SEMINAR IZ KRIPTOGRAFIJE

DES

predava: **Saša Habič (MORS)**

9. marec 1998

Na zadnjem seminarju:

- R. Petek: DES (nadaljevanje, do str. 88):
  - različni načini uporabe DES-a (ECB, CFB, CBC, OFB)
  - optimizacija po času oziroma spominu
- rešitev naloge 3.1.

Današnji načrt

- Saša Habič: DES (nadaljevanje in konec) **diferencialna kripto-analiza**
  - uvod
  - napad na DES s tremi iteracijami
  - napad na DES s šestimi iteracijami
  - drugi primeri diferencialne kripto-analize
- A.J.: še malo o DES-u
  - učinkovito iskanje DES ključa
  - 3-DES, DESX
  - drugi simetrični sistemi
- reševanje nalog iz 1. poglavja

O diferencialni kripto-analizi bo predavala
Saša Habič (MORS)

Po odkritju diferencialne kripto-analize je Don Coppersmith priznal, da je IBM v resnici
poznal ta napad (ne pa tudi linearno kripto-analizo) že ko so razvijali DES:

"Po posvetovanju z NSA, smo se zavedali, da utegne objava kriterijev načrtovanja odkriti tehniko kripto-analize. To je močno sredstvo, ki se ga da uporabiti proti mnogim tajnopisom. To bi zmanjšalo prednost ZDA pred drugimi na področju kriptografije."

Učinkovito iskanje DES ključa (1993)

Michael J. Wiener, Bell-Northern Research, Kanada

- Diferencialna kripto-analiza Bihama in Shamirja z 2^{47} izbranimi čistopisi
- Matsuijeva linearna kripto-analiza z 2^{47} poznanimi čistopisi

Zaenkrat so ti napadi zanimivi le teoretično.

Cilj Wienerjevega članka je precizna ocena časa in denarja potrebnega za graditev čipov za iskanje DES ključa.

Dan je par čistopis-tajnopis (P, C) ter začetni ključ K. Registri za vsako iteracijo so ločeni, tako da je vse skupaj podobno tekočemu traku:

- hitrost 50 MHz
- cena \$10.50 na čip
- 50 milijonov ključev na sekundo
- skupaj: \$100 tisoč, 5760 čipov, rabi 35 ur

Vse to je veljalo za ECB način.
Isti čipe se da uporabiti tudi za druge načine, cena in čas pa se nekoliko povečata. Recimo za CBC način rabimo \$1 milijon in 4 ure.

Varnost DES-a lahko enostavno povečamo, če uporabimo **3-DES** (zakaj ne 2-DES?).

$$\boxed{\begin{aligned}&\mathrm{DES_E(P, K_1)} \longrightarrow \mathrm{DES_D(DES_E(P, K_1), K_2)}\\ &\longrightarrow \mathrm{DES_E(DES_D(DES_E(P, K_1), K_2), K_3)}\end{aligned}}$$

$K_1 = K_2 = K_3$ dobimo običajni DES.

Običajno zamenjamo K_3 s K_1 in dobimo približno za faktor 10^{13} močnejši sistem.

Kako veliko je VELIKO?

sekund v enem letu	$\approx 3 \times 10^7$
(živimo "le" 2-3 milijarde sekund)	
starost našega sončnega sistema (v letih)	$\approx 6 \times 10^9$
urinih ciklov na leto (200 MHz)	$\approx 6.4 \times 10^{15}$
01-zaporedij dolžine 64	$2^{64} \approx 1.8 \times 10^{19}$

01-zaporedij dolžine 128	$2^{128} \approx 3.4 \times 10^{38}$
01-zaporedij dolžine 256	$2^{256} \approx 1.2 \times 10^{77}$
75 številčnih praštevil	$\approx 5.2 \times 10^{72}$
elektronov v vsem vesolju	$\approx 8.37 \times 10^{77}$

mega (M)	10^6
giga (G)	10^9
tera (T)	10^{12}
peta (P)	10^{15}
exa (E)	10^{18}

3-DES je trikrat počasnejši od DES-a.

To je pogosto nesprejemljivo, zato je leta 1984 Ron Rivest predlagal **DESX**:

$$\boxed{\mathrm{DESX}_{k.k1.k2}(x) = k2 \oplus \mathrm{DES}_k(k1 \oplus x).}$$

DESX ključ $K = k.k1.k2$ ima

$$56 + 64 + 64 = 184 \text{ bitov.}$$

DESX trik onemogoči preizkušanje vseh mogočih ključev (glej P. Rogaway, 1996). Sedaj rabimo več kot 2^{60} izbranega čistopisa.

Drugi simetrični sistemi:

FEAL, IDEA, SAFER,
RC2, RC4, RC5,
LOKI, CAST, 3WAY,
SHARK, SKIPJACK,
GOST, TEA, ...

Reševanje domačih nalog iz 1., 3. pogl.:

I/3: Določi število 2×2-matrik K (nad $\mathbb{Z}_{26}$), za katere je $K = K^{-1}$.

```
 n := 0;
for a from 0 to 25 do
  for b from 0 to 25 do
    for c from 0 to 25 do
      v := -a*a -b*c mod 26;
      if v = 25 then n:=n+1; fi
    od;
  od;
od;
ifactor(n);
quit;
```


Do naslednjega tedna

- pričnite brati 4. poglavje (str. 114-125)

- in končajte z reševanjem naloge iz 3. poglavja

Stinsonovega učbenika
Cryptography, Theory and Practice

Prihodnjič:

- Miroslav Masnoglav začel s 4. poglavjem (RSA)