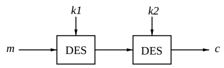
Dvojno šifriranje

2-DES: ključ $k = (k_1, k_2)$, $\quad k_1, k_2 \in_R \{0,1\}^{56}$.

Šifriranje: $c = \mathrm{DES}_{k_2}(\mathrm{DES}_{k_1}(m))$.



Odšifriranje: $m = \mathrm{DES}^{-1}_{k_1}(\mathrm{DES}^{-1}_{k_2}(c))$.

Dolžina ključa 2-DES-a je 112, torej za požrešno metodo potrebujemo 2^{112} korakov (nemogoče).

Opomba: dolžina blokov se ni spremenila.

Meet-in-the-middle napad na 2-DES

- Iz $c = E_{k_2}(E_{k_1}(m))$ sledi $E^{-1}_{k_2}(c) = E_{k_1}(m)$.
- INPUT: znani čp/tp pari $(m_1, c_1), (m_2, c_2), (m_3, c_3)$.
- OUTPUT: tajni ključ (k_1, k_2).

Za vsak $h_2 \in \{0,1\}^{56}$, izračunaj $E^{-1}_{h_2}(c_1)$ in shrani $[E^{-1}_{h_2}(c_1), h_2]$ v tabelo indeksirano s prvo koordinato.

Za vsak $h_1 \in \{0,1\}^{56}$ naredi naslednje:

1. Izračunaj $E_{h_1}(m_1)$.
2. Išči $E_{h_1}(m_1)$ v tabeli.
3. Za vsako *trčenje* $[E^{-1}_{h_2}(c_1), h_2]$ v tabeli preveri, ali je $E_{h_2}(E_{h_1}(m_2)) = c_2$ in $E_{h_2}(E_{h_1}(m_3)) = c_3$. Če se to zgodi, potem izpiši (h_1, h_2) in se vstavi.

Analiza:

- Število DES operacij je $\approx 2^{56} + 2^{56} = 2^{57}$.
- Pomnilnik: $2^{56}(64 + 56)$ bitov $\approx$983,040 TB.

Zaključek:

- 2-DES ima enako učinkovit ključ kot DES.
- 2-DES ni varnejši od DES-a.

Time-memory tradeoff:

- Čas: 2^{56+s} korakov; pomnilnik: 2^{56-s} enot, $1 \leq s \leq 55$. [DN]

Diferenčna kriptoanaliza

- požrešna metoda in metoda z urejeno tabel
- diferenčna metoda (za 1, 3, 6 in 16 ciklov)

Bločni tajnopisi s simetričnim ključen se ne uporabljajo samo za šifriranje, temveč konstrukcijo generatorjev psevdonaključnih p tokovnih tajnopisov, MAC in hash-funkcij.

Napadi na DES

1. **Požrešni napad**: preverimo vseh 2^{56} ključev (ne potrebujemo spomina).
2. Sestavimo **urejeno tabelo** $(e_K(x), K)$ za vseh 2^{56} ključev K in poiščemo v njej tak K, da je $y = e_K(x)$. Iskanje y-a je hitro, saj je tabela urejena.

   Ta metoda je praktična samo, če lahko večkrat uporabimo to tabelo.

Danes poznamo dva močna napada na DES: **diferenčno** kriptoanalizo in **linerno** kriptoanalizo.

Oba sta statistična, saj potrebujeta velike količine čistopisa in ustreznega tajnopisa, da določita ključ in zato nista praktična.

Zelo uspešna pa sta pri manjšem številu ciklov, npr. DES z 8imi cikli lahko razbijemo z diferenčno kriptoanalizo v nekaj minutah že na osebnem računalniku.

Diferenčno kriptoanalizo sta v letih 1990 in 1991 vpeljala Eli Biham in Adi Shamir (**izbran čistopis**).

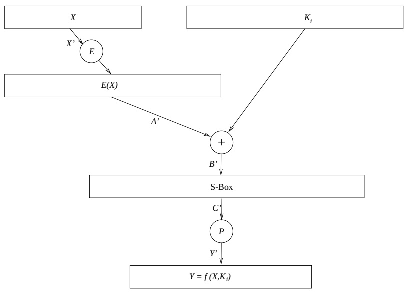
Oglejmo si pare tajnopisa za katere ima čistopis določene razlike. Diferenčna kriptoanaliza spremlja spreminjanje teh razlik, ko gre čistopis skozi nekaj ciklov DES-a in je šifriran z istim klučem. *Če poenostavimo*, ta tehnika izbere pare čistopisa s fiksno razliko (čistopis je lahko izbran naključno).

Z uporabo razlik tajnopisa določimo verjetnosti različnih ključev. Analiza mnogih parov tajnopisa nam na koncu da najbolj verjeten ključ.

Naj bosta X in X^* par čistopisov z razl Tajnopisa Y in Y^* poznamo, zato poznamo tu razliko Y'. Naj bo $A^{(*)} := E(X^{(*)})$ in $P(C^{(*)})$

Ker poznamo tudi razširitev E ter permuta poznamo A' in C' (glej sliko). $B^{(*)} = A^{(*)} \oplus$ poznamo, vendar je njuna razlika B' enaka ra

Trik je v tem, da za dano razliko A' niso enako vse razlike C'. Kombinacija razlik A' in C' vrednosti bitov izrazov $A \oplus K_i$ in $A^* \oplus K_i$. Od s pomočjo A in A^* dobimo informacije o ključ



V primeru, ko imamo več kot en cikel, si pomagamo z določenimi razlikami, ki jih imenujemo **karakteristike**. Le-te imajo veliko verjetnost, da nam dajo določene razlike tajnopisa ter se razširijo, tako da definirajo pot skozi več ciklov.

Poglejmo si zadnji cikel DES-a
(začetno in končno permutacijo lahko ignoriramo).
Če poznamo K_{16} poznamo 48 bitov originalnega ključa. Preostalih 8 bitov dobimo s požrešno metodo. Diferenčna kriptoanaliza nam da K_{16}.

Podrobnosti:

Škatla S_i oziroma funkcija $S_i : \{0,1\}^6 \longrightarrow \{0,1\}^4$ ima za elemente cela števila z intervala $[0,15]$:

		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
S_1:	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

Naj bo $B_j = b_1 b_2 b_3 b_4 b_5 b_6$.
$S_i(B_j)$ določimo na naslednji način.

Bita $b_1 b_6$ določita vrstico v, biti $b_2 b_3 b_4 b_5$ pa stolpec s v tabeli S_i, katere (v,s)-ti element je $S_i(B_j) \in \{0,1\}^4$

Za razliko $B_j' \in (\mathbb{Z}_2)^6$ definiramo množic
elementi: $\Delta(B_j') := \{(B_j, B_j \oplus B_j') \,|\, B_j \in (\mathbb{Z}_2$

Primer: oglejmo si škatlo S_1 in naj bo $B_j' =$
razlika (XOR) vhodov.

$\Delta(110100) =$ {(000000,110100),(000001,110101),...,(111111,00101

Za vsak urejen par izračunamo razliko izhoda

npr. $S_1(000000) = 1110$ in $S_1(110100) = 1001$
$\Longrightarrow$ razlika izhodov $C_j' =$ 0111.

Tabela izhodnih razlik C_j' in možnih vhodov B_j za vhodno razliko $B_j' = 110100$:

0000	-	
0001	8	000011, 001111, 011110, 011111, 101010, 101011, 110111, 111011
0010	16	000100, 000101, 001110, 010001, 010010, 010100, 100101, 011011, 100000, 100101, 010110, 101110, 101111, 110000, 110001, 111010
0011	6	000001, 000010, 010101, 100001, 110101, 110110
0100	2	010011, 100111
0101	-	
0110	-	
0111	12	000000, 001000, 001101, 010111, 011000, 011000, 011101, 100011, 101001, 101100, 110100, 111001, 111100
1000	6	001001, 001100, 011001, 101101, 111000, 111101
1001	-	
1010	-	
1011	-	
1100	-	
1101	8	000110, 010000, 010110, 011100, 100010, 100100, 101000, 110010
1110	-	
1111	6	000111, 001010, 001011, 110011, 111110, 111111

Tabela izhodnih razlik in porazdelitev vhodov za vhodno razliko 110100 (števila morajo biti soda, zakaj?):

0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
0	8	16	6	2	0	0	12	6	0	0	0	0	8	0	6

Pojavi se samo 8 od 16ih možnih izhodnih vrednosti.

Če pregledamo vse možnosti (za vsako škatlo S_i in vsako razliko), se izkaže, da je povprečno zastopanih samo 75-80% možnih razlik izhodov.

Ta neenakomerna porazdelitev je osnova za diferenčni napad.

Za vsako škatlo S_j (8 jih je) in za vsako vhodno razliko (2^6 jih je) sestavimo tako tabelo (skupaj 512 tabel).

Velja povdariti, da vhodna razlika ni odvisna od ključa K_i (saj smo že omenili, da je $A' = B'$), zato pa izhodna razlika C' *je* odvisna od ključa K_i.

Naj bo $A = A_1 \dots A_8$, $C = C_1 \dots C_8$ in
$j \in \{1, \dots, 8\}$.

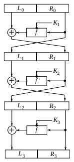
Potem poiščemo razliko $(C')_j$ v tabeli za S_j in $(A')_j$, ki nam določi vse možne vhode B_j iz katerih izračunamo vse $B_j \oplus A_j$, ki morajo vsebovati $(K_i)_j$.

Tako smo dobili nekaj kandidatov za $(K_i)_j$.

Primer: $A_1 = 000001$, $A_1^* = 110101$ in C_1'
Potem dobimo 13-to vrstico iz Tabele 1, ki v
elementov (torej smo zožili število možnosti iz
na 8).

Z naslednjim parom čistopisa dobimo nove ka
$(K_i)_j$ pa leži v preseku novih in starih kandid

Napad na DES s tremi cikli



Naj bo L_0R_0 in $L_0^*R_0^*$ par čistopisa in L_3R_3 in $L_3^*R_3^*$ par tajnopisa za katere velja:

$$L_3 = L_2 \oplus f(R_2, K_3) = L_0 \oplus f(R_0, K_1) \oplus f(R_2, K_3)$$

Še L_3^* izrazimo na podoben način in dobimo

$$L_3' = L_0' \oplus f(R_0, K_1) \oplus f(R_0^*, K_1) \oplus f(R_2, K_3) \oplus f(R_2^*, K_3)$$

Predpostavimo še, da je $R_0 = R_0^*$ oziroma $R_0' = 00\dots0$. Od tod dobimo

$$L_3' = L_0' \oplus f(R_2, K_3) \oplus f(R_2^*, K_3),$$

L_3' je razlika tajnopisov, L_0' pa razlika čistopisov, torej poznamo

$$f(R_2, K_3) \oplus f(R_2^*, K_3) \ \ (= L_0' \oplus L_3').$$

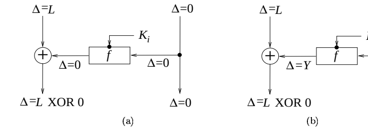
Naj bo $f(R_2, K_3) = P(C)$ in $f(R_2^*, K_3) = P(C^*)$, kjer sta C in C^* definirana enako kot prej (izhoda iz S škatel po tretjem ciklu). Potem je

$$C' = C \oplus C^* = P^{-1}(R_3' \oplus L_0').$$

Poznamo tudi $R_2 = R_3$ in $R_2^* = R_3^*$, saj sta R_3 in R_3^* dela tajnopisa.

Torej smo prevedli kriptoanalizo DES-a s tremi cikli na diferenčno kriptoanalizo DES-a z enim ciklom.

Napad na DES s 6-imi cikli



(a) (b)

(a) Leva stran je karkoli, desna razlika pa je (
To je trivialna karakteristika in velja z verjetn

(b) Leva stran je karkoli, desna vhodna razli
$0x60000000$ (vhoda se razlikujeta na 1. in 3
Verjetnost, da bosta izhodni razliki $0x6000$
$0x00808200$ je enaka $14/64$.

Karakteristika za n-ciklov, $n \in \mathbb{N}$, je seznam

$$L_0', R_0', L_1', R_1', p_1, \dots, L_n', R_n', p_n,$$

z naslednjimi lastnostmi:

- $L_i' = R_{i-1}'$ za $1 \le i \le n$.
- za $1 \le i \le n$ izberimo (L_{i-1}, R_{i-1}) in (L_{i-1}^*, R_{i-1}^*), tako da je $L_{i-1} \oplus L_{i-1}^* = L_{i-1}'$ in $R_{i-1} \oplus R_{i-1}^* = R_{i-1}'$. Izračunajmo (L_i, R_i) in (L_i^*, R_i^*) z enim ciklom DES-a. Potem je verjetnost, da je $L_i \oplus L_i^* = L_i'$ in $R_i \oplus R_i^* = R_i'$ natanko p_i.

Verjetnost karakteristike je $p = p_1 \times \cdots \times p_n$.

Začnimo s karakteristiko s tremi cikli:

$L_0' = 0x40080000$, $R_0' = 0x04000000$
$L_1' = 0x40000000$, $R_1' = 0x00000000$ $p = 1/4$
$L_2' = 0x00000000$, $R_2' = 0x04000000$ $p = 1$
$L_3' = 0x40080000$, $R_2' = 0x04000000$ $p = 1/4$
Potem velja

$$L_6' = L_3' \oplus f(R_3, K_4) \oplus f(R_3^*, K_4) \oplus f(R_5, K_6) \oplus f(R_5^*, K_6)$$

Iz karakteristike ocenimo $L_3' = 0x04000000$ in $R_3' = 0x40080000$ z verjetnostjo $1/16$.
Od tod dobimo razliko vhodov v S škatle 4. cikla: $001000000000000001010000\dots0$.

Razlike vhodov v škatle S_2, S_5, S_6, S_7 in S_8 so 000000. To nam omogoči, da z verjetnostjo $1/16$ določimo v 6-tem ciklu 30 bitov originalnega ključa.

V tabelah ne smemo nikoli naleteti na prazno vrstico (**filtracija**). Tako izključimo približno $2/3$ napačnih parov, med preostalimi pa je približno $1/6$ pravilnih.

...

Drugi primeri diferenčne kriptoana

Iste tehnike napadov na DES lahko uporabi
kadar imamo več kot 6 ciklov.

DES z n cikli potrebuje 2^m izbranega čistopis

n	m
8	14
10	24
12	31
14	39
16	47

Na diferenčno kriptoanalizo so občutljivi tu
algoritmi s substitucijami in permutacijami,
primer FEAL, REDOC-II in LOKI.

Napad na DES s 16-imi cikli

Bihan in Shamir sta uporabila karakteristiko s **3**-imi cikli in nekaj trikov v zadnjem ciklu.

Še več, z zvijačami sta dobila 56-bitni ključ, ki sta ga lahko testirala takoj (in se s tem izognila potrebi po števcih). S tem sta dobila linearno verjetnost za uspeh, tj. če je na voljo 1000 krat manj parov, imamo 1000 manj možnosti da najdemo pravi ključ.

Omenili smo že, da najboljši napad za DES s 16-imi cikli potrebuje 2^{47} izbranih čistopisov. Lahko pa ga spremenimo v napad z 2^{55} poznanega čistopisa, njegova analiza pa potrebuje 2^{37} DES operacij.

Diferenčni napad je odvisen predvsem od strukture S škatel. Izkaže se, da so DES-ove škatle zoptimizirane proti takemu napadu.

Varnost DES-a lahko izboljšamo s tem, da povečamo število ciklov. Vendar pa diferenčna kriptoanaliza DES-a s 17-imi ali 18-imi cikli potrebuje toliko časa kot požrešna metoda (več ciklov nima smisla).