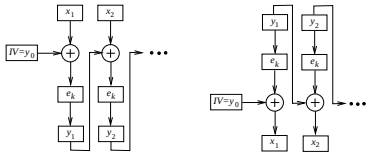
Cipher Block Chaining mode – CBC

čistopis/tajnopis: 64 bitni bloki $x_1, x_2, \ldots / y_1, y_2, \ldots$

Šifriranje: $y_0 := \mathrm{IV}$, $y_i := e_K(y_{i-1} \oplus x_i)$ za $i \geq 1$.



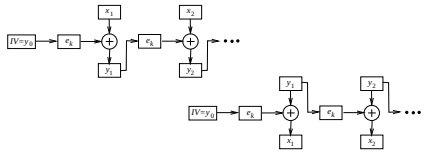
Odšifriranje: $y_0 := \mathrm{IV}$, $x_i := y_{i-1} \oplus d_K(y_i)$ za $i \geq 1$.

Identična čistopisa z različnimi IV dasta različen tajnopis. Eno-bitna napaka pri tajnopisu pokvari le odšifriranje dveh blokov.

Cipher Feedback mode – CFB

čistopis/tajnopis: 64 bitni bloki $x_1, x_2, \ldots / y_1, y_2, \ldots$

$y_0 := \mathrm{IV}$, šifriranje: $z_i := e_K(y_{i-1})$, $y_i := y_{i-1} \oplus x_i$, $i \geq 1$.



Odšifriranje ($y_0 := \mathrm{IV}$, $x_0 = e_K(\mathrm{IV})$):

$z_i := e_K(x_{i-1})$ in $x_i := y_i \oplus z_i$ za $i \geq 1$.

CFB se uporablja za preverjanje celovitosti sporočila (angl. message authentication code - MAC).

Output Feedback mode – OFB

čistopis/tajnopis: 64 bitni bloki $x_1, x_2, \ldots / y_1, y_2, \ldots$

Inicializacija: $z_0 := \mathrm{IV}$, šifriranje:

$z_i := e_K(z_{i-1})$ in $y_i := x_i \oplus z_i$ za $i \geq 1$.

Odšifriranje: ($z_0 := \mathrm{IV}$)

$z_i := e_K(z_{i-1})$ in $x_i := y_i \oplus z_i$ za $i \geq 1$.

OFB se uporablja za satelitske prenose.

Napadi na šifro DES

Požrešni napad: preverimo vseh 2^{56} ključev.

Leta 1993 Michael J. Wiener, Bell-Northern R
Kanada, predstavi učinkovito iskanje DES klj

- **diferenčna kriptoanaliza** z 2^{47} izbranim (Biham in Shamir 1989)
  – je učinkovita tudi na nekaterih drugih bloči
- **linearna kriptoanaliza** z 2^{47} poznanim (Matsui 1993):

Slednja napada sta statistična, saj potrebujet količine čistopisa in ustreznega tajnopisa, da ključ. Pred leti sta bila napada zanimiva le te

Wienerjev cilj je bil precizna ocena časa in denarja potrebnega za graditev čipov za iskanje DES ključa.

Požrešna metoda na prostor ključev: 2^{56} korakov je zlahka paralelizirana.

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

Pri linearni kriptoanalizi hranjenje parov zavzame 131,000 Gbytov. Implementirano leta 1993: 10 dni na 12 mašinah.

Po odkritju diferenčne kriptoanalize je
Don Coppersmith priznal, da je IBM v resnici
poznal ta napad (ne pa tudi linearno kriptoanalizo) že
ko so razvijali DES:

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

Novejši rezultati napadov

DES izivi pri RSA Security (3 poznani PT/CT pari):

The unkn	own mess	age is:	????????

junij 1997: razbito z internetnim iskanjem (3m).

julij 1998: razbito v treh dneh z DeepCrack mašino (1800 čipov; \$250,000).

jan. 1999: razbita v 22 h, 15 min (DeepCrack + porazdeljena.mreža).

V teku (porazdeljena.mreža): RC5 – 64-bitni izziv:

- pričeli konec 1997; trenutna hitrost: 2^{36} ključev/sec (2^{25} secs/leto; pričakovani čas: ≤ 8 let).

Implementacijski napadi na DE

Napadi s pomočjo diferencialne analize porabe
(angl. differential power analysis (**DPA**) atta

- Kocher, Jaffe, Jun 1999,
- procesorjeva poraba moči je odvisna od inst
- merimo porabo moči inštrukcij, ki se izvede krogih DES-a
- ≈1000 tajnopisa zadoščajo za odkritje tajne

Napadi s pomočjo diferenčne analize napak
(angl. differential fault analysis (**DFA**) attacl

- Biham, Shamir 1997.
- napad: zberi naključne napake v 16-ih krogi
- ≈200 napačnih odšifriranj zadošča za tajnega ključa.

Vse o napadih je veljalo za ECB način.

Isti čipe se da uporabiti tudi za druge načine, cena in čas pa se nekoliko povečata. Recimo po Wienerju za CBC način rabimo \$1 milijon in 4 ure.

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

$$\mathrm{DES_E}(\mathrm{P},\mathrm{K_1}) \longrightarrow \mathrm{DES_D}(\mathrm{DES_E}(\mathrm{P},\mathrm{K_1}),\mathrm{K_2}) \longrightarrow \mathrm{DES_E}(\mathrm{DES_D}(\mathrm{DES_E}(\mathrm{P},\mathrm{K_1}),\mathrm{K_2}),\mathrm{K_3})$$

Za $K_1 = K_2 = K_3$ dobimo običajni DES.

Običajno pa 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	$\approx 2^{64} \approx 1.8 \times 10^{19}$
01-zaporedij dolžine 128	$\approx 2^{128} \approx 3.4 \times 10^{38}$
01-zaporedij dolžine 256	$\approx 2^{256} \approx 1.2 \times 10^{77}$
75 številčnih praštevil	$\approx 5.2 \times 10^{72}$
elektronov v vsem vesolju	$\approx 8.37 \times 10^{77}$

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

3-DES je trikrat počasnejši od DES-a.

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

$$\boxed{\mathrm{DESX_{k,k1,k2}(x) = k2 \oplus DES_k(k1 \oplus x).}}$$

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.

Hitrost

Preneel, Rijmen, Bosselaers 1997.

Softwarski časi za implementacijo na 90MHz Pentiumu.

šifra	velikost ključa (biti)	hitrost
DES	56	10 Gbits/sec (ASI
DES	56	16.9 Mbits/s
3DES	128	6.2 Mbits/s
RC5-32/12	128	38.1 Mbits/s
Arcfour	variable	110 Mbits/s

Opis šifre AES

Dolžina blokov je 128 bitov, ključi imajo tri možne dolžine: 128 ($N_r = 10$), 192 ($N_r = 12$) in 256 ($N_r = 14$),

1. *Za dan čistopis x, inicializiramo* `State` *z x in opravimo* AddRoundKey, *ki z operacijo XOR prišteje* `RoundKey` *k* `State`.
2. *Za vsak od $N_r - 1$ krogov, opravi na* `State` *zaporedoma zamenjavo* SubBytes, *operaciji* ShiftRows *in* MixColumns *ter izvede* AddRoundKey.
3. *Naredi* SubBytes, ShiftRows *in* AddRoundKey.
4. *Za tajnopis y definiraj* `State`.

Vse operacije v AES so opravljene s pomočjo zlogov in vse spremenljivke so sestavljene iz določenega števila zlogov.

Čistopis x je sestavljen iz 16-ih zlogov: $x_0, \ldots, x_{15}$.

`State` je sestavljen iz (4×4)-dim. matrike zlogov:

$$\begin{pmatrix} s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1,0} & s_{1,1} & s_{1,2} & s_{1,3} \\ s_{2,0} & s_{2,1} & s_{2,2} & s_{2,3} \\ s_{3,0} & s_{3,1} & s_{3,2} & s_{3,3} \end{pmatrix}.$$

`State` dobi vrednosti iz x na naslednji način:

$$\begin{pmatrix} s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1,0} & s_{1,1} & s_{1,2} & s_{1,3} \\ s_{2,0} & s_{2,1} & s_{2,2} & s_{2,3} \\ s_{3,0} & s_{3,1} & s_{3,2} & s_{3,3} \end{pmatrix} := \begin{pmatrix} x_0 & x_4 & x_8 & x_{12} \\ x_1 & x_5 & x_9 & x_{13} \\ x_2 & x_6 & x_{10} & x_{14} \\ x_3 & x_7 & x_{11} & x_{15} \end{pmatrix}.$$

Na vsak zlog bomo gledali kot na dve šestnajstiški števili.

Operacija SubBytes deluje kot zamenjava, permutacija π_S $\{0,1\}^8$, na vsakem zlogu od `State` posebej, z uporabo S-škatel.

Druge simetrične šifre:

MARS, RC6, Serpent, Twofish
FEAL, IDEA, SAFER,
RC2, RC4, RC5,
LOKI, CAST, 3WAY,
SHARK, SKIPJACK,
GOST, TEA, ...