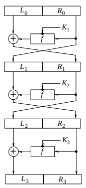
Napad na DES s tremi cikli



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 $R_0' = 00\ldots0$. 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

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

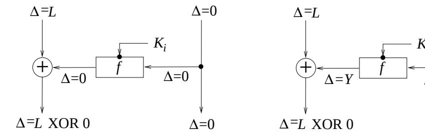
Naj bo $f(R_2, K_3) = P(C)$ in $f(R_2^*, K_3) = P(C^*)$, kjer sta C in C^* definirana enako kot prej (izhoda iz S škatel po tretjem ciklu). Potem je

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

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 0
To je trivialna karakteristika in velja z verjetno

(b) Leva stran je karkoli, desna vhodna razlik
$0x60000000$ (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

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

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: $00100000000000000001010000\ldots0$.

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 uporabin
kadar imamo več kot 6 ciklov.

DES z n cikli potrebuje 2^m izbranega čistopisa

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

Na diferenčno kriptoanalizo so občutljivi tud
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 13-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).

4. poglavje

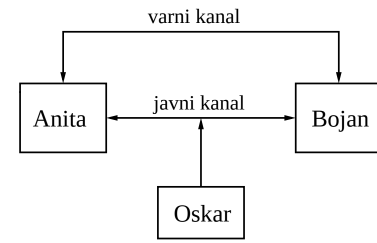
RSA sistem in faktorizacija

- Uvod
  - pomankljivosti simetrične kriptografije
  - kriptografija z javnimi ključi
- Teorija števil
- Opis in implementacija RSA
- Gostota praštevil
- Generiranje praštevil
- Gaussov izrek (o kvadratni recipročnosti)

Uvod

Pomankljivosti simetrične kriptogra

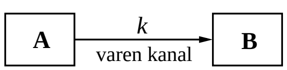
Sodelujoči si delijo *tajno* informacijo.



Dogovor o ključu

Kako Anita in Bojan vzpostavita tajni ključ k?

1. metoda: delitev point-to-point

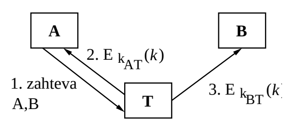


Varni kanal je lahko:
– kurir
– izmenjava na štiri oči (v temnem hodniku/ulici)

To ni praktično za večje aplikacije.

2. metoda: z neodvisnim centrom zaupanja T

– *Vsak* uporabnik A deli tajni ključ k_{AT} s centrom zaupanja T za simetrično šifrirno shemo E.
– Za vzpostavitev tega ključa mora A obiskati center zaupanja T *samo enkrat*.
– T nastopa kot **center za distribucijo ključev**: (angl. key distribution centre - KDC):



1. A pošlje T zahtevek za ključ, ki si ga želi deliti z B.
2. T izbere ključ k, ga zašifrira za A s ključem k_{AT}.
3. T zašifrira ključ k za osebo B s ključem k_{BT}.

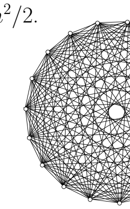
Problemi pri uporabi KDC

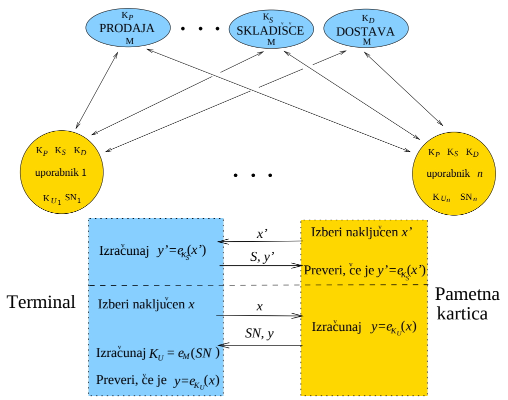
- centru zaupanja T moramo brezpogojno zaupati:
  - to ga naredi za očitno tarčo.
- Zahteva za stalno zvezo (on-line) s centrom T:
  - potencialno ozko grlo,
  - kritično za zanesljivost.

Upravljanje ključev

- v mreži z n uporabniki, mora vsak uporab različen ključ z vsakim uporabnikom,
- zato mora hraniti vsak uporabnik $n-1$ tajnih ključev,
- vseh tajnih ključev je $\binom{n}{2} \approx n^2/2$.

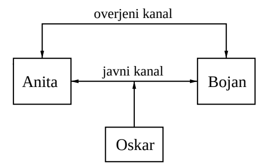
(Tudi preprečevanje tajenja je nepraktično.)





Kriptografija z javnimi ključi

Udeleženci si predhodno delijo *overjeno/avtentično* informacijo.



L. **1976** sta jo predlagala Whitfield **Diffie** in Martin **Hellman** (L. 1970 pa tudi James Ellis, ki je bil član Communication Electronics Security Group pri British Government Communications Headquarters).

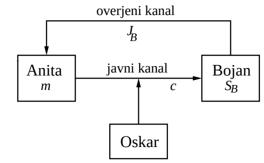
Generiranje para ključev

Vsaka oseba A naredi naslednje:

- generira par ključev (J_A, S_A),
- S_A je A-jev zasebni/tajni ključ,
- J_A je A-jev javni ključ.

Varnostna zahteva: za napadalca mora biti nemogoče priti do kluča S_A iz ključa J_A.

Šifriranje z javnimi ključi



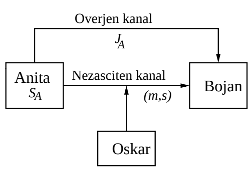
Da bi Bojanu poslala zaupno sporočil m, Anit

- dobi overjenjo kopijo Bojanovega javnega kju
- izračuna $c = E(J_B, m)$, kjer je E šifrirna fun
- pošlje Bojanu tajnopis c.

Za odšifriranje tajnopisa c Bojan naredi nasle

- Izračuna $m = D(S_B, c)$, kjer je D odšifrirna

Digitalni podpisi



Za podpis sporočila m Anita naredi naslednje:

- izračuna $s = \mathsf{Sign}(S_A, m)$,
- pošlje m in s Bojanu.

Bojan preveri Anitin podpis s sporočila m:

- pridobi si overjeno kopijo javnega ključa J_A,
- sprejme podpis, če je $\mathsf{Verify}(J_A, m, s) = \mathsf{Accept}$.

Prednosti kriptosistemov z javnimi ključi

- Ni zahteve po varnem kanalu.
- Vsak uporabnik ima 1 par ključev.
- Poenostavljeno upravljanje s ključi.
- Omogoča preprečevanje tajenja.

Pomanjkljivosti kriptosistemov z javnimi ključi

- Sheme z javnimi ključi so počasnejše.
- Javni ključi so večji od simetričnih.

V praksi uporabljamo skupaj sheme s simetričnimi in javnimi ključi in jim rečemo **hibridne sheme**

Primer: Da bi Bojanu poslala podpisano tajno sporočilo m, Anita naredi naslednje:

- izračuna $s = \mathsf{Sign}(S_A, m)$,
- izbere tajni ključ k simetrične šifrirne sheme (AES),
- pridobi overjeno kopijo Bojanovega javnega ključa J_B,
- pošlje $c_1 = E(J_B, k)$, $c_2 = \mathsf{AES}(k, (m, s))$.

Za odkritje sporočila m in preverjanje avtentičnosti, Bojan:

- odšifrira c_1: $k = D(S_B, c_1)$,
- odšifrira c_2 z uporabo ključa k, da dobi (m, s),
- pridobi overjeno kopijo javnega ključa J_A,
- preveri podpis s sporočila m.

Že l. 1977 so Ronald L. **Rivest**, Adi **Shamir** Leonard M. **Adleman** naredili prvo realizacij takšnega kriptosistema (**RSA**) (tajno pa že l. 1973 **C. Cocks** pri GCHQ).

Temu so sledili številni drugi nesimetrični kriptosistemi, med katerimi pa so danes najbolj pomembni naslednji:

- RSA (faktorizacija),
- Merkle-Hellman Knapsack (metoda nahrbtn
- Chor-Rivest
- McEliece (linearne kode),
- ElGamal (diskretni logaritem),
- eliptične krivulje.

Javni kriptosistemi **niso** nikoli brezpogojno var študiramo računsko/časovno zahtevne sisteme.

Teorija števil

Evklidov algoritem in reševanje Diofantske enačbe

$$ax + by = d, \qquad \text{kjer} \ \ D(a,b) \mid d.$$

Evklidov algoritem je zasnovan na preprostem dejstvu, da iz $k \mid a$ in $k \mid b$ sledi $k \mid a - b$.

Če je $D(a,b) = 1$ in poznamo eno rešitev (x_0, y_0), tj.

$$ax_0 + by_0 = d,$$

potem ima poljubna rešitev (x, y) naslednjo obliko:

$$x = x_0 - kb, \quad y = y_0 + ka, \quad \text{za } k \in \mathbb{Z}.$$

Zgodovina Evklidovega algoritma

Evklidov algoritem poišče največji skupni delitelj dveh naravnih števil in je zasnovan na dejstvu, da če število d deli števili a in b, potem deli tudi njuno razliko $a - b$.

V literaturi naletimo nanj prvič 300 p.n.š. v 7. knjigi Evklidovih **Elementov**.

Nakateri strokovnjaki so mnenja, da je njegov avtor Eudoxus (c. 375 p.n.š.). Gre za *najstarejši* netrivialen algoritem, ki je preživel do današnjih dni (glej Knuth).

Eno rešitev lahko poiščemo z **razširjenim Evklidovim algoritmom**.

Privzemimo, da je $a > b$ in zapišimo zgornjo enačbo malo bolj splošno (z zaporedji):

$$ap_i + bq_i = r_i.$$

Poiščimo dve trivialni rešitvi:

$$p_1 = 1, \quad q_1 = 0, \quad r_1 = a$$

in

$$p_2 = 0, \quad q_2 = 1, \quad r_2 = b.$$

Zaradi rekurzije

$$r_{i+1} = r_i - s_i r_{i-1}$$

(kjer je s_i izbran tako, da je $r_{i+1} < r_i$) si lahko izberemo še

$$p_{i+1} = p_i - s_i p_{i-1} \quad \text{in} \quad q_{i+1} = q_i - s_i q_{i}$$

Ko računamo a^{-1} (po modulu praštevila p), računamo samo r_i ter p_i (ne pa tudi q_i).

Zgled za razširjeni algoritem:

$4864 = 1{\cdot}3458{+}1406$	$p_2 := p_1 - 1 \cdot p_0 = 1$
$3458 = 2{\cdot}1406{+}646$	$p_3 := p_2 - 2 \cdot p_1 = -2$
$1406 = 2{\cdot}646{+}114$	$p_4 := p_3 - 2 \cdot p_2 = 5$
$646 = 5{\cdot}114{+}76$	$p_5 := p_4 - 5 \cdot p_3 = -27$
$114 = 1{\cdot}76{+}38$	$p_6 := p_5 - 1 \cdot p_4 = 32$
$76 = 2{\cdot}38{+}0$	$p_7 := p_6 - 2 \cdot p_5 = -91$

$4864 = 1{\cdot}3458{+}1406$	$p_2 = 1$	$q_2 = -1$
$3458 = 2{\cdot}1406{+}646$	$p_3 = -2$	$q_3 = 3$
$1406 = 2{\cdot}646{+}114$	$p_4 = 5$	$q_4 = -7$
$646 = 5{\cdot}114{+}76$	$p_5 = -27$	$q_5 = 38$
$114 = 1{\cdot}76{+}38$	$p_6 = 32$	$q_6 = -45$
$76 = 2{\cdot}38{+}0$	$p_7 = -91$	$q_7 = 128$

$$4864 \cdot (-91) + 3458 \cdot (128) = 38$$

Čeprav uporabljamo ta algoritem že stoletja, pa je presenetljivo, da ni vedno najboljša metoda za iskanje največjega skupnega delitelja.

R. Silver in **J. Terzian** sta leta **1962**
(v lit. J. Stein, *J. Comp. Phys.* **1** (1967), 397-405)
predlagala **binarni algoritem**:

B1. *Poišči tak največji $k \in \mathbb{Z}$, da bosta števili a in b deljivi z 2^k; $a \leftarrow a/2^k$ in $b \leftarrow b/2^k$, $K \leftarrow 2^k$.*

B2. *Dokler $2|a$ ponavljaj $a \leftarrow a/2$ in dokler $2|b$ ponavljaj $b \leftarrow a/2$.*

B3. *Če je $a = b$, je $D(a,b) = a * K$, sicer pa v primeru $a > b$, priredi $a \leftarrow a - b$, sicer $b \leftarrow b - a$ in se vrni na korak B2.*

Lehmerjev algoritem deli z majhnimi n
velikimi števili (izboljšave J. Sorenson, Jaebela

Dobro vprašanje je kako prenesti te ideje v GF

R. Schroeppel je že naredil prvi korak s
algoritmom **almost inverse**.

Kitajski izrek o ostankih. *Če so števila $m_1, m_2, ..., m_r$ paroma tuja, tj. $D(m_i, m_j) = 1$ za $i \neq j$, in $a_1, a_2, ..., a_r \in \mathbb{Z}$, potem ima sistem kongruenc*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r} \end{aligned}$$

enolično rešitev po modulu $M = m_1 \cdot m_2 \cdots m_r$,

$$x = \sum_{i=1}^{r} a_i \cdot M_i \cdot y_i \pmod{M},$$

kjer je $M_i = M/m_i$, $y_i = M_i^{-1} \bmod m_i$, $i = 1, ..., r$.

(angl. Chinese Reminder Theorem oziroma CRT)

Red elementa g v končni multiplikativni grupi je najmanjše celo število m tako, da $g^m = 1$.

Lagrangev izrek: *Naj bo G multiplikativna grupa reda n in $g \in G$, potem red g deli n.*

Naj bo p praštevilo. Generatorju multiplikativne grupe $\mathbb{Z}_p^*$ pravimo **primitiven element**.

DN: Koliko primitivnih elementov ima $\mathbb{Z}_p$?
Naj bo α primitiven element, potem za $\forall \beta \in \mathbb{Z}_p^*$ obstaja tak $i \in \{0, 1, \ldots, p-2\}$, da je $\beta = \alpha^i$.
Pokaži, da je red elementa β enak $\dfrac{p-1}{D(p-1, i)}$.

Eulerjevo funkcijo φ definiramo s

$$\varphi(n) = |\{x \in \mathbb{N} \mid x < n \text{ in } D(x, n) = 1\}|.$$

Potem za praštevilo p, naravno število n in poljubni tuji si števili a in b velja

$$\varphi(p^n) = p^n - p^{n-1} \quad \text{in} \quad \varphi(ab) = \varphi(a)\varphi(b).$$

Če poznamo faktorizacijo števila n, poznamo tudi $\varphi(n)$.

Fermatov izrek
Za praštevilo p in $b \in \mathbb{Z}_p$ velja $b^p \equiv b$ (mo

Eulerjev izrek
Če je $a \in \mathbb{Z}_n^*$ oziroma $D(n, a) = 1$, potem v

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$