

Općenito iz definicije *n*-rundne karakteristike i definicije vjerojatnosti *n*-rundne karakteristike, vjerojatnost karakteristike Ω koja je nastala konkatenacijom karakteristike Ω^1 s karakteristikom Ω^2 produkt je njihovih vjerojatnosti: $p^\Omega = p^{\Omega^1} \cdot p^{\Omega^2}$. Kao rezultat, svaka n-rundna karakteristika može se prikazati kao konkatenacija *n* 1-rundnih karakteristika sa vjerojatnošću koja je produkt 1-rundnih vjerojatnosti.

Za praktične svrhe, značajna vjerojatnost u odnosu na karakteristiku je vjerojatnost da par kojem je XOR otvorenog teksta jednak XOR-u otvorenog teksta karakteristike je pravi par koristeći fiksan ključ (onaj kojeg pokušavamo pronaći). Ta vjerojatnost nije konstantna za sve ključeve, no možemo pretpostaviti da za nasumično odabrani ključ dobro je aproksimirana vjerojatnošću karakteristike.

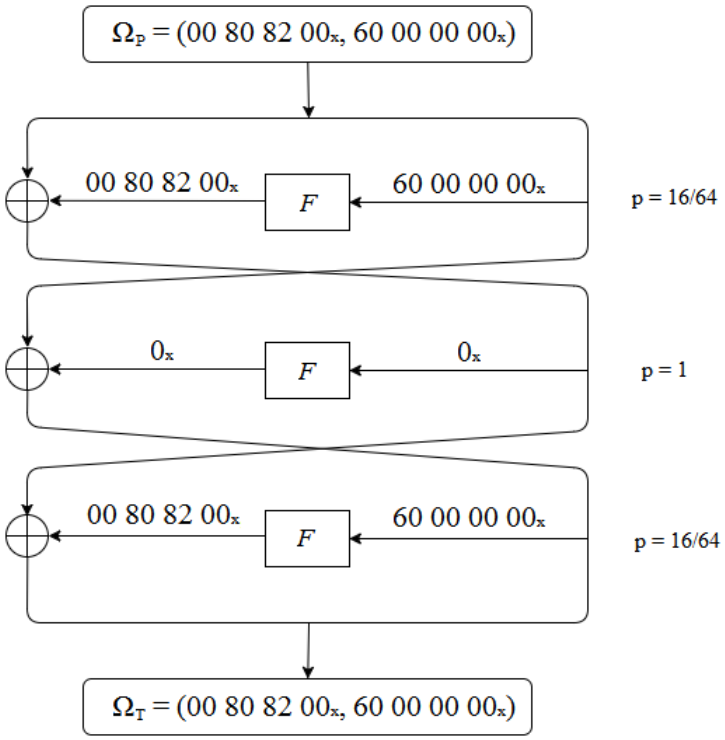
Primjer 1.4.5. *Konkatenacijom karakteristike iz Primjera* **??** *sa karakteristikom iz Primjera* **??** *dobije se 3-rundna karakteristika s vjerojatnošću* $p = \frac{16}{64}^2 = \frac{1}{20}$. *Definiciju joj vidimo na Slici* **??**.

Vidimo da kada se otvoreni tekstovi razlikuju na 5 određenih bitova, s vjerojatnošću od 0.05 postoji razlika od samo 3 bita u inputu 4. runde.
Struktura tri runde sa input XOR-om jednakim 0 u sredini vrlo je korisna i čini najbolju moguću vjerojatnost za 3-rundnu karakteristiku. To je zbog toga što nije moguće imati manje od dvije različite S-kutije, a koristili smo svaku s najboljom mogućom vjerojatnošću.

Među najkorisnijim karakteristikama su one koje se mogu iterirati.

Definicija 1.4.6. *Kažemo da je karakteristika* $\Omega = (\Omega_P, \Omega_\Lambda, \Omega_T)$ *iterativna karakteristika ako se može konkatenirati sama sa sobom.*

Možemo konkatenirati iterativnu karakteristiku samu na sebe proizvoljan broj puta i dobiti karakteristike s proizvoljnim brojem rundi. Prednost iterativnih karakteristika je



Slika 1.4: 3 - rundna karakteristika iz Primjera **??**

da pomoću njih možemo dobiti n-rundnu karakteristiku za bilo koji veliki n sa fiksnom stopom smanjenja vjerojatnosti za svaku dodatnu rundu, dok u ne-iterativnim karakteristikama stopa smanjenja obično se povećava zbog efekta lavine.

1.5 Omjer signala i buke

Statističko ponašanje većine karakteristika ne dopušta nam da tražimo presjek svih ključeva koje sugeriraju razni parovi. No, budući da su karakteristike po broju rundi kraće od kriptosustava, moguće je identificirati prave parove i prema tome je presjek predloženih ključeva obično prazan: krivi parovi ne izdvajaju nužno prave ključeve kao moguće vrijednosti. Međutim, znamo da prava vrijednost ključa mora rezultirati iz svih pravih parova koji se pojavljuju (približno) s vjerojatnosti karakteristike. Sve druge moguće vrijednosti ključeva su poprilično nasumično distribuirane. Očekivana XOR-vrijednost (koja obično nije prava vrijednost u paru) s poznatim parom šifrata može uzrokovati to da je bilo koji ključ jednako moguć, čak i krive vrijednosti ključa koje sugeriraju pravi parovi su dosta nasumične. Po-

sljedica toga je da pravi ključ ima vjerojatnost karakteristike (iz pravih parova) plus ostale nasumične vrijednosti koje se pojavljuju (iz krivih parova). Kako bismo pronašli ključ, moramo prebrojati koliko se svaki od sugeriranih ključeva pojavljuje. Pravi ključ vjerojatno je onaj koji se najčešće pojavljuje.

Svaka karakteristika dozvoljava nam da simultano tražimo određeni broj bitova u potključu posljednje runde kriptosustava (svi bitovi koji ulaze u neke fiksne S-kutije). Najkorisnije karakteristike one su koje imaju najveće vjerojatnosti i najveći mogući broj bitova potključeva takvih da im se broj pojavljivanja može prebrojati. Nije nužno prebrojavati veliki broj bitova potključa istodobno, no prednosti brojanja nad svim mogućim bitovima potključa istodobno su dobra identifikacija pravih vrijednosti ključa i mala količina potrebnih podataka. S druge strane, to zahtjeva veliku memoriju koja čini napad nepraktičnim. Možemo prebrojavati nad manjim brojem bitova potključa koji ulaze u manji broj S-kutija i koristiti ostale S-kutije samo kako bi identificirali i odbacili krive parove kod kojih input XOR u takvim S-kutijama ne može uzrokovati traženi output XOR. Budući da je oko 20% unosa u tablici distribucije razlika nemoguće, oko 20% krivih parova može biti odbačeno od strane svake S-kutije prije nego se krene s prebrojavanjem.

Sljedeća definicija daje nam alat za procjenu iskoristivosti sheme prebrojavanja utemeljene na karakteristikama.

Definicija 1.5.1. *Omjer između broja pravih parova i prosječnog broja krivih potključeva u shemi prebrojavanja zove se omjer signala i buke sheme prebrojavanja i označava se sa* S/N.

Kako bi pronašli pravi ključ pomoću sheme prebrojavanja, trebamo karakteristiku s velikom vjerojatnosti i dovoljno parova šifrata da imamo garanciju da postoji nekoliko pravih parova. Primjerice za karakteristiku s vjerojatnosti $\frac{1}{10000}$ trebamo nekoliko desetaka tisuća parova. Broj parova koji trebamo ovisi o vjerojatnosti p, broju k simultanih bitova ključa nad kojima možemo prebrojavati, prosječan broj α po analiziranom paru (bez krivih parova koji se mogu odbaciti prije prebrojavanja), i omjer β analiziranih parova od svih parova. Ako tražimo k bitova ključa, tada brojimo koliko puta se pojavljuje 2^k mogućih vrijednosti ključa u 2^k brojača. Brojači sadrže prosječno $\frac{m\cdot\alpha\cdot\beta}{2^k}$ brojeva gdje je m broj stvorenih parova ($m \cdot \beta$ je očekivani broj analiziranih parova). Prava vrijednost ključa prebroji se oko $m \cdot p$ puta od strane pravih parova plus dodatna nasumična prebrojavanja procijenjena ranije za sve moguće ključeve. Prema tome, omjer signala i buke u shemi prebrojavanja je:

$$S/N = \frac{m \cdot p}{m \cdot \alpha \cdot \beta / 2^k} = \frac{2^k \cdot p}{\alpha \cdot \beta}.$$

U praksi je jednostavnije izračunati prosječan broj prebrojanih ključeva po paru ($\alpha \cdot \beta$) nego odvojene vrijednosti od α i β.

Posljedica te formule je da je omjer signala i buke neovisan o broju parova koji se koriste u shemi prebrojavanja. Također, različite sheme prebrojavanja temeljene na istoj karakteristici ali s različitim brojevima bitova potključa imaju različite omjere buke i signala.

Obično se broj parova potrebnih za prebrojavanje veže s brojem potrebnih pravih parova. Broj potrebnih pravih parova uglavnom ovisi o omjeru signala i buke. Kada je taj omjer dovoljno velik, tek nekoliko pojavljivanja pravih parova potrebno je za jedinstvenu identifikaciju prave vrijednosti bitova potključa. Eksperimentalno se utvrdilo da kada je omjer signala i buke oko 1-2, dovoljno je oko 20-40 pojava pravih parova. Kada je omjer puno manji, identifikacija prave vrijednosti traži nerazumno velik broj parova.

Primjenjivost diferencijalnog kriptoanalitičkog napada određuje se uspoređivanjem broja enkripcija potrebnih za napad s veličinom prostora ključeva i veličinom prostora otvorenih tekstova. Ako je broj enkripcija veći od veličine prostora ključeva, očekivano vrijeme enkripcije odabranih otvorenih tekstova veće je od vremena potrebnog za iscrpnu potragu za ključem. Ako je broj enkripcija veći od prostora otvorenih tekstova, napad nije izvediv.

Poglavlje 2

Kriptoanaliza DES-a

U ovom poglavlju obrađujemo napade na razne oblike DES-a. Na početku podsjećamo se o samom algoritmu za šifriranje, zatim opisujemo kriptoanalizu DES-a reduciranog na 4, 8 i s proizvoljnim brojem rundi.

2.1 Opis DES-a

Data Encryption Standard (DES) je algoritam za enkripciju koji je bio korišten kao standardni algoritam u SAD-u od 1976. do 2002. godine. DES je blokovni kriptosustav: šifrira otvoreni tekst fiksne duljine (64 bitova) koristeći ključ duljine 56 bitova i stvara šifrat iste duljine.
Njegov rad odvija se u 3 koraka:

1. Inicijalna permutacija
   Otvoreni tekst x permutira se pomoću fiksne inicijalne permutacije IP i tako se dobije x_0. Zatim se x_o zapiše u obliku $x_0 = L_0R_0$. L_0 je niz koji sadrži prva (lijeva) 32 bita, a R_0 sadrži 32 zadnja (desna) bita od x_0.

2. Šifriranje
   Računamo L_i i R_i, $1 \leq i \leq 16$ na sljedeći način:

   $$L_i = R_{i-1}$$
   $$R_i = L_{i-1} \oplus F(R_{i-1}, k_i)$$

   gdje $\oplus$ označava operaciju "ekskluzivno ili" (XOR), $K_1, K_2, ..., K_{16}$ su nizovi bitova duljine 48 koji se dobivaju kao permutacije nekih bitova iz ključa K. Funkciju F definiramo kasnije.

3. Inverzna permutacija
   Primjenom inverzne permutacije IP^{-1} na $R_{16}L_{16}$ dobivamo šifrat y.

Funkcija F ima dva argumenta: niz bitova A duljine 32 i niz bitova J duljine 48, Rezultat je niz bitova duljine 32. Računa se na sljedeći način:

1. A se proširi do niza duljine 48 pomoću fiksne funkcije proširenja E. E(A) se dobije permutacijom 32 bita od A s tim da se 16 bitova od A ponavlja dvaput.

2. Računa se $E(A) \oplus J = B$, te se B zapiše kao konkatenacija od osam 6-bitnih nizova:

$$B = B_1B_2B_3B_4B_5B_6B_7B_8$$

3. Supstitucijske ili S-kutije su fiksne 4 x 16 matrice čiji su elementi brojevi između 0 i 15. DES koristi osam S-kutija. U ovom koraku računamo:

$$S(B) = S_1(B_1)S_2(B_2)S_3(B_3)S_4(B_4)S_5(B_5)S_6(B_6)S_7(B_7)S_8(B_8)$$

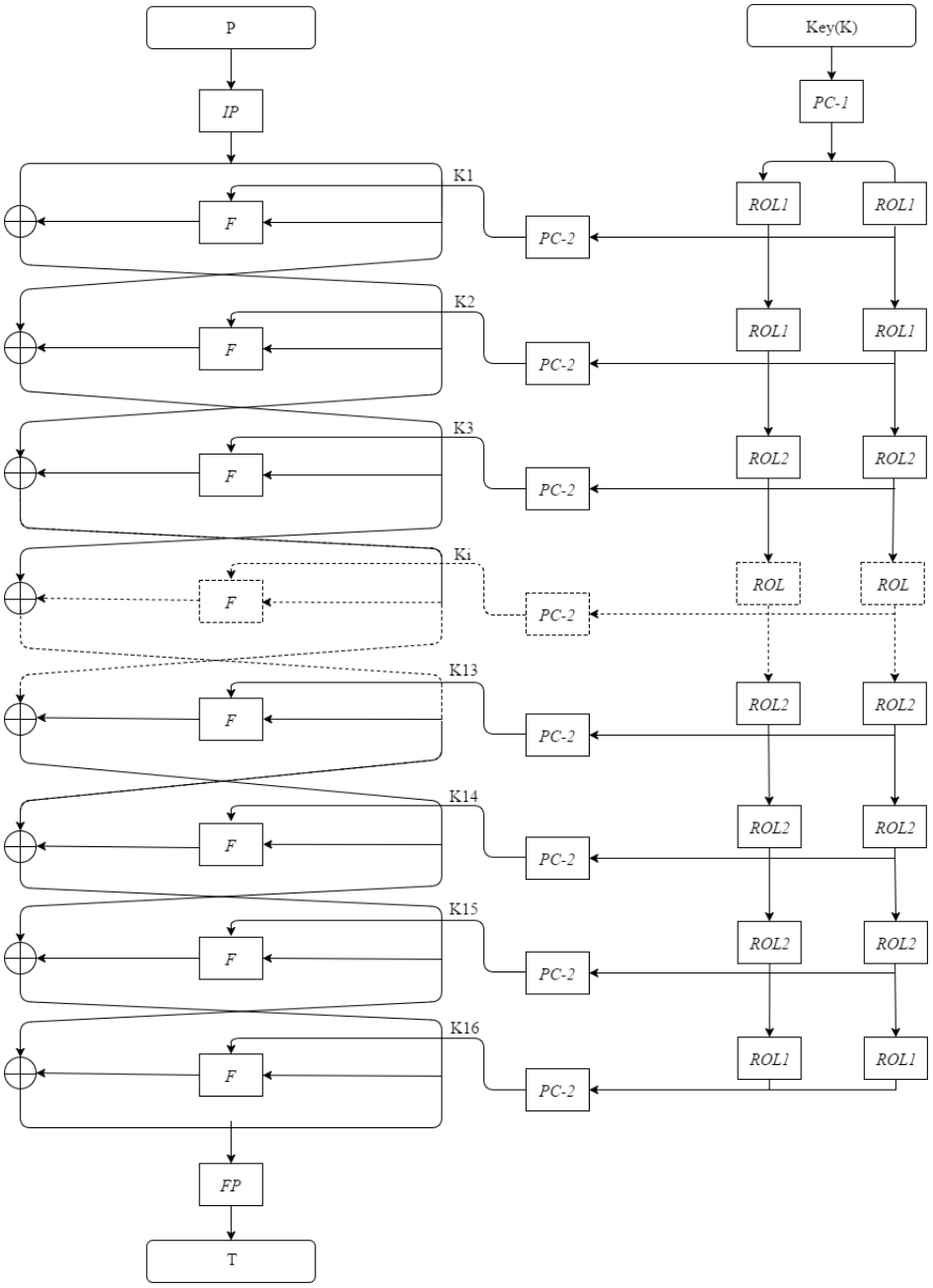
   Ako je $B_j = b_1b_2b_3b_4b_5b_6$ dani niz bitova duljine 6, $S_j(B_j)$ odredi se tako da dva bita b_1b_6 određuju binarni zapis retka r od S-kutije S_j a četiri bita $b_2b_3b_4b_5$ određuju binarni zapis stupca c od S_j. Uz te oznake, $S_j(B_j) = S_j(r, c)$ zapisano kao binarni broj duljine 4.

4. Na kraju, niz $C = C_1C_2C_3C_4C_5C_6C_7C_8$ permutira se pomoću fiksne završne permutacije P. Tako dobivamo $P(C)$, što je jednako $F(A, J)$

Ključ K sastoji se od 64 bita, od kojih je 56 ključ a preostalih 8 služe za testiranje pariteta. Bitovi na pozicijama 8,16,...,64 definirani su tako da svaki bajt (niz od 8 bitova) sadrži neparan broj jedinica. Te bitove ignoriramo prilikom računanja tablice ključeva.
Primjer takvog niza bitova:
1111000**1**11100000**0**10101011011101**0**11111110000000**1**11111011111111**0**.
Podebljani bitovi predstavljaju paritetne bitove.

Tablica ključeva $K_1, K_2, ..., K_{16}$ računa se iz ključa K na sljedeći način:

1. Kod danog 64-bitnog ključa K ignoriramo paritetne bitove te permutiramo preostale bitove pomoću fiksne permutacije $PC1$. Zapišemo $PC1(K) = C_0D_0$, gdje je C_0 lijevih 28 bitova a D_0 desnih 28 bitova od $PC1(K)$.



Slika 2.1: Skica algoritma DES i algoritma dodjeljivanja ključa

2. Računamo:

$$C_i = LS_i(C_{i-1})$$
$$D_i = LS_i(D_{i-1})$$
$$K_i = PC2(C_iD_i),\ i = 1, 2, \ldots, 16.$$

Gdje LS_i predstavlja ciklički pomak ulijevo za 1 ili 2 pozicije, ovisno od i: za neparne i-eve pomak za jednu poziciju, a inače je pomak za dvije pozicije. $PC2$ je još jedna fiksna permutacija.

Kriptoanaliza DES-a

Diferencijalna kriptoanaliza prvi je objavljeni napad koji može razbiti puni 16-rundni DES u složenosti manjoj od 2^{55}. Ovaj napad može se primjeniti na razne varijante DES-a i drugih sličnih supstitucijskih/permutacijskih kriptosustava. Ta metoda bila je poznata konstruktorima DES-a već 1974. godine, te su je imali u vidu kod dizajna S-kutija i permutacije P. Algoritam za DES koji smo opisali je originalni, sa 16 rundi. U sljedećim poglavljima demonstriramo kriptoanalizu DES-a reduciranog na 4, 8, 16 i proizvoljnim brojem rundi (manjim od 16). Najprije dajemo još dva rezultata koja vežu pojmove iz prvog poglavlja sa DES-om.

Lema 2.1.1. *U DES-u, ako vrijedi $X \to Y$ po funkciji F, s vjerojatnosti p tada svaki fiksan input-par Z, Z^* takav da $Z' = Z \oplus Z^* = X$ uzrokuje da je output XOR funkcije F jednak Y u istom dijelu p mogućih vrijednosti podključeva.*

U ostalim iterativnim kriptosustavima ova lema nužno ne vrijedi. Međutim, pretpostavljamo da je razlomak po vrijednosti vrlo blizu p, što je obično slučaj.

Pronalaženje bitova ključa koji ulaze u S-kutije može se proširiti na pronalaženje potključeva koji ulaze u funkciju F.

Metoda se sastoji od sljedećih koraka:

1. Odabir prikladnog XOR-a otvorenog teksta
2. Stvaranje prikladnog broja parova otvorenog teksta s odabranim XOR-om otvorenog teksta. Zatim se ti parovi šifriraju i zadržavaju se samo rezultirajući parovi šifrata.
3. Za svaki par izvodi se očekivani output XOR iz što više S-kutija u zadnjoj rundi iz XOR-a otvorenog teksta i para šifrata. (Input par zadnje runde je poznat jer se pojavljuje kao dio para šifrata)

4. Za svaku moguću vrijednost ključa, izbroji se broj parova koji rezultiraju s očekivanim output XOR-om koristeći taj ključ u posljednjoj rundi

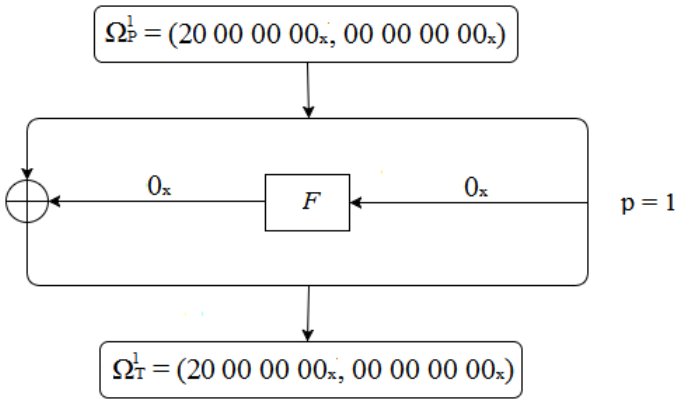
5. Tražena vrijednost ključa je (nadamo se, jedinstvena) vrijednost ključa koju sugeriraju svi parovi.

Teorem 2.1.2. *Formalno definirana vjerojatnost karakteristike* $\Omega = (\Omega_P, \Omega_\Lambda, \Omega_T)$ *je stvarna vjerojatnost da je proizvoljan fiksiran otvoreni tekst koji zadovoljava* $P' = \Omega_P$ *pravi par kada se koriste nasumični nezavisni ključevi.*

Dokaz. Vjerojatnost da je bilo koji fiksan par otvorenih tekstova koji zadovoljava $P' = \Omega_P$ pravi par je vjerojatnost da u svim rundama i: $\lambda_I^i \rightarrow \lambda_O^i$. Vjerojatnost u svakoj rundi neovisna je od svog točnog inputa (što slijedi iz Leme **??**)i neovisna od akcija prethodnih runda, budući da neovisni ključevi u potpunosti izmješaju (randomize) inpute u svaku S-kutiju što ostavlja samo XOR vrijednost fiksnu. Prema tome, vjerojatnost da je par pravi par produkt je vjerojatnosti $\lambda_I^i \rightarrow \lambda_O^i$ što je upravo definicija vjerojatnosti karakteristike. □

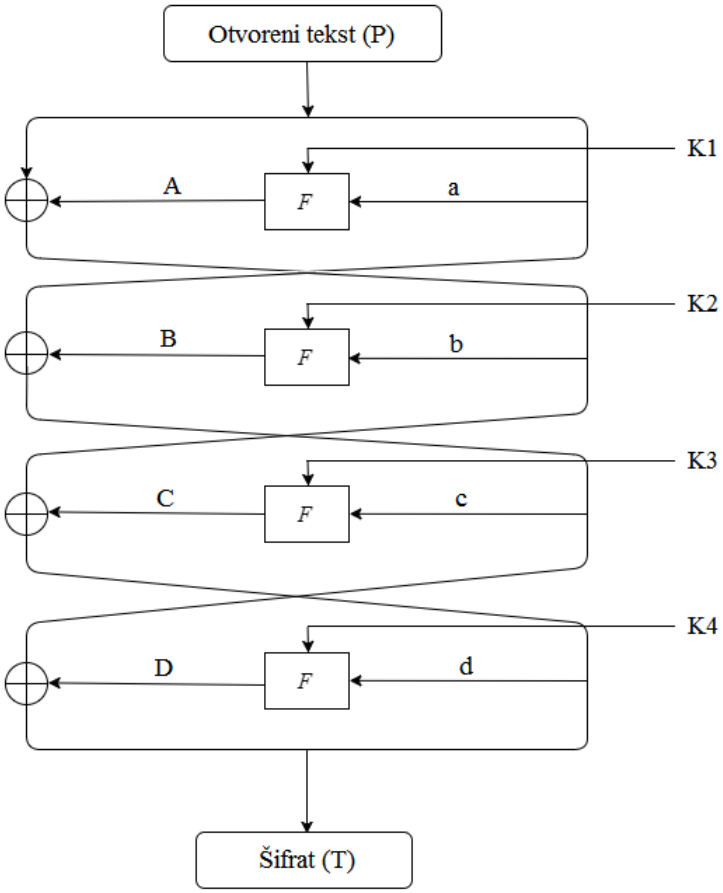
2.2 DES sa 4 runde

Kriptoanaliza ovog slučaja prilično je jednostavna budući da koristi karakteristiku sa vjerojatnošću 1 opisanu na slici 2.1, koja je specijalni slučaj karakteristike opisane u Primjeru **??**:



Slika 2.2:

Promatramo par šifrata P i P^* takvih da je $P' = P \oplus P^*$.
U prvoj rundi karakteristika ima $a' = 0 \rightarrow A' = 0$ s vjerojatnošću 1. Razlika u jednom



Slika 2.3: DES reduciran na četiri runde

bitu između dva otvorena teksta počinje igrati ulogu u drugoj rundi u $S1$. Naime, kako se inputi od S1 razlikuju samo u jednom bitu, outputi se moraju razlikovati u barem dva bita (to je poznato svojstvo S-kutija). Obično takva dva bita ulaze u tri S-kutije u trećoj rundi ($a' = a' \oplus B' = B'$), gdje se javlja razlika od po jedan bit u svakom od inputa S-kutija. Prema tome, oko 6 (dva bita po svakoj od tri S-kutije) output bitova razlikuje se u trećoj rundi. Izvrši se XOR operacija tih bitova s poznatom razlikom inputa od $S1$ u drugoj rundi $d' = b' \oplus C'$, čime dobivamo razliku od oko 7 bitova kod inputa četvrte runde, te oko 11 bitova nakon E ekspanzije. Kao posljedica toga, vrlo je izgledno da se inputi svih S-kutija razlikuju kod četvrte runde. Čak i ako se inputi S-kutija ne razlikuju u jednom paru bitova, mogu se razlikovati u nekom drugom paru pa je točna vrijednost od d' obično različita za svaki par.

28 output XOR-eva od S2, ... , S8 u B' mora biti nula, budući da su njihovi input XOR-evi nula. Iz slike **??** vidimo da vrijedi: $T'_L = D \oplus c = D' \oplus B' \oplus a'$, pritom T'_L označava lijevu polovicu od T'. Dakle vrijednost od D' može se izračunati pomoću a', B' i T'_L:

$$D' = a' \oplus B' \oplus T'_L \tag{2.1}$$

Kada su poznati parovi šifrata T i T^*, znamo i da su d i d^* njihove desne polovice, jer je $d = T_R$. Kako su a', T'_L i 28 bitova od B' poznati, također je poznato i odgovarajućih 28 bitova od D' po jednakosti 2.1. Tih 28 bitova upravo su output XOR-i od S-kutija $S2, \ldots, S8$. Drugim riječima, sada znamo vrijednosti od S_{Ed}, S^*_{Ed} i S'_{Od} od sedam S-kutija u četvrtoj rundi.

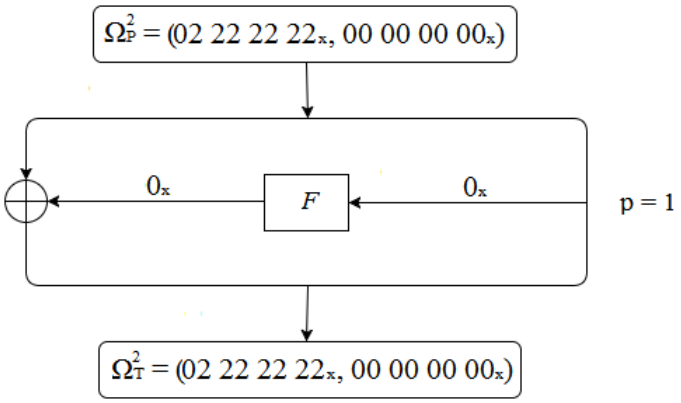
Uz četiri enkriptirana para, koristimo zaseban postupak računanja za svaku od sedam S-kutija u četvrtoj rundi. Imamo 64 moguće vrijednosti od S_{Kd} jer se radi o nizu šest bitova. Isprobavamo sve moguće vrijednosti od S_{Kd} i provjeravamo vrijedi li:

$$S(S_{Ed} \oplus S_{Kd}) \oplus S(S_{Ed^*} \oplus S_{Kd}) = S'_{Od}.$$

Za svaki ključ prebrojimo za koliko parova naš test uspijeva. Prava vrijednost ključa biti će ona vrijednost koju sugeriraju svi parovi budući da koristimo karakteristiku s vjerojatnošću 1, za koju su svi parovi pravi parovi. Ostale 63 vrijednosti ključa mogu se pojaviti u nekim parovima. Nije vjerojatno da se vrijednost pojavljuje u baš svim parovima, koji imaju različite vrijednosti od S'_E i S'_o. U rijetkim slučajevima kada je više od jedne vrijednosti ključa sugerirani od svih parova, nekoliko dodatnih parova može se testirati ili se analiza ostalih dijelova ključa može izvesti u paraleli za sve preostale kandidate.

Do sada smo pronašli $7 \cdot 6 = 42$ bitova potključa u posljednjoj rundi ($K4$). Ukoliko su potključevi izračunati pomoću algoritma dodjeljivanja ključeva od DES-a, imamo 42 stvarna bita ključa od postojećih 56 bitova, pa nam nedostaje 14 bitova. Sada možemo isprobavati svih 2^{14} mogućnosti za bitove koji nedostaju i dekriptirati šifrate koristeći te ključeve. Pravi ključ mora zadovoljavati poznatu vrijednost XOR-a otvorenih tekstova, no ostalih $2^{14} - 1$ vrijednosti imaju samo vjerojatnost od 2^{-64} da zadovolje ovaj uvijet.

Može li se DES ojačati tako da svi potključevi Ki budu nezavisni ili barem da se dobiju na kompliciraniji način iz duljeg ključa K? Naš napad može se izvesti čak i u tom slučaju. Kako bismo pronašli 6 preostalih bitova od K4 i otkrili K3, koristimo jednu drugu vrijednost XOR-a otvorenih tekstova sa sljedećom karakteristikom Ω^2:



Slika 2.4:

Vrijednost od $S1'_{Eb}$ je nula, pa je $S1'_{Ob} = 0$. Kao iznad, pronalazimo $S1'_{Od}$ pomoću jednadžbe 2.1, te na sličan način pronađemo odgovarajućih 6 dijelova ključa $S1_{Kd}$.
Sada znamo čitav potključ $K4$ četvrte runde. Pomoću $K4$ djelomično dekriptiramo sve šifrate tako što "poništavamo" efekt zadnje runde. Ostanu nam šifrati trorundnog kriptosustava. U tom kriptosustavu, možemo ponovo koristiti karakteristiku Ω^2 kako bi izračunali potključ treće runde ($K3$). Ulazi u treću rundu c i $c*$ poznati su kao polovice šifrata trorundnog kriptosustava. Input XOR c' lako izračunamo. Output XOR C' izračunamo kao $C' = b' \oplus d'$, gdje je b' lijeva polovica od Ω_P^2, a d'je desna polovica XOR-a šifrata (T'_R). Metoda prebrojavanja koristi se prilikom brojanja ponavljanja mogućih ključeva od svih osam S-kutija u trećoj rundi. Vrijednosti koje su izračunate za sve parove su najvjerojatnije prave vrijednosti ključa. Kao rezultat, pronađe se čitav $K3$ s velikom vjerojatnosti.

XOR-ovi otvorenih tekstova tih karakteristika nisu dovoljni za pronalazak jedinstvene vrijednosti za $K2$ budući da su vrijednosti od S'_{Eb} konstantne za sve parove i prema tome prave vrijednosti ključa ne mogu se razlikovati od alternativnih vrijednosti dobivenih XOR-om sa S'_{Eb}. Iako možemo pronaći te dvije vjerojatnosti za svaku S-kutiju (tj. 2^8 mogućnosti za $K2$), ne možemo koristiti te karakteristike kako bi pronašli $K1$ jer su oba XOR-a otvorenih tekstova desne polovice su nula pa su a' i A' također nula (bez obzira na potključ, ako vrijedi $a' = 0$, tada su sve moguće vrijednosti od $K1$ jednako vjerojatne).
Kako bismo rješili ovaj problem moramo koristiti dodatne XOR-eve otvorenih tekstova koji imaju ne-nula input XOR-eve za sve S-kutije prve runde. Uz to želimo da možemo razlikovati vrijednosti ključeva svih S-kutija pa uzimamo dva XOR-a otvorenih tekstova: P'_3 i P'_4. Ti XOR-i mogu biti proizvoljno odabrani pod sljedećim uvijetima:

- $S'_{Ea} \neq 0$ za sve S-kutije koristeći ili P'_3 ili P'_4

- Vrijednost od S'_{Ea} izvedena iz P'_3 razlikuje se od vrijednosti S'_{Ea} dobivene iz P'_4 za svaku S-kutiju.

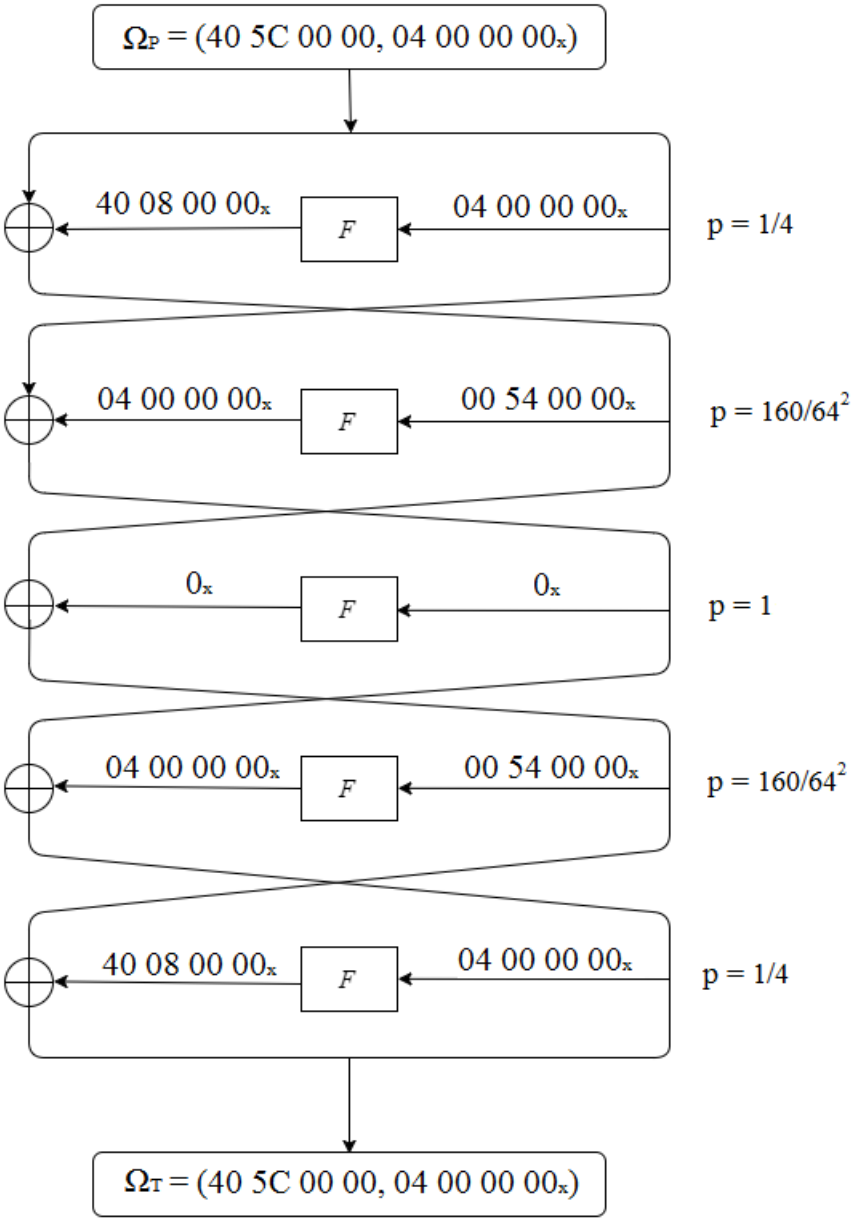
b i $b*$ poznati su iz dekripcije treće runde i B' je poznat iz: $B' = a' \oplus c' = P'_R \oplus c'$. Pomoću metode prebrojavanja pronađemo $K2$. Ovaj put moramo koristiti prikladne vrijednosti P'_R za svaki par. Sada su $a, a*$ i a' poznati pomoću dekripcije druge runde i A' je poznat preko $A' = P'_L \oplus b'$. Metodom prebrojavanja pronađemo i $K1$. Koristeći $K1, K2, K3$ i $K4$ možemo dešifrirati originalne šifrate kako bi dobili odgovarajuće otvorene tekstove i tada potvrditi njihove vrijednosti XOR-eva otvorenih tekstova. Ako pronađemo samo jednu mogućnost za sve potključeve, verifikacija mora uspjeti. S druge strane, ako je pronađeno više mogućnosti, tada je izgledno da će samo jedna od njih biti uspješno verificirana pa se pravi ključ i u tom slučaju može identificirati.

Za ovaj napad obično se koristi 16 odabranih otvorenih tekstova. Tih 16 otvorenih tekstova sadrži 8 parova karakteristike Ω^1, 8 parova karakteristike Ω^2, 4 para sa XOR-om otvorenog teksta P'_3 i 4 para s XOR-om otvorenih tekstova P'_4. Kako bi izbjegli povećanje količine potrebnih podataka, koristimo dva okteta koja daju četiri para od kojih svaki od tri XOR-a otvorenih tekstova. Verzija napada s poznatim otvorenim tekstom traži oko $2^{33.5}$ poznatih otvorenih tekstova.

2.3 DES sa 8 rundi

DES reduciran na osam rundi može se razbiti koristeći oko 25 000 parova šifrata za koje je XOR otvorenih tekstova P' jednak 40 5C 00 00 04 00 00 00_x. Ta metoda razotkrije 30 bitova od $K8$. 18 bitova može se pronaći sličnim manipulacijama s parovima, a 8 preostalih bitova može se pronaći iscrpnom analizom.

Sada koristimo karakteristiku sa slike 2.4. Ona ima vjerojatnost $\frac{1}{10485 \cdot 76}$. Input XOR u šestoj rundi pravog para je $f' = 405C0000_x$. Posljedica toga je da za pet S-kutija $S'_{Ef} = S'_{Lf} = 0$ i $S'_{Of} = 0$. Kod pravih parova, pet S-kutija S2, S5, S6, S7 i S8 zadovoljavaju $S'_{Ef} = S'_{If} = 0$ i $S'_{Of} = 0$. Pomoću forumule $H' = T'_L \oplus g' = T'_L \oplus e' \oplus F'$ možemo izračunati output XOR-eve odgovarajućih S-kutija u osmoj rundi. Input osme runde poznat je iz šifrata.
Dakle, možemo koristiti metodu prebrojavanja da bi pronašli 30 bitova potključa koji ulaze u pet S-kutija u osmoj rundi. Omjer signala i buke kod ovog prebrojavanja je: $S/N = \frac{2^{30}}{4^5 10845 \cdot 76} = 100$.


ΩP = (40 5C 00 00, 04 00 00 00x)
40 08 00 00x
F
04 00 00 00x
p = 1/4
04 00 00 00x
F
00 54 00 00x
p = 160/64^2
0x
F
0x
p = 1
04 00 00 00x
F
00 54 00 00x
p = 160/64^2
40 08 00 00x
F
04 00 00 00x
p = 1/4
ΩT = (40 5C 00 00, 04 00 00 00x)

Slika 2.5:

Prebrojavanje na 30 bitova potključa zahtjeva veliku memoriju. Usprkos tome, možemo smanjiti količinu potrebne memorije prebrojavajući nad manje bitova potključa koji ulaze u manje S-kutija. Preostale S-kutije mogu se koristiti za identifikaciju nekih od krivih parova (za koje $S'_{Eh} \nrightarrow S'_{Oh}$).
Oko 20% ulaza u tablici distribucija razlika su nemogući, pa svaka preostala S-kutija odbacuje 20% krivih parova. Prebrojavanje nad 24 bitova ključa sada ima $S/N = \frac{2^{24}}{4^40.8 \cdot 10845 \cdot 76} \approx 7.8$ i prebrojavanje nad 18 bitova ključa ima $S/N = \frac{2^{18}}{4^3 \cdot 0.8^2 \cdot 10845 \cdot 76} \approx 0.6$

Kod shema prebrojavanja koje broje nad reduciranim brojem bitova možemo proizvoljno odabrati reducirani skup S-kutija. U tom specifičnom slučaju možemo odabrati reducirani skup na način koji maksimizira vjerojatnost karakteristike te omjer signala i buke koristeći blago modificiranu karakteristiku koja ignorira output bitove koji se svakako ne prebrojavaju. Modificirana karakteristika slična je originalnoj osim što je u petoj rundi samo jedan bit od $S2'_{Oe}$ fiksiran a sve kombinacije ostala tri bita su dozvoljene:

$$e' = 04\ 00\ 00\ 00_x \rightarrow E' = P(0W\ 00\ 00\ 00_x) = X0\ 0Y\ Z0\ 00_x,$$

gdje $W \in \{0, 1, 2, 3, 8, 9, A, B\}$, $X \in \{0, 4\}$, $Y \in \{0, 8\}$ i $Z \in \{0, 4\}$. Prema tome, u šestoj rundi : $f' = X0\ 5V\ Z0\ 00_X$, gdje je $V = Y \oplus 4$.
Jedina moguća kombinacija u kojoj je $Z = 0$ je $04\ 00\ 00\ 00_x \rightarrow 40\ 08\ 00\ 00_x$ koja ima vjerojatnost $\frac{16}{64}$. Sve ostale kombinacije (za koje je $Z = 4$) imaju ukupnu vjerojatnost $\frac{20}{64}$. Ne možemo računati na bitove potključa $S5_{Kh}$ no još uvijek se preporučuje provjeriti vjerojatnost od $S5'_{Kh} \rightarrow S5'_{Oh}$ koju zadovoljava 80% parova.
Prema tome, vjerojatnost od $e' \rightarrow E'$ je $\frac{16}{64} + 0.8\frac{20}{64} = \frac{32}{64} = \frac{1}{2}$. Vjerojatnost petrundne modificirane karakteristike je $\frac{16 \cdot 10 \cdot 16}{64^3} \cdot \frac{16 \dot{1} 0 \cdot 32}{64^3} \approx \frac{1}{5243}$. Omjer signala i buke sheme koja prebrojava nad 24 bita potključa koja ulaze u S2, S6, S7 i S8 je: $S/N = \frac{2^{24}}{4^40.8 \cdot 5243} \approx 15.6$. S takvim omjerom obično je moguće identificirati ispravne bitove potključa sa samo pet pravih parova. Prema tome, napad koristi ukupnu količinu od 25000 parova. Verzija ovog napada s poznatim otvorenim tekstom treba oko 2^40 poznatih otvorenih tekstova. Omjer signala i buke sheme koja prebrojava nad 18 bita potključa koja ulaze u tri S-kutije od S2, S6, S7 i S8 je: $S/N = \frac{2^{18}}{4^3 \dot{0}.8^2 \cdot 5243} \approx 1.2$. Ta shema prebrojavanja treba 150000 parova i ima u prosjeku oko 24 prebrojavanja za svaki pogrešan ključ i oko 53 prebrojavanja za pravu vrijednost ključa ($53 = 24 + \frac{150000}{5243} = 24 + 29$).

Ova metoda kriptoanalize može se sažeti na sljedeći način:

1. Postaviti niz od $2^{18} = 256K$ jednobajtnih (bajt - niz od 8 bitova) brojača koji je inicijaliziran nulama. Niz odgovara 2^{18} vrijednosti od 18 bitova ključa K8 koji ulaze u S6, S7 i S8.

2. Izvrši predobradu mogućih vrijednosti od S_1 koji zadovoljavaju $S'_1 \rightarrow S'_O$ za osam S-kutija u tablicu. Ta tablica se koristi za ubrzavanje algoritma.

3. Za svaki par šifrata:

   a) Pretpostavi $h' = T'_R, H' = T'_L$ i $h = T_R$. Izračunaj $S'_{Eh} = S'_{Ih}$ i S'_{Oh} za S2, S5, S6, S7 i $S8$ pomoću h' i H'. Izračunaj S_{Eh} za S6, S7 i S8 pomoću h.

   b) Za svaku od S-kutija S2, S5, S6, S7 i S8 provjeri vrijedi li $S'_{Ih} \nrightarrow S'_{Oh}$. Ako $S'_{Ih} \nrightarrow S'_{Oh}$ za bar jednu od S-kutija tada odbaci taj par kao krivi par.

   c) Za svaku od S-kutija S6, S7 i S8: dohvati iz pretprocesirane tablice svih vrijednosti od S_{Ih} koje su moguće za $S'_{Ih} \rightarrow S'_{Oh}$. Za svaku moguću vrijednost izračunaj $S_{Kh} = S_{Ih} \oplus S_{Eh}$. Uvećaj za jedan brojače koji odgovaraju svim mogućim 18-bitnim konkatenacijama od jedne 6-bitne vrijednosti sugerirane za $S6_{Kh}$, jedne 6-bitne vrijednosti sugerirane za $S7_{Kh}$ i jedne 6-bitne vrijednosti sugerirane za $S8_{Kh}$.

4. Pronađi element niza koji sadrži najveći broj. Indeks elementa najvjerojatnije je prava vrijednost od $S6_{Kh}$, $S7_{Kh}$ i $S8_{Kh}$ što je upravo vrijednost od 18 bitova (od 31. do 48. bita) od $K8$.

Kako bismo pronašli preostale bitove, filtriramo sve parove i ostavimo samo parove sa očekivanom vrijednosti od S'_O koristeći poznate vrijednosti od h i poznate bitove od $K8$ koji ulaze u $S6$, $S7$ i $S8$. Očekivani broj preostalih parova je 53. Taj broj je dovoljno mali da si možemo priuštiti analizu svakog para puno detaljnije nego u prvoj fazi i tako razotkriti više bitova ključa.

Ostali bitovi koji su nam nepoznati su 12 bitova od $K8$ koji odgovaraju S2 i S5. Koristimo sličnu metodu prebrojavanja (iskorištavanje poboljšanog omjera signala i buke stvorenog većom koncentracijom pravih parova) i onda filtriramo više paro va. Krivi par se ne odbacuje niti ovim filterom ni njegovim prethodnikom s vjerojatnosti 2^{-20} i time su skoro svi preostali parovi pravi parovi.

Koristeći poznate bitove potključa $K8$ možemo izračunati vrijednosti 20 bitova od svakog od H i $H*$ za svaki par i time 20 bitova od svakog od g i $g*$ (preko formule $g = T_L \oplus H$). Tablica 2.1 pokazuje ovisnost bitova od g i bitova potključa $K7$ u sedmoj rundi na poznatim

oznaka S-kutije	g bitovi S_{Eg}	bitovi ključa S_{Kg}
S1	+4++++	3+..4+
S2	++3++1	13433
S3	+14+++	+1+41+
S4	++++31	11..1+
S5	31++4+	+++.++
S6	4+13+	+.+.++
S7	3+4+++	+++.++
S8	++31+4	+++++

Tablica 2.1:

i nepoznatim bitovima potključa $K8$ u osmoj rundi. Znamenke 1,3 i 4 znače da oni ovise o vrijednosti nepoznatih bitova ključa koji ulaze u odgovarajuću S-kutiju u osmoj rundi. + znači da ovisi samo o poznatim bitovima od K8. Osam bitova ključa koji se uopće ne koriste u $K8$ označeni su točkom.

Očekivana vrijednost od G' poznata je iz formule $G' = f' \oplus h'$. Sada možemo tražiti 18 bitova koji nedostaju iz $K8$ iscrpnom pretragom 2^{18} vjerojatnosti za svaki par. Tako pronađemo vrijednosti od $H, H*, g, g*$ i 40 bitova od $K7$. Za svaki par provjeravamo ima li očekivanu vrijednost od G'. Za desni dio od tih 18-bitnih ključeva očekivani G' postiže se kod gotovo svih filtriranih parova. Sve ostale vrijednosti zadovoljavaju očekivanu vrijednost od G' samo za nekoliko parova (obično 2-3 para dok prava vrijednost vrijedi za 15 parova). Kako bi brže računali, primarno tražimo 12 bitova ključa koji ulaze u $S1$ i $S4$ u osmoj rundi. Oni su dovoljni za računanje $S3'_{Og}$ kao što se vidi iz Tablice 2.1. Kad pronađemo tih 12 bitova, možemo pronaći i preostalih šest. Ovim se završava računanje 48 bitova od $K8$. Samo osam bitova ključa još uvijek nedostaje i oni se mogu pronaći pretragom 256 slučajeva, koristeći jedan par šifrata i provjerom je li vrijednost XOR-a otvorenog teksta u skladu s očekivanom.

Kako bi optimizirali ovaj proces možemo filtrirati parove čim su stvoreni i odbaciti sve krive parove. Na takav način u slučaju da prebrajamo nad 24 bita, 25000 parova se reducira na oko 7500 parova. Međutim, kad se prebrajanje izvršava nad 18 bitova 150000 parova se reducira na 50000 parova. U tom slučaju uvodimo još jedan kriterij kojim odbacujemo većinu krivih parova dok ostavljamo skoro sve prave parove. Ovaj kriterij temelji se na pažljivo odabranoj težinskoj funkciji i odbacuje svaki par čija je težina niža od određene granice. Nadalje, taj kriterij produljenje je filtriranja krivih parova koji se izdvajaju (gdje je granica zapravo nula) i temelji se na ideji da pravi par obično sugerira više mogućih vrijednosti ključa nego krivi par. Težinska funkcija produkt je broja mogućih ključeva u

$S2_I$	$S2_I^*$	$S2_O$	$S2_O*$
123456	123456	1234	1234
000010	001010	0001	1011
000110	001110	1110	0100
010001	011001	1100	0110
010101	011101	0001	1011
100000	101000	0000	1010
100010	101010	1110	0100
100100	101100	0111	1101
100110	101110	1011	0001

Tablica 2.2: Moguće instance od $08_r \rightarrow A_r$ po $S2$ (u binarnom sustavu)

svakoj od pet S-kutija (broj u odgovarajućem unosu u tablici distribucija razlika). Granica se odabere tako da maksimizira broj odbačenih parova, dok ostavlja što više pravih parova. Eksperimentalno se pokazalo da je najbolja vrijednost granice 8192, koja odbacuje oko 97% krivih parova i ostavlja skoro sve prave parove. Ovo smanjuje broj parova koje zapravo analiziramo sa 150000 na oko 7500 sa odgovarajućom redukcijom u vremenu izvršavanja napada.

Implementirani algoritam pronalazi ključ u manje od dvije minute na osobnom računalu koristeći 150000 parova sa stopom uspjeha od 95%. Korištenjem 250000 parova, stopa uspjeha penje se na skoro 100%. Program koristi 460Kb memorije, od koje se većina koristi za niz prebrojavanja (jedan bajt dovoljan je svaki brojač budući da je maksimalan broj oko 53 pa prema tome ukupna veličina niza je 2^{18} bajtova), i pri izračunu tablice. Program koji prebrojava koristeći 2^{24} ćelije memorije pronalazi ključ koristeći samo 25000 parova. Napad s poznatim otvorenim tekstom koristi oko 2^{40} otvorenih tekstova.

Poboljšana vjerojatnost karakteristike

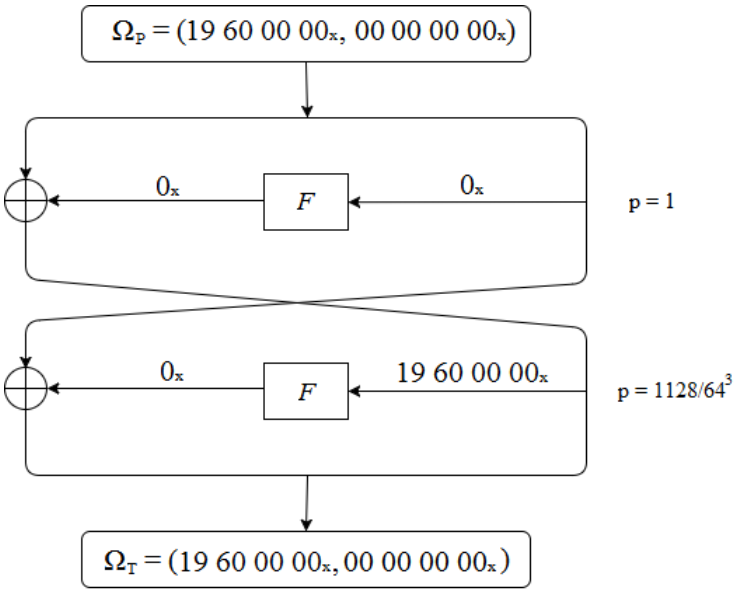
Osim statističkog ponašanja karakteristike, možemo koristiti i moguće vrijednosti pojedinih input i output bitova S-kutija. Promotrimo prvu rundu karakteristike. Imamo $08_x \rightarrow A_x$ po S2 s vjerojatnosti $\frac{16}{64}$. Tablica 2.2 opisuje moguće vrijednosti inputa i outputa.
Primjećujemo da su input bitovi broj 2 i 6 uvijek jednaki. Osim toga, za 12 od 16 input vrijednosti oni su oba 0, a za 4 od 16 input vrijednosti oba bita jednaka su 1. Ako poznajemo XOR bitova ključa koji ulaze u ta dva bita od $S2$ u prvoj rundi (bitovi 57 i 42 od ključa), možemo koristiti samo otvorene tekstove za koje odgovarajući bitovi (5. i 9. bit) imaju istu XOR vrijednost. što uzrokuje da su 2. i 6. bit jednaki. Ostali parovi otvorenog teksta ne mogu zadovoljiti karakteristiku. Vjerojatnost karakteristike i omjer signala i buke su tada

dvostruko bolji i dozvoljavaju nam korištenje upola manje parova.

Ukoliko znamo vrijednosti oba bita ključa, možemo odabrati dva bita u otvorenom tekstu tako da su vrijednosti bitova koje ulaze u $S2$ obe nula. U tom slučaju vjerojatnost od $S2$ postaje $\frac{12}{64}$ umjesto $\frac{16}{64}$. Tako dobijemo faktor od 3 u vjerojatnosti i omjeru signala i buke. Veći omjer signala i buke dopušta nam da koristimo manje od $\frac{1}{3}$ parova koji su nam prvotno trebali. Faktor od četiri može se lako dobiti pomoću karakteristike koja vrijedi i za sve inpute kod kojih bit broj 1 ima vrijednost 1 i oba bita broj 2 i 6 imaju vrijednost 0.

2.4 DES s proizvoljnim brojem rundi

Sljedeća dvorundna iterativna karakteristika s vjerojatnosti od oko $\frac{1}{234}$ može se koristiti za kriptoanalizu verzija DES-a s proizvoljnim brojem rundi.



Slika 2.6:

Iterativnom konkatenacijom iterativne karakteristike same sa sobom i s jednorundnom karakteristikom s vjerojatnosti 1 (opisanom u Primjeru **??**) dobijemo karakteristiku s neparnim brojem rundi čije se vjerojatnosti nalaze u Tablici 2.3. Te karakteristike imaju $\Omega_P = \Omega_T = (19\ 60\ 00\ 00_x, 00\ 00\ 00\ 00) = (\psi, 0)$. U sljedećoj rundi (ako se doda u karakteristiku) input XOR funkcije F je ψ i pet njenih S-kutija zadovoljava $S'_E = 0$.
Postoji još jedna vrijednost $\psi' = 1B\ 60\ 00\ 00_x$ za koju iterativna karakteristika ima istu

broj rundi	vjerojatnost
3	$2^{-79} \approx \frac{1}{234}$
5	$2^{-15.7} \approx \frac{1}{55000}$
7	$2^{-23.6}$
9	$2^{-31.5}$
11	$2^{-39.4}$
13	$2^{-47.2}$
15	$2^{-55.1}$

Tablica 2.3: Vjerojatnost iterativne karakteristike u ovisnosti o broju rundi

vjerojatnost. Osim nje, postoji još nekoliko dodatnih vrijednosti za koje su vjerojatnosti još manje. Najbolja od njih je $\psi'' = 00\,19\,60\,00_x$ koja ima vjerojatnost $\frac{1}{256}$. Produljenje ove iterativne karakteristike na 15 rundi ima vjerojatnost 2^{-56}.

Postoji nekoliko mogućih tipova napada, ovisno o broju dodatnih rundi u kriptosustavu koje nisu pokrivene karakteristikom samom po sebi. Napad na DES reduciran na osam rundi koji smo opisali koristi petrundnu karakteristiku sa tri dodatne runde koje nisu pokrivene karakteristikom. Ova vrsta napada zove se 3R-napad.
Druge vrste napada su 2R-napad s dvije dodatne runde u 1R-napad s jednom dodatnom rundom. Također je moguć i 0R-napad, ali on se može reducirati na 1R-napad s boljom vjerojatnosti i istim omjerom signala i buke. Za fiksan kriptosustav preporuča se korištenje najkraće moguće karakteristike zbog njene bolje vjerojatnosti. Ukratko: 3R-napad preporuča se prije 2R-napada, a oba se preporučuju prije 1R-napada.

3R-napadi

Kod 3-R napada prebrojavanje se može vršiti nad bitovima potključa posljednje runde koja ulazi u S-kutije čije odgovarajuće S-kutije u rundi koja slijedi posljednju rundu karakteristike imaju input XOR-ove nula. Napadi na DES reduciran na 4 i 8 rundi opisani u prethodnim sekcijama ovog su tipa.

Kod DES-a reduciranog na osam rudni prvih 30 bitova potključa mogu se pronaći koristeći iterativnu karakteristiku sa pet rundi (čija je vjerojatnost oko $\frac{1}{55000}$) pomoću napada sličnom onom opisanom u sekciji 2.3. Koristeći niz duljine 2^{24} imamo $S/N = \frac{2^{24}}{4^4 \cdot 0.8 \cdot 55000} = 1.5$, te trebamo oko 2^{20} parova. Koristeći niz duljine 2^{30} imamo $S/N = \frac{2^{30}}{4^5 \cdot 55000} = 19$. Oko 67% (što je $1 - 0.8^5$) krivih parova možemo odbaciti prije napada.

Za DES reduciran na deset ili više rundi, omjer signala i buke 3R-napada postaje premali, pa se 3R napadi na takvim varijantama ne preporučuju.

Poglavlje 3

Kriptoanaliza drugih kriptosustava

3.1 Diferencijalna kriptoanaliza FEAL-a

FEAL je simetričan kriptografski algoritam koji je sugeriran kao alternativa DES-u, a prilagođen za efikasnu implementaciju na mikroprocesorima. Prvu verziju algoritma, koja je imala 4 runde i 64-bitni ključ, objavili su 1987. Akihiro Shimizu i Shoji Miyaguchi. Već 1988. Bert den Boer opisuje napad koji traži 100–10000 odabranih otvorenih tekstova, a Sean Murphy 1990. pronalazi poboljšanje koje traži samo 20 odabranih otvorenih tekstova. Kako bi uklonili nedostatke udvostručuju se runde i nastaje FEAL-8 (Shimizu i Muyaguchi, 1988). Međutim, i to se pokazalo nedovoljnim pa 1989. Biham i Shamir opisuju diferencijalni napad na FEAL-8 kojeg opisujemo u ovom poglavlju.
Struktura FEAL-a slična je onoj od DES-a, uz modificiranu F funkciju, te različitu inicijalnu i završnu permutaciju i algoritam dodjeljivanja ključeva. Kod F funkcije permutacija P i S-kutije zamijenjene su s rotacijama bitova i operacijama zbrajanja. Te operacije mogu se efikasno implementirati na mikroprocesorima.

S-kutije S_0 i S_1 FEAL-a uzimaju dva input bita i računaju jedan input bit na sljedeći način: $S_i(x, y) = ROL2(x + y + i \ (mod\ 256))$, gdje $ROL2$ rotira svoj ulazni byte dva bita nalijevo. Na primjer, $ROL2(11001010) = 00101011$.
Općenito, $ROLn(X)$ označava rotaciju od X za n bitova ulijevo a $RORn(X)$ označava rotaciju od X za n bitova udesno.
Funkcija F iz 32-bitnog inputa i 16-bitnog potključa računa 32-bitni output primjenom S-kutija četiri puta sekvencijalno. Inicijalna i finalna permutacija zamijenjene su inicijalnom i završnom transformacijom kod kojih se čitav 64-bitni niz XOR-a s 64-bitnim potključevima i desna polovica niza se XOR-a s lijevom polovicom.
Na slici 3.1 možemo vidjeti izgled osmorundnog FEAL-a i njegovu F funkciju. Algoritam dodjeljivanja ključa zamijenjen je s algoritmom procesiranja ključa pomoću kojeg

potključevi ovise o ključu na kompleksniji način. Algoritam procesiranja ključa i njegove F_k funkcije opisane su na slici 3.2.

Budući da svaka S-kutija ima 16 input bitova i samo osam output bitova ne preporuča se izravno korištenje tablice distribucija razlika. Umjesto toga, u prvom stadiju analize koristimo združenu distribucijsku tablicu od dvije srednje S-kutije funkcije F. Ta kombinacija ima 16 input i 16 output bitova i tablica ima mnogo zanimljivih ulaza. Postoje dva ulaza s vjerojatnošću 1: $00\ 00_x \rightarrow 00\ 00_x$ i $80\ 80_x \rightarrow 00\ 02_x$. Otprilike 98% unosa je nemoguće. Prosječna vrijednost svih ulaza je 1, no prosječna vrijednost unosa različitih od nule je oko 50.

S-kutije također imaju sljedeća svojstva u odnosu na parove: Neka je $Z = S_i(X, Y)$. Ako $X' = 80_x$ i $Y' = 80_x$ tada $Z' = 00_x$. Ako $X' = 80_x$ i $Y' = 00_x$ tada $Z' = 02_x$. Za bilo koje input XOR-ove X' i Y' S-kutija, najvjerojatniji output XOR je $Z' = ROL2(X' \oplus Y')$. On se dobije s vjerojatnošću od oko $\frac{1}{2^{\#(X'|Y')}}$, gdje # označava broj bitova postavljenih na 1 u nižih 7 bitova bytea X, a — je operator logičko ili. Kako je svaki bit različit u parovima (u X i X^*, Y i Y^*), to uzrokuje prenošenje drugacije znamenke s vjerojatnošću od 0.5.

Input F funkcije u posljednjoj rundi funkcija je šifrata XOR-anog s dodatnim potključem finalne tranformacije (kod DES-a ovisi samo o šifratu).
Postoji ekvivalentan opis FEAL-a kod kojeg se eliminira XOR s potključevima u finalnoj transformaciji, te zamijeni 16-bitne potključeve XOR-ane s dva srednja bajta inputa F-funkcija u raznim rundama s 32-bitnim vrijednostima.

Definicija 3.1.1. *32-bitni potključevi ekvivalentnog opisa kod kojih je XOR s potključevima u finalnoj tranformaciji eliminiran nazivaju se stvarni potključevi. Stvarni potključ koji zamjenjuje potključ K_i označava se s AK_i. 16-bitne kombinacije XOR-a $mx(AKi) = (AKi_0 \oplus AKi_1, AKi_2 \oplus AKi_3)$ zovu se 16-bitni stvarni potključevi.*
Stvarni potključ posljednje runde kriptosustava zove se posljednji stvarni potključ.

Stvarni potključevi kod parnih $i + 1$ rundi su:

$$AKi = Kcd \oplus Kef \oplus am(Ki)$$

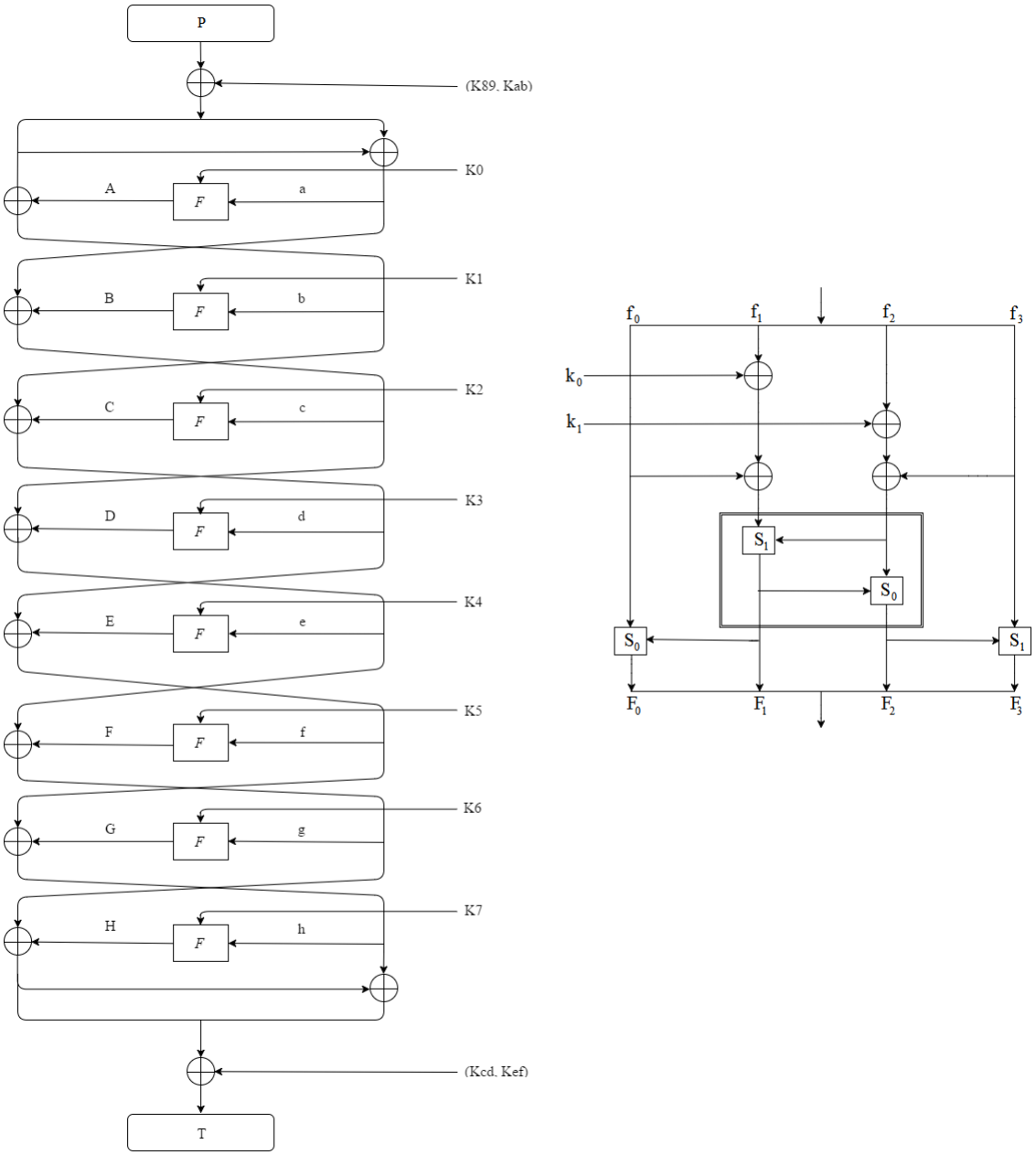
Stvarni potključevi kod neparnih $i + 1$ rundi su:

$$AKi = Kcd \oplus am(Ki)$$

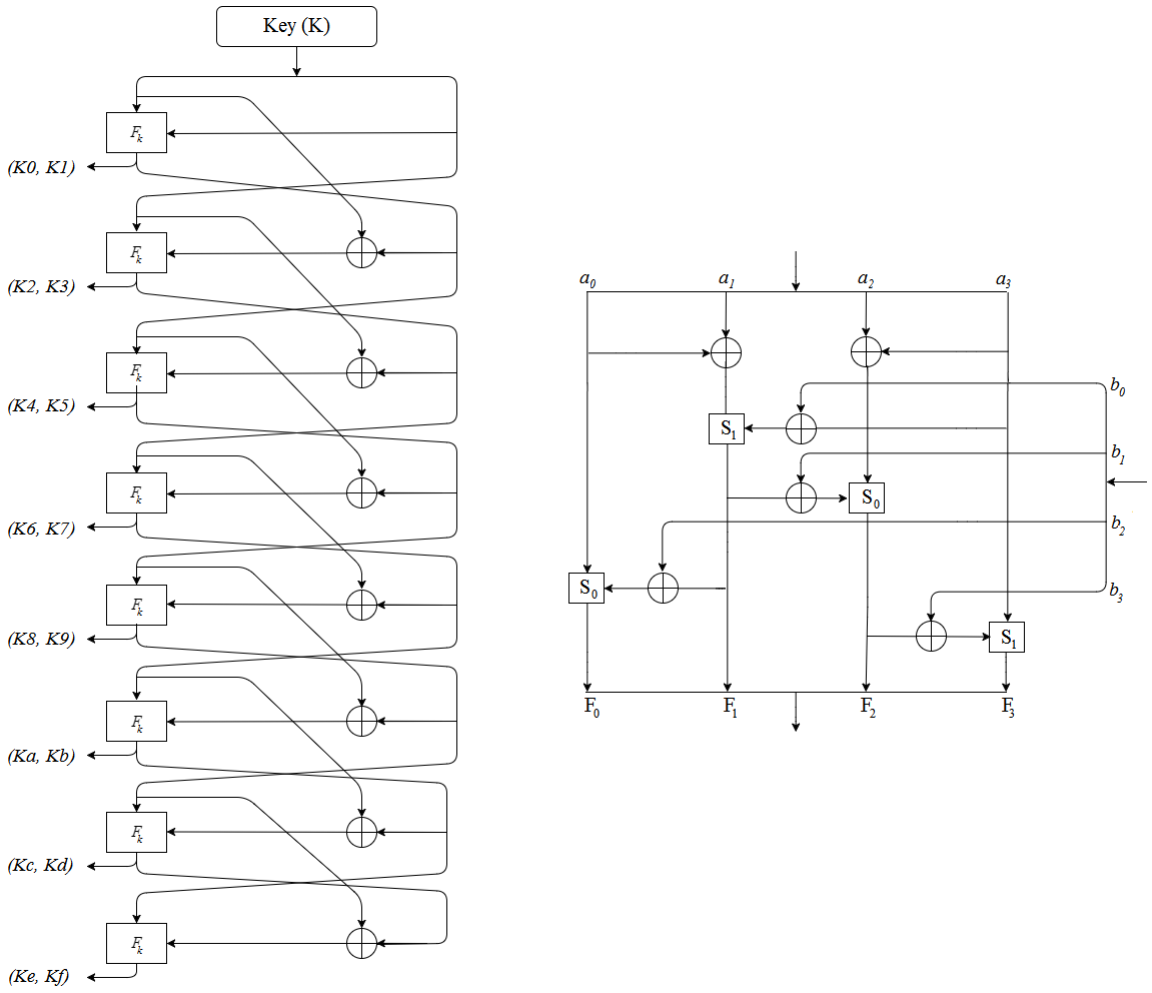
Stvarni potključevi kod inicijalnih transformacija su:

$$AK89 = K89 \oplus Kcd \oplus Kef$$

$$AKab = Kab \oplus Kef$$

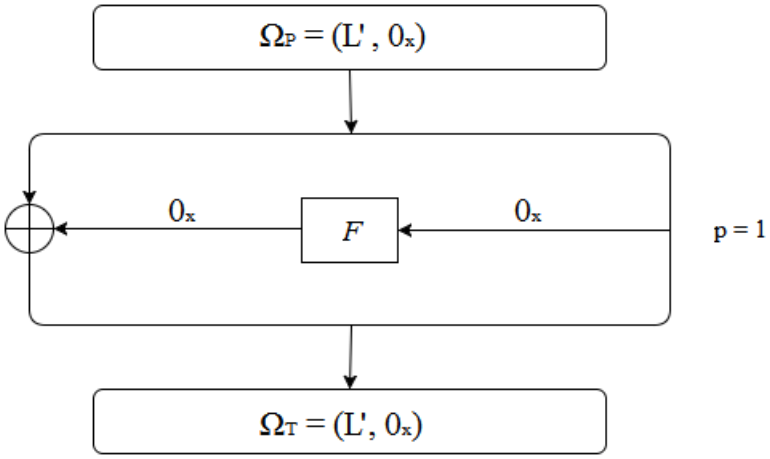


Slika 3.1: Algoritam FEAL-8 i njegova F-funkcija



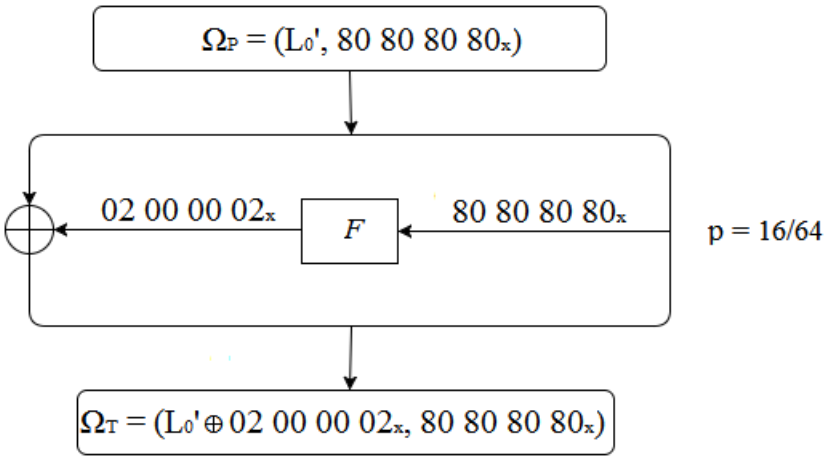
Slika 3.2: Algoritam obrađivanja ključa FEAL-a i njegova F_k funkcija

Stvarni potključevi finalne transformacije su eliminirani pa su njihove vrijednosti nula. Naš napad pronalazi stvarne potključeve a ne potključeve budući da pronalazi XOR-eve šifrata i interne vrijednosti u F-funkciji.
Najjednostavnija 1-rundna karakteristika s vjerojatnošću 1, za bilo koji L' je:



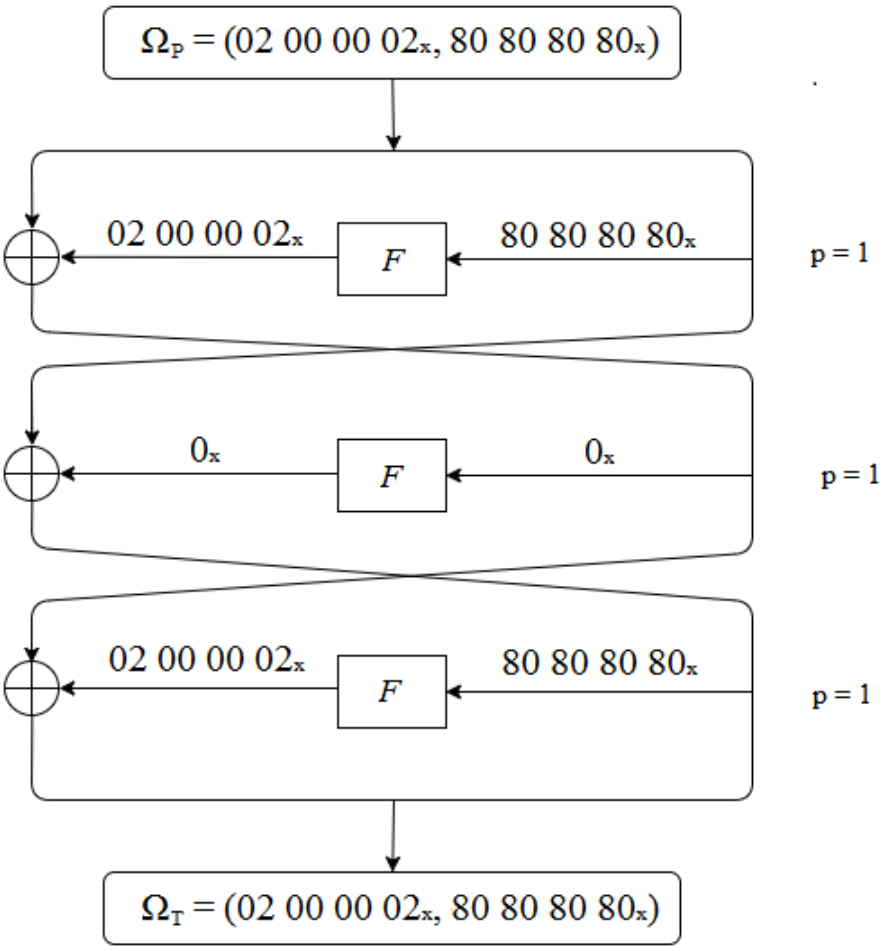
Slika 3.3:

Ta karakteristika slična je 1-rundnoj karakteristici s vjerojatnošću 1 DES-a.
Za razliku od DES-a, FEAL ima tri druge 1-rundne karakteristike s vjerojatnošću 1. Tipičan primjer je:



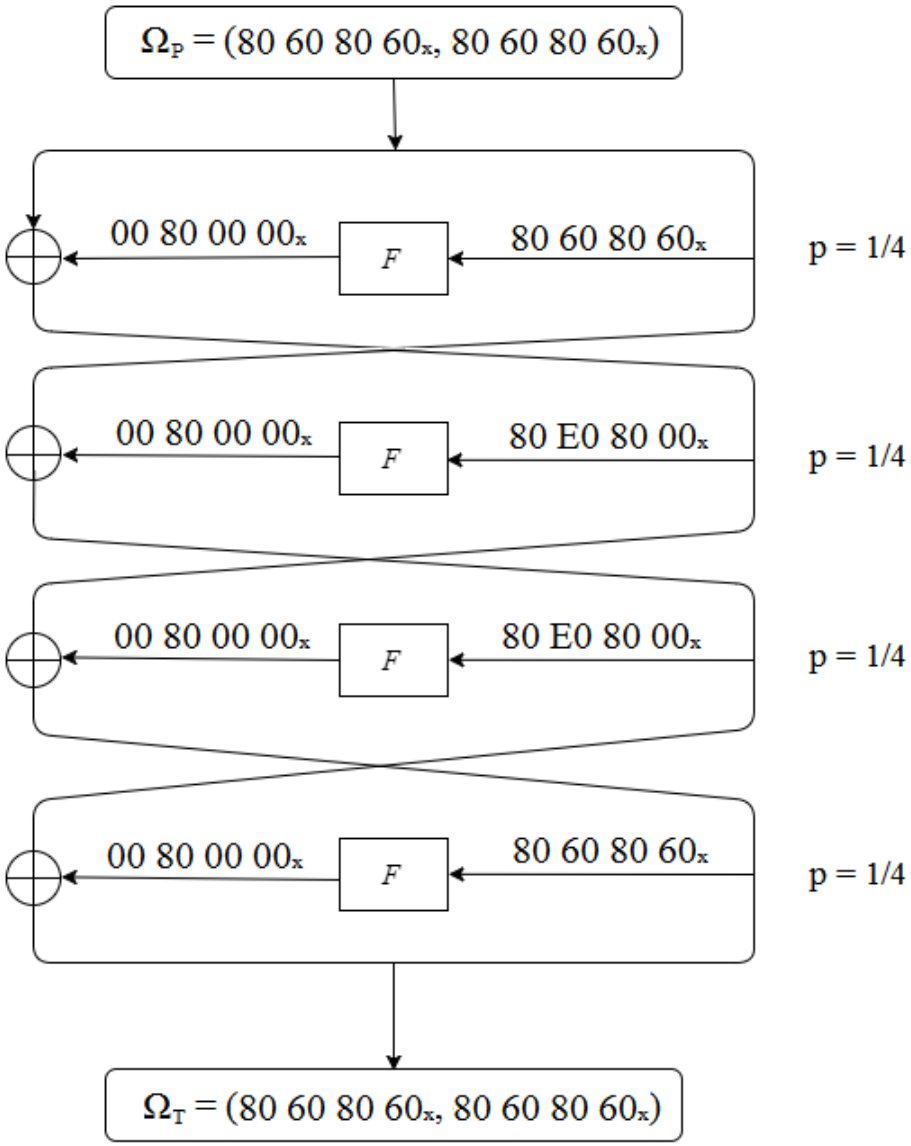
Slika 3.4:

Iz karakteristika sa Slike 3.3 i Slike 3.5 može se izvesti i sljedeća:



Slika 3.5:

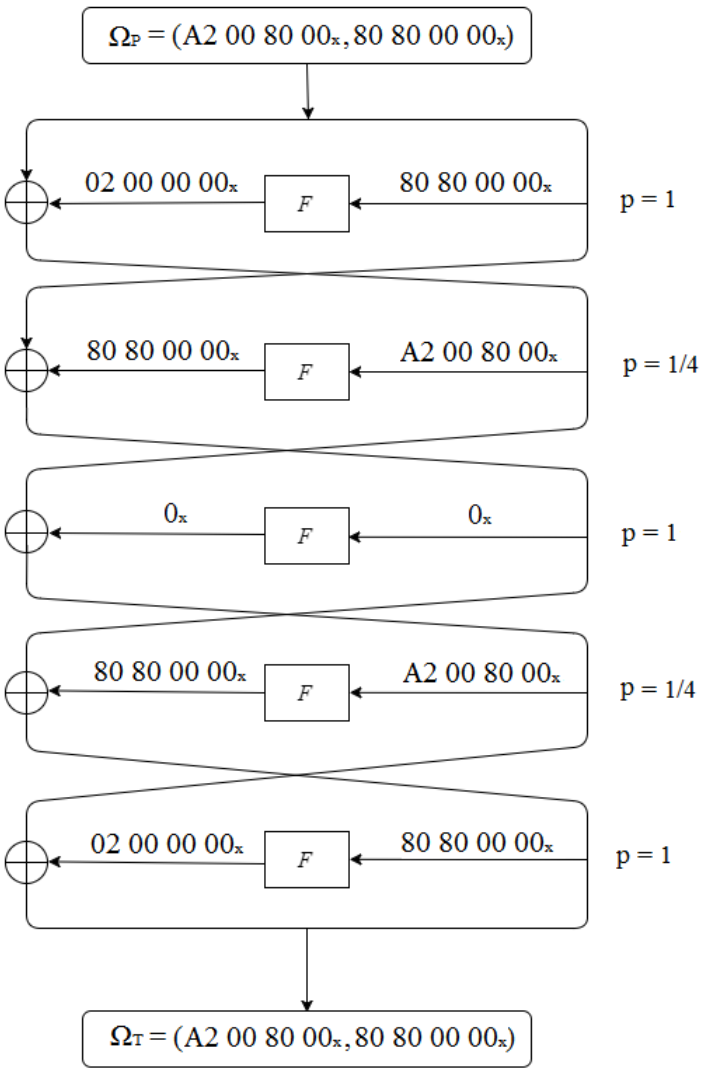
Među iterativnim karakteristikama FEAL-a ne može se pronaći ona kod koje input F-funkcije različit od nule može uzrokovati da je output XOR nula (kako je F funkcija reverzibilna), ali postoje druge vrste iterativnih karakteristika. Sljedeća iterativna karakteristika ima vjerojatnost $\frac{1}{4}$ u svakoj rundi:


$\Omega_P = (80\ 60\ 80\ 60_x, 80\ 60\ 80\ 60_x)$
00 80 00 00x
F
80 60 80 60x
p = 1/4
00 80 00 00x
F
80 E0 80 00x
p = 1/4
00 80 00 00x
F
80 E0 80 00x
p = 1/4
00 80 00 00x
F
80 60 80 60x
p = 1/4
$\Omega_T = (80\ 60\ 80\ 60_x, 80\ 60\ 80\ 60_x)$

Slika 3.6:

3.2 Kriptoanaliza za FEAL-8

Diferencijalna kriptoanaliza odabranim otvorenim tekstom traži oko 128 parova šifrata čiji su odgovarajući XOR-i otvorenih tekstova $P' = A2\ 00\ 80\ 00\ 22\ 80\ 80\ 00_x$. On se može konvertirati u napad poznatim otvorenim tekstom koji koristi oko 2^{36} poznatih otvorenih tekstova i njima odgovarajućih šifrata. Ovaj XOR otvorenih tekstova koristi sljedeću 5-rundnu karakteristiku čija je vjerojatnost $\frac{1}{16}$:



Slika 3.7:

Četiri kraće karakteristike mogu se izvesti iz prvih nekoliko rundi te pet-rundne karakteristike. Svaka karakteristika ima različit broj rundi, no svaka od njih ima istu vrijednost ω_P. Jednorundna karakteristika koja se dobije iz prve rundne pet-rundne karakteristike ima vjerojatnost 1. Dvorundna i trorundna karakteristika koje se dobiju iz prve dvije i tri runde imaju vjerojatnost $\frac{1}{4}$. Četverorundna karakteristika ima vjerojatnost $\frac{1}{16}$.

Redukcija FEAL-8 na sedam rundi

Neka su T i T^* šifrati pravog para. Tada možemo izračunati:

$$\begin{aligned} h &= T_L \oplus T_R \\ h' &= T'_L \oplus T'_R \\ g' &= d' \oplus E' \oplus h' = A2\ 00\ 80\ 00_x \oplus T'_L \oplus T'_R \\ F' \oplus G' &= T'_L \oplus e' = T'_L \oplus 80\ 80\ 00\ 00_x \end{aligned}$$

Prije nego počnemo primjenom metode prebrojavanja pronalaziti 16-bitni posljednji stvarni potključ, filtriranjem možemo odbaciti oko $\frac{15}{16}$ krivih parova. Kako je operacija aditivnosti linearna u svom najmanje važnom bitu i kako $h' \rightarrow H'$, vrijedi sljedeće:

$$\begin{aligned} h'_{0,0} &= H'_{0,2} \oplus H'_{1,0} \\ h'_{3,0} &= H'_{3,2} \oplus H'_{2,0} \\ h'_{2,0} &= H'_{2,2} \oplus H'_{1,0} \oplus h'_{3,0} \\ h'_{1,0} &= H'_{1,2} \oplus h'_{0,0} \oplus h'_{2,0} \oplus h'_{3,0} \end{aligned}$$

Slične jednadžbe vrijede i za $f' \rightarrow F'$. Kako su te jednadžbe linearne i vrijednost od $F' \oplus G'$ je poznata, možemo izračunati XOR ta četiri bita u f' i u h' : $f'_{i,0}, i \in \{0, ..., 3\}$. Kako su f' i h' poznati za pravi par, uspoređivanjem ta četiri bita s očekivanim vrijednostima možemo odbaciti oko $\frac{15}{16}$ krivih parova. Budući da se pravi parovi pojavljuju s karakteristikama s vjerojatnošću $\frac{1}{16}$, otprilike polovica preostalih parova su pravi parovi.

Zatim primjenjujemo specijalan oblik 3R-napada. Umjesto da tražimo nul-bitove u F', računajući odgovarajuće bitove u H' i isprobavamo sve moguće potključeve, ovdje radimo u drugom smjeru. Shema prebrojavanja broji broj parova kod kojih je moguća svaka vrijednost 16-bitnog posljednjeg pravog potključa $mx(AK7)$. Za svaku takvu vrijednost računamo $\hat{H}$ i $\hat{H}^*$ i dobivamo $\hat{F}^*$ jer je $F' \oplus H'$ poznat. Pritom oznaka $\hat{X}$ predstavlja 16-bitnu vrijednost dva srednja bajta (X_1, X_2) od proizvoljnog 32-bitnog niza X. Zatim provjeravamo može li f' uzrokovati izračunatu vrijednost od $\hat{F}^*$. Očekivani omjer signala i buke je:

$$S/N = \frac{2^{16} \cdot 2^{-4}}{0.02 \cdot \frac{1}{4}} \approx 2^{20}$$

Taj omjer je toliko velik da nam je obično potrebno samo osam pravih parova za napad, pa je ukupan broj parova koje moramo proučavati oko $8 \cdot 16 = 128$. Primjetimo da ne možemo razlikovati pravu vrijednost 16-bitnog pravog potključa i tu vrijednost XOR-anu s $80\,80_x$. Zbog toga dobivamo dvije mogućnosti za 16-bitni posljednji potključ.

Sada opisujemo shemu prebrojavanja za pronalazak stvarnog posljednjeg potključa. Za svaki par, od svih parova, računamo $\hat{H}$ i $\hat{H}^*$, te dobivamo $\hat{H}'$. Zatim računamo $\hat{g}' = \hat{T}'_L \oplus \hat{H}', \hat{F}' = \hat{e}' \oplus \hat{g}'$ i nekoliko ostalih bitova od g', te odbacujemo parove za koje ne možemo zaključiti da $g' \nrightarrow G'$ po F-funkciji koristeći bitove koje smo pronašli.

Sada isprobavamo 128 mogućnosti za najnižih sedam bitova od $AK7_0$. Za svaku vrijednost računamo H_0, H_0^*, H'_0 i $F'_0 = e'_0 \oplus H'_0 \oplus T'_{L0}$ i potvrditi da f'_0 (iz karakteristike) i F'_1 (iz $\hat{F}'$) mogu uzrokovati taj F'_0. Prebrojimo parove koji zadovoljavaju taj uvjet. Vrijednost od $AK7_0$ koje ima najviše vjerojatno je prava vrijednost. Budući da ne možemo razlikovati gornji bit vrijednosti, isprobavamo 128 mogućnosti (umjesto 256, kao što bi se očekivalo) i zatim isprobamo dvije moguće vrijednosti u sljedećim koracima sve dok ne prepoznamo krivu. Na sličan način pronađemo $AK7_3$. Kao rezultat, preostaje nam osam mogućnosti za posljednji stvarni potključ od $AK7$. Za razliku od DES-a, ne možemo lako otkriti bitove ključa iz jednog stvarnog potključa. Međutim, možemo reducirati kriptosustav na sedmorundni tako što eliminiramo posljednju rundu koristeći poznati posljednji stvarni potključ i analizirati dobiveni kriptosustavi sličnim metodama.

Redukcija sedam rundnog kriptosustava na šest rundi

Pretpostavljamo da je posljednji stvarni potključ poznat i da se kriptosustav može reducirati na sedmorundni. Pravi par u odnosu na pet-rundnu karakteristiku zadovoljava:

$$\begin{aligned} f' &= A2\ 00\ 80\ 00_x \\ g' &= T'_L \oplus H' \\ G' &= h' \oplus f' = h' \oplus A2\ 00\ 80\ 00_x \\ F' &= e' \oplus g' = T'_L \oplus H' \oplus 80\ 80\ 00\ 00_x \end{aligned}$$

Potvrđujemo da $f' \to F'$ i $g' \to G'$ i prebrajamo u dva koraka. U prvom koraku prebrajamo na 16-bitnom stvarnom potključu. Drugi korak prebraja na svakom od preostala dva bajta pravog potključa.

Omjer signala i buke prvog koraka koji pronalazi 16-bitni stvarni potključ $mx(AK6)$ je:

$$S/N = \frac{2^{16}}{16 \cdot (\frac{1}{7})^4 \cdot (\frac{1}{7})^2 \cdot 1} \approx 2^{29}$$

U drugom koraku koji pronalazi $AK6_0$ i $AK6_3$ omjer signala i buke je:

$$S/N = \frac{2^{8}}{16 \cdot (\frac{1}{7})^4 \cdot 2^{-16} \cdot 1} \approx 2^{31}$$

Kod prvog koraka jedan bit je neraspoznatljiv a u drugom koraku su dva. Zbog toga isprobavamo svih osam rezultirajućih mogućnosti za $AK6$ u paraleli u sljedećim koracima. Ukupno pronalazimo najviše 64 mogućnosti za zadnja dva stvarna potključa i tako možemo reducirati kriptosustav na šest rundi.

Redukcija kriptosustava na 5, 4, 3, 2 i 1 rundu

Koristeći zadnja dva stvarna potključa, možemo izračunati H i G za bilo koji šifrat T i reducirati kriptosustav na šest rundi. Svi pravi parovi u odnosu na pet-rundnu karakteristiku zadovoljavaju $f' = h' \oplus G' = A2008000_x$ i $f' \rightarrow g' \oplus 80800000_x$ (g' se može izračunati koristeći poznati $AK7$). Dva bajta od $AK5$ jednaki su odgovarajućim bajtovima u $AK7$. Isprobavamo svih 2^16 mogućnosti za 16-bitni stvarni potključ $mx(AK5)$. Za svaku mogućnosti i svaki par računamo F, F^* i $F' = F \oplus F^*$. Pravi par zadovoljava $F' = g' \oplus 80\ 80\ 00\ 00_x$. Prebrojavamo parove koji zadovoljavaju $f' = A2\ 00\ 80\ 00_x$, koji imaju jednake odgovarajuće vrijednosti od F' i vrijedi $f' \rightarrow F'$. Vrijednost od $mx(AK5)$ koja se najviše prebroji najizglednija je prava vrijednost. Omjer signala i buke za ovaj korak je:

$$S/N = \frac{2^{16}}{16 \cdot 2^{-32} \cdot 2^{-16}} = 2^{60}$$

U ovom koraku uvijek možemo razotkriti sve bitove stvarnog potključa.

S poznatim $AK5$ možemo reducirati kriptosustav na pet rundi i pronaći $AK4$ koristeći trorundnu karakteristiku. Dva bajta od AK4 imaju istu vrijednost kao njihovi odgovarajući bajtovi u $AK6$. Za svaku moguću vrijednost od $mx(AK4)$ prebrojavamo parove koji zadovoljavaju $e' = g' \oplus F' \neq 80\ 80\ 00\ 00_x$ (parovi za koje je $e' = 80\ 80\ 00\ 00_x$ možemo izbaciti jer oni imaju fiksan XOR), $e' \rightarrow E'$ i $d' \rightarrow D' = g' \oplus F'$. $AK3$ se izračuna na sličan način, prebrojavanjem parova za koje je $d' = A2\ 00\ 80\ 00_x$ i $d' \rightarrow D'$. $AK2$ također se računa na sličan način koristeći jednorundnu karakteristiku i prebrojavanjem parova za koje je $c' \neq 0, c' \rightarrow C'$ i $b' \rightarrow B'$. $AK1$ se računa prebrojavanjem parova za koje je $b' \rightarrow B'$.

$AK0$ ne možemo izračunati koristeći te parove jer njihov XOR otvorenih tekstova uvijek uzrokuje $A' = 02\ 00\ 00\ 00_x$ pa su sve mogućnosit jednako vjerojatne. Zbog toga koristimo druge karakteristike. Stvarni potključevi inicijalne transformacije $AK89$ i $AKab$ ne mogu se pronaći bez vrijednosti otvorenog teksta čak i kad su svi ostali potključevi poznati. U našem slučaju $AK0, AK89$ i $AKab$ nisu potrebni jer se sam ključ može pronaći preko stvarnih potključeva koje smo već izračunali.

Iako smo pronašli stvarne potključeve pomoću (ispravne) pretpostavke da mnogi stvarni potključevi imaju zajedničke vrijednosti u dva njihova bajta, moguće je proširiti ovaj napad na općeniti slučaj u kojem su svi stvarni potključevi neovisni.

Računanje ključa

Koristeći vrijednosti stvarnih potključeva $AK1 - AK7$, mogu se dobiti sljedeći XOR-ovi originalnih potključeva:

$$\begin{aligned} &K5 \oplus K7 \\ &K4 \oplus K6 \\ &K3 \oplus K5 \\ &K2 \oplus K4 \\ &K1 \oplus K3 \end{aligned} \tag{3.1}$$

Sam ključ može se izračunati iz tih vrijednosti analizom strukture algoritma procesiranja ključa.

Na početku isprobavamo svih 256 mogućih vrijednosti za $K5_1$. Za svaku vrijednost računamo (vrijednosti u uglatim zagradama poznate su iz 3.1):

$$\begin{aligned} K7_1 &= K5_1 \oplus [K5_1 \oplus K7_1] \\ K3_1 &= K5_1 \oplus [K3_1 \oplus K5_1] \\ K1_1 &= K3_1 \oplus [K1_1 \oplus K3_1]. \end{aligned}$$

Do četvrte runde algoritma procesiranja ključa imamo:

$$\begin{aligned} K7_0 &= K1_1 \oplus K5_1 \oplus S_1^{-1}(K7_1, K3_1) \\ K5_0 &= K7_0 \oplus [K5_0 \oplus K7_0] \\ K3_0 &= K5_0 \oplus [K3_1 \oplus K5_0] \\ K1_0 &= K3_0 \oplus [K1_1 \oplus K3_0]. \end{aligned}$$

Sada pronalazimo dva bajta samog ključa, jedan iz treće runde algoritma procesiranja ključa, a drugi iz druge runde:

$$K_7 = K3_1 \oplus K5_0 \oplus S_1^{-1}(K5_1, K1_1)$$
$$K_3 = K1_1 \oplus K3_0 \oplus S_1^{-1}(K3_1, K_7).$$

Zatim potvrđujemo pomoću prve runde algoritma da:

$$S_1(K1_0 \oplus K_7, K_3) = K1_1.$$

Za svaku preostalu vrijednosti isprobavamo svih 256 mogućnosti od $K4_0$. Zatim imamo:

$$K6_0 = K4_0 \oplus [K4_0 \oplus K6_0]$$
$$K2_0 = K4_0 \oplus [K2_0 \oplus K4_0].$$

Do četvrte runde algoritma procesiranja ključa:

$$K6_1 = K1_0 \oplus K5_0 \oplus S_0^{-1}(K6_0, K2_0)$$
$$K4_1 = K6_1 \oplus [K4_1 \oplus K6_1]$$
$$K2_1 = K4_1 \oplus [K2_1 \oplus K4_1]$$
$$K0_0 = K4_0 \oplus K3_0 \oplus K3_1 \oplus S_1^{-1}(K6_1, K2_0 \oplus K2_1)$$
$$K0_1 = K4_1 \oplus K6_1 \oplus S_0^{-1}(K7_0, K3_0 \oplus K3_1).$$

Ostatak ključa može se pronaći pomoću treće runde algoritma procesiranja ključa:

$$K_4 = K2_0 \oplus K1_0 \oplus K1_1 \oplus S_1^{-1}(K4_1, K0_0 \oplus K0_1)$$
$$K_5 = K2_1 \oplus K4_1 \oplus S_0^{-1}(K5_0, K1_0 \oplus K1_1)$$
$$K_6 = K3_0 \oplus K4_1 \oplus S_0^{-1}(K4_0, K0_0).$$

Do druge runde:

$$K_0 = K0_0 \oplus K6 \oplus K7 \oplus S_1^{-1}(K2_1, K4 \oplus K5)$$
$$K_1 = K0_1 \oplus K2_1 \oplus S_0^{-1}(K3_0, K6 \oplus K7)$$
$$K_2 = K1_0 \oplus K2_1 \oplus S_0^{-1}(K2_0, K4).$$

Kada imamo ključ, možemo potvrditi da je uistinu procesiran do poznatih stvarnih potključeva i da je XOR dešifriranog para šifrata jednak odabranoj XOR vrijednosti otvorenih tekstova. Ukoliko je ovaj uvijet zadovoljen, tada je izračunati ključ vjerojatno ispravan.

Bibliografija

[1] Eli Biham i Adi Shamir, *Differential Cryptanalysis of the Data Encryption Standard*, Springer-Verlag, London, UK, UK, 1993, ISBN 0-387-97930-1.

[2] Andrej Dujella, *Kriptografija, skripta*.

[3] Lars Knudsen i Matthew Robshaw, *The block cipher companion*, Information security and cryptography, Springer, Heidelberg, London, 2011, ISBN 978-3-642-17341-7, AU@.

[4] Douglas Robert Stinson, *Cryptography : theory and practice*, Discrete mathematics and its applications, Chapman & Hall/CRC, Boca Raton, 2006, ISBN 1-584-88508-4.

Sažetak

U ovom radu obrađeni su napadi diferencijalnom kriptoanalizom na neke inačice DES-a i FEAL. Diferencijalna kriptoanaliza je oblik kriptoanalize primjenjiv prvenstveno na blokovne kriptosustave, no također i kriptografske hash funkcije. U slučaju blokovnih kriptosustava odnosi se na skup tehnika za praćenje razlika kroz niz transformacija, otkrivanje mjesta gdje šifrat pokazuje ne-nasumično ponašanje i iskorištavanje takvih svojstava u svrhu otkrivanja tajnog ključa.
Prvo poglavlje opisuje te tehnike i pojmove, a primjenu obrađujemo u iduća dva poglavlja. U drugom poglavlju promatramo napade na razne varijante DES-a a u trećem poglavlju napad na FEAL.

Summary

In this paper we study the attacks on some variants of DES and FEAL. Differential cryptanalysis is a form of cryptanalysis applicable primarily to the block cryptsystems but also can be used to decipher cryptographic hash functions. When used to attack a block cipher, it consists of a set of techniques for tracking the differences through the series of transformations, looking for places where the cipher exhibits non-random behavior, and using such properties in order to reveal the secret key.
The first chapter describes those techniques and in the following two chapters we apply them on DES and FEAL.

Životopis

Leonora Gašpar rođena je 13. studenog 1991. u Makarskoj kao najmlađa od tri kćeri. Odrasta u Pločama gdje je pohađala Osnovnu školu Vladimira Nazora te završila opću gimnaziju u Srednjoj školi fra Andrije Kačića Miošića. Nakon završetka srednjoškolskog obrazovanja, godine 2010. upisuje preddiplomski studij matematike na Matematičkom odsjeku Prirodoslovno-matematičkog fakulteta Sveučilišta u Zagrebu. Tokom preddiplomskog studija razvija veliki interes za kolegije vezane uz računarstvo, pa nakon završetka preddiplomskog studija godine 2014. upisuje diplomski studij Računarstva i matematike na istom fakultetu. Tokom visokoškolskog obrazovanja učlanjuje se u veslački klub Prirodoslovno-matematičkog fakulteta u sklopu kojeg uspješno nastupa na brojnim natjecanjima. Na ljeto 2015. godine sudjeluje na ljetnoj radionici tvrke Ericsson Nikola Tesla, gdje, nakon završetka radionice, nastavlja raditi paralelno uz studij.