Blok shifruesit

Qëllimet dhe objektivat

- Studimi i blok shifuresve si vegël qendrore në disenjin e protokoleve për kriptografi më çelës të përbashkët (d.m.th., kriptografi simetrike)
- Theksimi i shfrytëzimit të drejtë të blok shifruesve kundrejt disenjit dhe analizës së tyre
- Njoftimi me blok shifruesit DES dhe AES

Përmbajtja

Permutacionet dhe funksionet inverse

- Një funksion $f : \{0,1\}^\ell \to \{0,1\}^\ell$ është *permutacion* në qoftë se ekziston funksioni invers $f^{-1} : \{0,1\}^\ell \to \{0,1\}^\ell$ i tillë që

$$(\forall x \in \{0,1\}^\ell) f^{-1}(f(x)) = x.$$

- Pra, f duhet të jetë funksion bijektiv (një-një dhe mbi), d.m.th. për çdo $y \in \{0,1\}^\ell$ ekziston dhe është i vetëm një $x \in \{0,1\}^\ell$ i tillë që $f(x) = y$.

Permutacionet dhe funksionet inverse (Vazhdim)

x	00	01	10	11
$f(x)$	01	11	00	10

Tabela: Një permutacion

x	00	01	10	11
$f^{-1}(x)$	10	00	11	01

Tabela: Inversi i tij

x	00	01	10	11
$f(x)$	01	11	11	10

Tabela: Jo një permutacion

Blok shifruesit

- Le të jetë
$$E : \{0,1\}^k \times \{0,1\}^\ell \to \{0,1\}^\ell$$
një funksion që pasqyron një çelës $K \in \{0,1\}^k$ dhe një hyrje $x \in \{0,1\}^\ell$ për të kthyer në dalje $E(K,x) \in \{0,1\}^\ell$. Për një K të fiksuar le të jetë $E_K : \{0,1\}^\ell \to \{0,1\}^\ell$ funksioni i përkufizuar me
$$E_K(x) = E(K,x).$$

- Themi se E është një blok shifrues në qoftë se
  - $E_K : \{0,1\}^\ell \to \{0,1\}^\ell$ është permutacion për çdo K, d.m.th. ka një funksion invers E_K^{-1},
  - E dhe E^{-1} janë të kompjutueshëm në mënyrë efikase, ku $E^{-1}(K,x) = E_K^{-1}(x)$.

Shembull

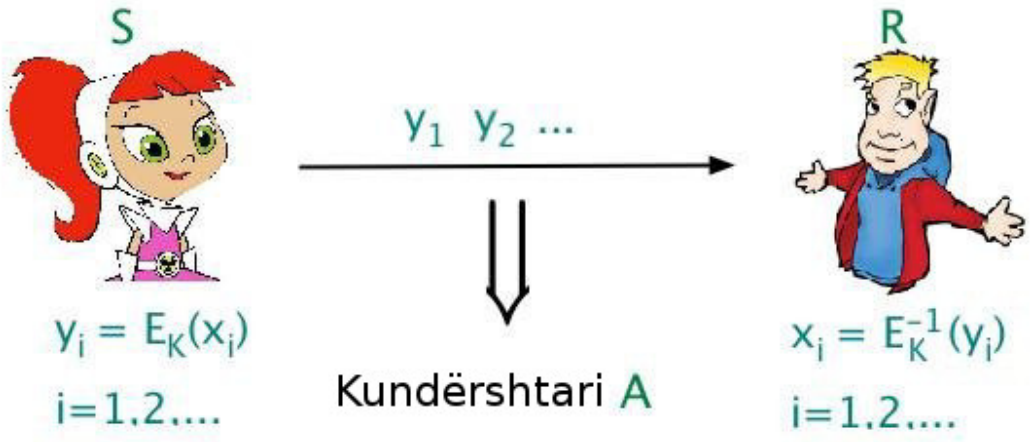
- Fusha e tabelës që i korrespondon çelësit K në rresht dhe hyrjes x në shtyllë është kodi i shifruar $E_K(x)$.

	00	01	10	11
00	00	01	10	11
01	01	00	11	10
10	10	11	00	01
11	11	10	01	00

- Në këtë rast, shifruesi invers E^{-1} jepet me të njëjtën tabelë: fusha e tabelës që i korrespondon çelësit K në rresht dhe daljes y në shtyllë është mesazhi E_K^{-1}.

Përdorimi i blok shifruesit

- $K \xleftarrow{\$} \{0,1\}^k$.
- K ju jepet (në mënyrë magjike) palëve S dhe R, por jo A
- S, R përdorin E_K
- Algoritmi E është publik! Mendojeni E_K si enkriptim nën çelësin K.



- Shpie nga kërkesa të sigurisë si:
  - Vështirë të kthehet K nga y_1, y_2,...
  - Vështirë të kthehet x_i nga y_i

Histori e DES

- Në vitin 1972 NBS (tani NIST) kërkoi një blok shifrues të standardizuar
- Në vitin 1974 IBM disenjoi Lucifer, i cili në fund evoluoi në DES (Data Encryption Standard).
- I adaptuar gjerë si standard, përfshirë ANSI dhe American Bankers Association
- Shfrytëzohet në ATM makinat
- Në vitin 2001 u zëvendësua me AES

Parametrat e DES

- Gjatësia e çelësit $|K| = k = 56$
- Gjatësia e blokut $|x| = \ell = 64$
- Kështu,

$$\text{DES} : \{0,1\}^{56} \times \{0,1\}^{64} \to \{0,1\}^{64}$$
$$\text{DES}^{-1} : \{0,1\}^{56} \times \{0,1\}^{64} \to \{0,1\}^{64}$$

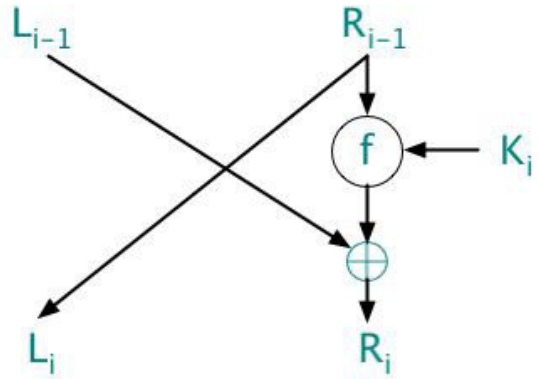
Konstruktimi i DES

function $\mathrm{DES}_K(M)$ ▷ $|K| = 56$ dhe $|M| = 64$
  $(K_1, \ldots, K_{16}) \leftarrow \mathit{KeySchedule}(K)$ ▷ $|K_i| = 48$ $(1 \leq i \leq 16)$
  $M \leftarrow \mathit{IP}(M)$
  Parso M si $L_0 \parallel R_0$ ▷ $|L_0| = |R_0| = 32$
  for $i = 1$ to 16 **do**
    $L_i \leftarrow R_{i-1}$
    $R_i \leftarrow f(K_i, R_{i-1}) \oplus L_{i-1}$
  end for
  $C \leftarrow \mathit{IP}^{-1}(L_{16} \parallel R_{16})$
  return C
end function

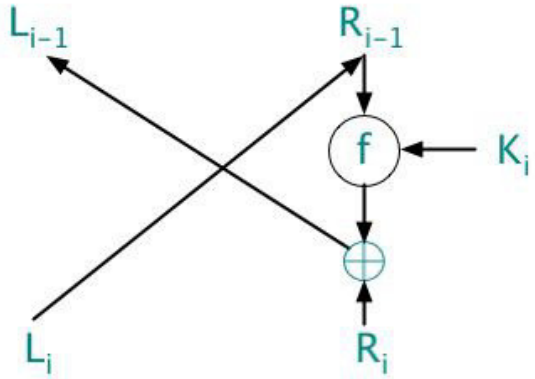
Konstruktimi i DES (Vazhdim)

function $\mathrm{DES}_K(M)$
  $(K_1, \ldots, K_{16}) \leftarrow KeySchedule(K)$ ▷ $|K| = 56$ dhe $|M| = 64$
  $M \leftarrow IP(M)$ ▷ $|K_i| = 48$ $(1 \leq i \leq 16)$
  Parso M si $L_0 \parallel R_0$ ▷ $|L_0| = |R_0| = 32$
  for $i = 1$ to 16 **do**
    $L_i \leftarrow R_{i-1}$
    $R_i \leftarrow f(K_i, R_{i-1}) \oplus L_{i-1}$
  end for
  $C \leftarrow IP^{-1}(L_{16} \parallel R_{16})$
  return C
end function

Raundi i



Invertibil për K_i të dhënë



Konstruktimi i DES (Vazhdim)

function $\mathrm{DES}_K(M)$ ▷ $|K| = 56$ dhe $|M| = 64$
  $(K_1, \ldots, K_{16}) \leftarrow \mathit{KeySchedule}(K)$ ▷ $|K_i| = 48$ $(1 \leq i \leq 16)$
  $M \leftarrow IP(M)$
  Parso M si $L_0 \parallel R_0$ ▷ $|L_0| = |R_0| = 32$
  for $i = 1$ to 16 **do**
    $L_i \leftarrow R_{i-1}$
    $R_i \leftarrow f(K_i, R_{i-1}) \oplus L_{i-1}$
  end for
  $C \leftarrow IP^{-1}(L_{16} \parallel R_{16})$
  return C
end function

function $\mathrm{DES}_K^{-1}(C)$ ▷ $|K| = 56$ dhe $|C| = 64$
  $(K_1, \ldots, K_{16}) \leftarrow \mathit{KeySchedule}(K)$ ▷ $|K_i| = 48$ $(1 \leq i \leq 16)$
  $C \leftarrow IP(C)$
  Parso C si $L_{16} \parallel R_{16}$ ▷ $|L_{16}| = |R_{16}| = 32$
  for $i = 16$ downto 1 **do**
    $R_{i-1} \leftarrow L_i$
    $L_{i-1} \leftarrow f(K_i, R_{i-1}) \oplus R_i$
  end for
  $M \leftarrow IP^{-1}(L_0 \parallel R_0)$
  return M
end function

Konstruktimi i DES (Vazhdim)

function $\mathrm{DES}_K(M)$
  $(K_1, \ldots, K_{16}) \leftarrow \mathit{KeySchedule}(K)$ ▷ $|K| = 56$ dhe $|M| = 64$
  $M \leftarrow IP(M)$ ▷ $|K_i| = 48$ $(1 \leq i \leq 16)$
  Parso M si $L_0 \parallel R_0$ ▷ $|L_0| = |R_0| = 32$
  for $i = 1$ to 16 **do**
    $L_i \leftarrow R_{i-1}$
    $R_i \leftarrow f(K_i, R_{i-1}) \oplus L_{i-1}$
  end for
  $C \leftarrow IP^{-1}(L_{16} \parallel R_{16})$
  return R
end function

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

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

Konstruktimi i DES (Vazhdim)

function $f(J, R)$ ▷ $|J| = 48$ dhe $|R| = 32$
  $R \leftarrow E(R)$
  $R \leftarrow R \oplus J$
  Parso R si $R_1 \parallel R_2 \parallel R_3 \parallel R_4 \parallel R_5 \parallel R_6 \parallel R_7 \parallel R_8$ ▷ $|R_i| = 6$ $(1 \leq i \leq 8)$
  for $i = 1, \ldots, 8$ **do**
    $R_i \leftarrow S_i(R_i)$ ▷ Secila S-kuti kthen 4 bit
  end for
  $R \leftarrow R_1 \parallel R_2 \parallel R_3 \parallel R_4 \parallel R_5 \parallel R_6 \parallel R_7 \parallel R_8$ ▷ $|R| = 32$
  $R \leftarrow P(R)$
  return C
end function

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

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

S-kutitë

S_1

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

S_2

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

S_3

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

Kriptoanalizë: Sulmet për kthim çelësi mbi blok shifruesit

- Kundërshtari A din $E : \{0,1\}^k \times \{0,1\}^\ell \to \{0,1\}^\ell$.
- Për (M_1, C_1),...,(M_q, C_q) të dhëna, ku $C_i = E(T, M_i)$ $(i = 1, \ldots, q)$ dhe M_1,...,M_q të ndryshme
- Gjej T
- Sigurisht, A ka C_1,...,C_q. Por pse A di M_1,...,M_q?
  - Aposteriori zbulim i të dhënave
  - Apriori dituri mbi kontekstin
- Të qenit konservativ është cilësi!

Aposteriori zbulim i të dhënave

- S, R ndajnë çelësin K
- Më 18 mars S enkripton

$$M = \text{Le të takohemi nesër ne orën 17}$$

  dhe i dërgon R tekstin e shfruar C.
- Kundërshtari kap C
- Më 19 mars kundërshtari vrojton se S, R takohen në 17 dhe konkludon se M është si më sipër.
- Kundërshtari di C dhe dekriptimin e tij M.

Apriori dituri mbi kontekstin

- S, R ndajnë çelësin K
- Email-at gjithmonë fillojnë me fjalën kyqe "From"
- S enkripton një email
- Kundërshtari merr tekstin e shifruar C
- Meqë di një pjesë të tekstit të mesazhit ("From") mund të ketë një shembull hyrje-dalje të blok shifruesit nën K.

Kriptoanalizë: Sulmet për kthim çelësi (Vazhdim)

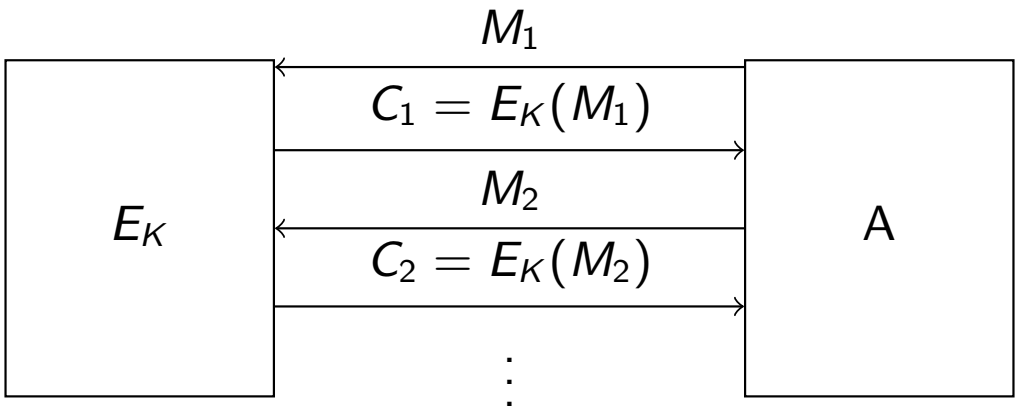
- Kundërshtari A din $E : \{0,1\}^k \times \{0,1\}^\ell \to \{0,1\}^\ell$.
- Për (M_1, C_1),. . . ,(M_q, C_q) të dhëna, ku $C_i = E(T, M_i)$ $(i = 1, \ldots, q)$ dhe M_1,. . . ,M_q të ndryshme
- Gjej T

Llojet e sulmeve

- *Sulmi i mesazhit të njohur (known-plaintext attack):*
  Për $M_1,\ldots,M_q$ të çfarëdoshme (jo të zgjedhura nga A)
- Për $(M_1, C_1),\ldots,(M_q, C_q)$ të dhëna, ku $C_i = E(T, M_i)$ $(i = 1, \ldots, q)$ dhe $M_1,\ldots,M_q$ të ndryshme
- Gjej T

Llojet e sulmeve (Vazhdim)

- *Sulmi i mesazhit të zgjedhur (chosen-plaintext attack):* A mund të zgjedhë $M_1,\ldots,M_q$, madje edhe në mënyrë adaptive, d.m.th. zgjedh M_i si funksion të $(M_1, C_1),\ldots,(M_{i-1}, C_{i-1})$ $(i = 1,\ldots,q)$.
- Për $(M_1, C_1),\ldots,(M_q, C_q)$ të dhëna, ku $C_i = E(T, M_i)$ $(i = 1,\ldots,q)$ dhe $M_1,\ldots,M_q$ të ndryshme
- Gjej T



Kërkimi i të gjithë çelësave

- Le të jenë $T_1, \ldots, T_{2^k}$ të gjithë çelësat k bitësh. Le të jetë $T \xleftarrow{\$} \{0,1\}^k$ çelësi i targetuar dhe (M_1, C_1) le të plotësojë kushtin $C_1 = E(T, M_1)$.

---

function $EKS_E(M_1, C_1)$ ▷ Exhaustive Key Search
  for $i = 1, \ldots, 2^k$ **do**
    if $E(T_i, M_1) = C_1$ **then**
      return T_i
    end if
  end for
end function

- A e gjen algoritmi çelësin e targetuar T?

Përkufizim

Një çelës K është konsistent me (M_1, C_1) në qoftë se $C_1 = E(K, M_1)$.

- Le të jetë S bashkësia e të gjithë çelësave konsistentë me (M_1, C_1). Atëherë EKS_E gjen ndonjë çelës në S.
- Në qoftë se $\ell \geq k$, atëherë T është „zakonisht“ i vetmi çelës në S.

Kërkimi i të gjithë çelësave (Vazhdim)

- Le të jenë $T_1, \ldots, T_{2^k}$ të gjithë çelësat k bitësh. Le të jetë $T \xleftarrow{\$} \{0,1\}^k$ çelësi i targetuar dhe (M_1, C_1) le të plotësojë kushtin $C_1 = E(T, M_1)$.

---

function $EKS_E(M_1, C_1)$ ▷ Exhaustive Key Search
  for $i = 1, \ldots, 2^k$ **do**
    if $E(T_i, M_1) = C_1$ **then**
      return T_i
    end if
  end for
end function

- A e gjen algoritmi çelësin e targetuar T?
- Po, zakonisht

Rritja e gjasës për të kthyer çelësin e targetuar

- Le të jenë $T_1, \ldots, T_{2^k}$ të gjithë çelësat k bitësh. Le të jetë $T \xleftarrow{\$} \{0,1\}^k$ çelësi i targetuar dhe $(M_1, C_1), \ldots, (M_q, C_q)$ le të plotësojnë kushtet $C_i = E(T, M_i)$ $(i = 1, \ldots, q)$.

---

function $EKS_E((M_1, C_1), \ldots, (M_q, C_q))$ ▷ Exhaustive Key Search
  for $i = 1, \ldots, 2^k$ **do**
    if $E(T_i, M_1) = C_1$ and $\cdots$ and $E(T_i, M_q) = C_q$ **then**
      return T_i
    end if
  end for
end function

Sa zgjat kërkimi i të gjithë çelësave?

- DES mund të kompjutohet me 1.6 Gbit/s në harduer.
- DES teksti i mesazhit 64 bit
- Një çip mund të performojë $(1.6 \cdot 10^9)/64 = 2.5 \cdot 10^7$ DES kompjutime në sekond.
- Pritet që DES të ketë sukses në 2^{55} DES kompjutime, prandaj merr kohën

$$\frac{2^{55}}{2.5 \cdot 10^7} \approx 1.4 \cdot 10^9 \text{ sekonda}$$
$$\approx 45 \text{ vjet}$$

- Komplementimi i çelësit (key-complementation): $45/2 = 22.5$ vjet
  - Që është parandaluese!
- A do të thotë kjo se DES është i sigurt?

Kriptoanaliza diferenciale dhe lineare

- Kërkimi i të gjithë çelësave është një sulm gjenerik: Nuk përpiqet të „shikojë përbrenda“ DES dhe t'i gjejë/eksploatojë dobësitë.

Metoda	Viti	q	Tipi i sulmit
Kriptoanaliza diferenciale	1992	2^{47}	Mesazh i zgjedhur
Kriptoanaliza lineare	1993	2^{44}	Mesazh i njohur

- Por thjesht ruajtja e 2^{44} çifteve hyrje-dalje kërkon 281 TiB.
- Në praktikë kostoja e këtyre sulmeve është parandaluese.

EKS sërish

function $EKS_E(M_1, C_1)$ ▷ Exhaustive Key Search
  for $i = 1, \ldots, 2^k$ **do**
    if $E(T_i, M_1) = C_1$ **then**
      return T_i
    end if
  end for
end function

- Observim: E kompjutimet mund të kryhen paralelisht.
- Wiener 1993:
  - $1 milion
  - 57,000 çipa
  - Parashikonte ta gjente çelësin në 3.5 orë
- EFF 1998:
  - $250,000
  - Gjen çelësin për 56 orë.

Përmbledhje mbi sigurinë e DES

- DES konsiderohet „i thyer“ meqë gjatësia e vogël e tij e çelësit lejon kërkim të shpejtë çelësi.
- Por, DES është disenj shumë i fortë, siç dëshmohet nga fakti se akoma nuk ka asnjë sulm praktik që eksploaton strukturën e tij.

2DES

- Blok shifruesi 2DES : $\{0,1\}^{112} \times \{0,1\}^{64} \to \{0,1\}^{64}$ përkufizohet me

$$2\mathrm{DES}_{K_1K_2}(M) = \mathrm{DES}_{K_2}(\mathrm{DES}_{K_1}(M)).$$

- Kërkimi i të gjithë çelësave merr 2^{112} DES kompjutime, që është tepër madje edhe për makina.
- Rezistent ndaj kriptoanalizave diferenciale dhe lineare

Sulmi i takimit në mes mbi 2DES

- Supozoni se K_1K_2 është një çelës i targetuar 2DES dhe se kundërshtari ka M, C të tillë që

$$C = 2\text{DES}_{K_1K_2}(M) = \text{DES}_{K_2}(\text{DES}_{K_1}(M))$$

- Atëherë,

$$\text{DES}^{-1}_{K_2}(C) = \text{DES}_{K_1}(M).$$

Sulmi i takimit në mes mbi 2DES (Vazhdim)

- Supozomi se $\mathrm{DES}_{K_2}^{-1}(C) = \mathrm{DES}_{K_1}(M)$ dhe $T_1, \ldots, T_N$ janë të gjithë DES çelësat e mundshëm, ku $N = 2^{56}$.
- Atëherë plani i sulmit do të ishte

$$\mathrm{DES}(T_i, M) \stackrel{?}{=} \mathrm{DES}^{-1}(T_j, C)$$

  - Ndërto tabelat L dhe R nga e majta dhe e djathta
  - Gjej i, j të tillë që $L[i] = R[j]$
  - Merr se $K_1 K_2 = T_i T_j$

Sulmi i takimit në mes mbi 2DES (Vazhdim)

- Le të jetë $T_1, \ldots, T_{2^{56}}$ një listë e DES çelësave.

---

function $MinM_{2\text{DES}}(M_1, C_1)$ ▷ Meet-in-the-middle
  for $i = 1, \ldots, 2^{56}$ **do**
    $L[i] \leftarrow \text{DES}(T_i, M_1)$
  end for
  for $j = 1, \ldots, 2^{56}$ **do**
    $R[j] \leftarrow \text{DES}^{-1}(T_j, C_1)$
  end for
  $S \leftarrow \{(i, j) : L[i] = R[j]\}$
  Zgjedh një $(l, r) \in S$ dhe **return** $T_l \parallel T_r$
end function

- Sulmi merr rreth 2^{57} $\text{DES}/\text{DES}^{-1}$ kompjutime.
- Interesant, por jo praktik

3DES

- Blok shifruesit

$$3\mathrm{DES3} : \{0,1\}^{168} \times \{0,1\}^{64} \to \{0,1\}^{64},$$
$$3\mathrm{DES2} : \{0,1\}^{168} \times \{0,1\}^{64} \to \{0,1\}^{64}$$

  përkufizohen me

$$3\mathrm{DES3}_{K_1\|K_2\|K_3}(M) = \mathrm{DES}_{K_3}((\mathrm{DES}^{-1}_{K_2}(\mathrm{DES}_{K_1}(M))),$$
$$3\mathrm{DES2}_{K_1\|K_2}(M) = \mathrm{DES}_{K_2}((\mathrm{DES}^{-1}_{K_1}(\mathrm{DES}_{K_2}(M))).$$

- Sulmi i takimit në mes mbi 3DES2 redukton gjatësinë „efektive“ të tij të çelësit në 112 bit.

Kufizimi i madhësisë së blokut

- Më vonë do të shohim se sulmet „birthday“ thyejnë një blok shifrues $E : \{0,1\}^k \times \{0,1\}^\ell \to \{0,1\}^\ell$ me kompleksitet $2^{\ell/2}$.
- Për DES ky është $2^{64/2} = 2^{32}$, që është i vogël, dhe kompleksiteti mbetet i pandryshuar për 2DES dhe 3DES.
- Kërkohet madhësi më e madhe e blokut

Histori e AES

- Më 1998: NIST shpall konkursin për një blok shifrues të ri
  - gjatësia e çelësit 128 bit
  - gjatësia e blokut 128 bit
  - më i shpejt sesa DES në softuer
- Dorëzime nga tërë bota: MARS, Rijndael, Two-Fish, RC6, Serpent, Loki97, Cast-256, Frog, DFC, Magenta, E2, Crypton, HPC, Safer+, Deal
- Më 2001: NIST përzgjedh Rijndael të bëhet AES

AES

function $\mathrm{AES}_K(M)$ ▷ $|K| = 128$ dhe $|M| = 128$
  $(K_0, \ldots, K_{10}) \leftarrow expand(K)$ ▷ $|K_i| = 128$ $(0 \leq i \leq 10)$
  $s \leftarrow M \oplus K_0$
  for $r = 1$ to 10 **do**
    $s \leftarrow S(s)$
    $s \leftarrow shift\_rows(s)$
    if $r \leq 9$ **then**
      $s \leftarrow mix\_cols(s)$
    end if
    $s \leftarrow s \oplus K_r$
  end for
  return s
end function

Implementimi i AES

- Më pak tabela sesa DES
- Operacione fushe të fundme
- AES-NI: harduer për AES, present në shumë procesorë. Mund të ekzekutojë AES me 1 cikël. Shumë shpejt!

Siguria e AES

- Sulmi më i mirë për kthim çelësi ka kompleksitet 2^{128}
- Siguria e blok shifruesve sillet në pohimin: „Nuk kemi arritur të gjejmë sulme efektive, dhe kemi provuar sulme nëpër linjat vijuese. . . “
  - Marrë parasysh zgjuarsinë dhe eksperiencën e deklaruesve. . .
  - Sugjerimi se blok shifruesit janë të mirë

Siguria ndaj kthimit të çelësit

- Kundërshtari A din $E : \{0,1\}^k \times \{0,1\}^\ell \to \{0,1\}^\ell$.
- $T \xleftarrow{\$} \{0,1\}^k$ është çelësi i targetuar
- Për (M_1, C_1),. . . ,(M_q, C_q) të dhëna, ku $C_i = E(T, M_i)$ $(i = 1, \ldots, q)$ dhe M_1,. . . ,M_q të ndryshme
- Gjej T
- Deri më tani, një blok shifrues është parë si i sigurt në qoftë se i reziston khimit të çelësit, d.m.th. në qoftë se nuk ekziston mënyrë efikase për të zgjidhur problemin e mësipërm.

Kufizimet e sigurisë ndaj kthimit të çelësit

- A është siguria ndaj kthimit të çelësit e mjaftueshme?
- Jashtëtokësorët nga planeti Kripton kanë një shifrues (të ri).
- Kundërshtari A din $A : \{0,1\}^{128} \times \{0,1\}^{128} \rightarrow \{0,1\}^{128}$ që garanton t'i rezistojë kthimit të çelësit. A do ta përdornit për të enkriptuar?
- Shifruesi është:

$$A_K(M) = M$$

- E pamundur të gjende çelësi nga shembuj hyrje/dalje, por
- Enkriptimi është i pasigurt meqë për tekstin e dhënë të shifruar dihet teksti i mesazhit.

Ani cka?

- Reaksion i mundshëm: Por DES, AES nuk janë të disenjuar sikur A, prandaj çfarë rëndësie ka kjo?
- Përgjegjja: Na thotë se siguria kundrejt kthimit të çelësit nuk është, si veti e një blok shifruesi, e mjaftueshme për siguri përdorimi të blok shifruesit.
- Si disenjues dhe shfrytëzues dëshirojmë të dijmë çfarë vetish të një blok shifruesi na japin siguri kur blok shifruesi të shfrytëzohet.

Pra çfarë është një blok shifrues „i mirë“?

Vetitë e mundshme	E nevojshme	E mjaftueshme
Siguria kundrejt kthimit të çelësit	Po	Jo!
Vështirë të gjendet M kur dihet $C = E_K(M)$	Po	Jo!
$\vdots$		

- Nuk mund të definojmë dhe të kuptojmë mirë sigurinë me anë të një liste të tillë (të pacaktuar)
- Dëshirojmë një veti „master“ të vetme të një blok shifruesi që eshtë e mjaftueshme të sigurojë siguri të shfrytëzimeve të zakonshme të blok shifruesit.