College Cryptografie

Cursusjaar 2006

Moderne systemen

7 januari 2006

Blokgeheimschrift

Data Encryption Algorithm

Cryptoanalyse van DES

Alternatieven voor DES

Advanced Encryption Standard

ONDERWERPEN

- n-bits→n-bits bijectieve afbeelding
- maximaal $2^n!$ afbeeldingen mogelijk
- 64-bits blok, 56 bit sleutel: $2^{56} \ll 2^{64}!$
- herhaalde encryptie $M \to C \to C^2 \to \cdots \to C^p = M$
  - fixed point $E(M,K) = M$
  - antifixed point $E(M,K) = \overline{M}$
  - zwakke sleutel $E(E(M,K),K) = M$
- *whitening* $M \oplus W_k = M' \to \cdots \to C' \oplus W'_k = C$
- CBC = Cipher Block Chaining, IV = Initial Vector

$$C_0 = IV,\ C_i = E(M_i \oplus C_{i-1})$$

$E(M,K)$: $L_1, R_1 = R_0,\ L_0 \oplus F(R_0, K_1)$

$L_2, R_2 = R_1,\ L_1 \oplus F(R_1, K_2)$

$L_3, R_3 = R_2,\ L_2 \oplus F(R_2, K_3)$

$D(C,K)$: $L_2, R_2 = R_3,\ L_3 \oplus F(R_3, K_3)$

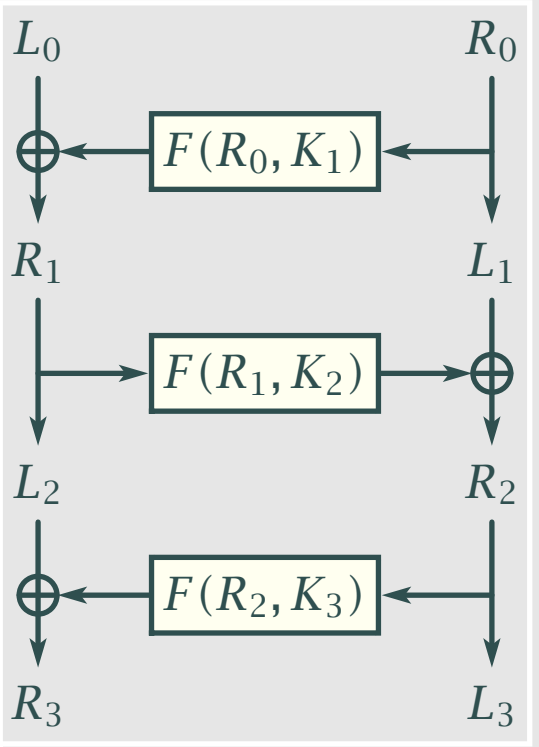
$L_1, R_1 = R_2,\ L_2 \oplus F(R_2, K_2)$

$L_0, R_0 = R_1,\ L_1 \oplus F(R_1, K_1)$

Geen bijzondere eisen aan F

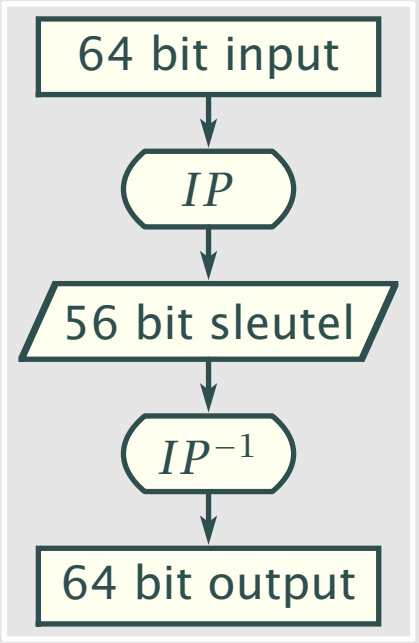
Meer stappen i.h.a. meer veiligheid

Gebalanceerd is # bits L = # bits R

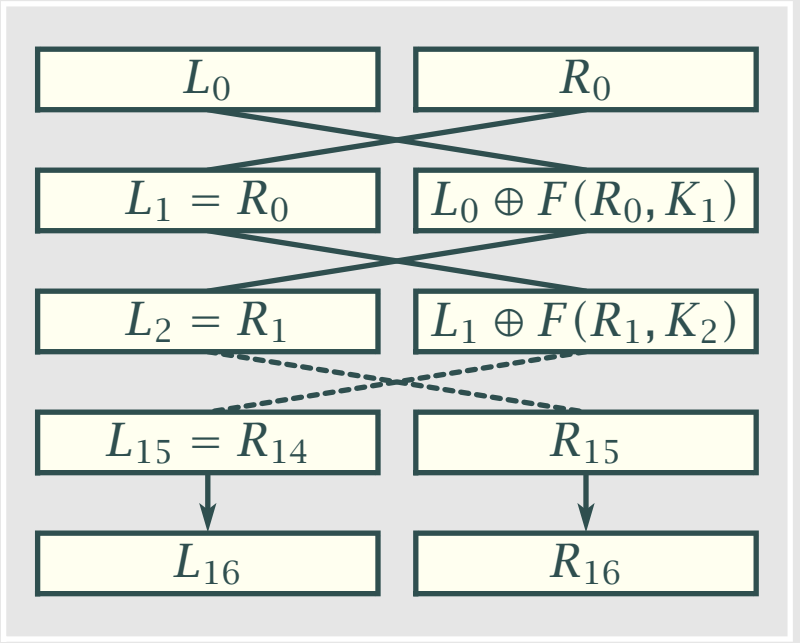


Feistel geheimschrift

1973	Initiatief National Bureau of Standards (nu NIST)
1975	IBM enige inzender voor DEA/DES
1978	Hearings US Senate Committee on Intelligence
1980	Hellman Time Memory Tradeoff
	partiële resultaten in de volgende jaren
1991	Biham en Shamir Differential Cryptanalysis
1993	Matsui Linear Cryptanalysis
1997	Software brute force
	NIST start ontwikkeling van AES
1998	Hardware brute force
1999	DES verlengd, waarschijnlijk voor het laatst

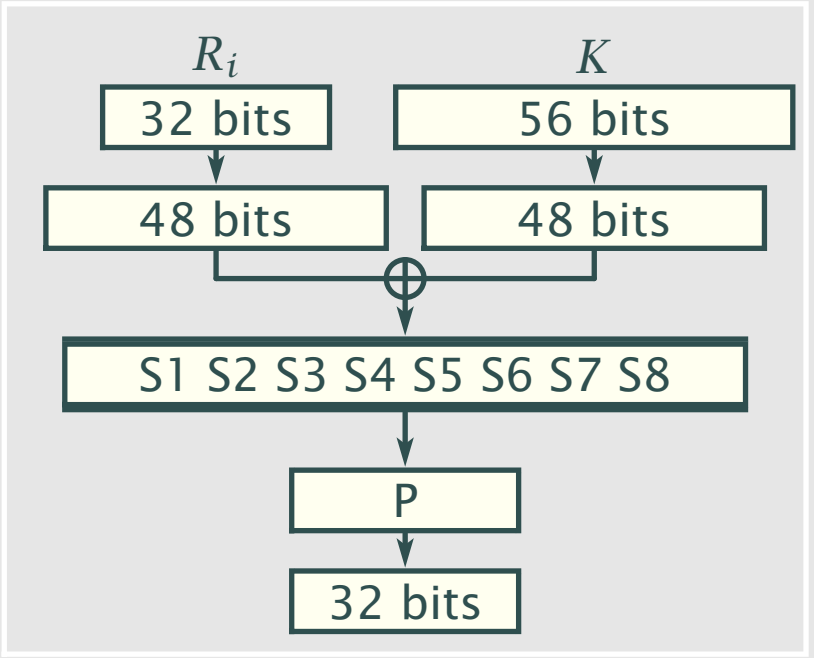


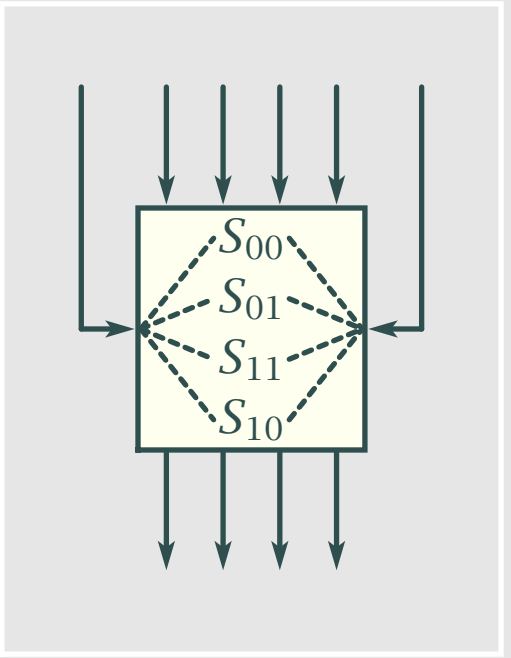
hoofdschema



transformatie

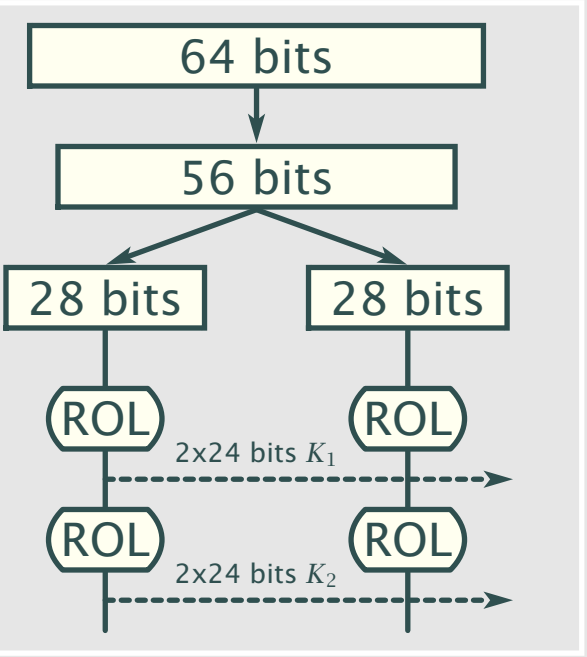
Schematisch overzicht





Complementariteitseigenschap: $DES(M,K) = \overline{DES(\overline{M},\overline{K})}$

Transformatie functie



- drop pariteitsbits 64→56
- rotaties 112222221222221
- 4 zwakke sleutels
  (00...) (11...)
  $M = E(E(M,K),K)$
- 12 halfzwakke sleutels
  (0101...) (1010...)
  $M = E(E(M,K'),K)$

Sleutelschema

- 56 bit DES niet veilig genoeg meer
- 2x DES is $E(E(M,K_1),K_2)$ *niet* equivalent 112 bits
  maar slechts 57 bits wegens "meet in the middle" aanval
- 3X DES is $E(D(E(M,K_1),K_2),K_3)$ EDE-schema
  Triple DES standaard
  Drie mogelijkheden:
  1. $K_1 \neq K_2 \neq K_3$
  2. $K_1 = K_3 \neq K_2$
  3. $K_1 = K_2 = K_3$ "DES compatibility mode"

Triple DES

Onderwerpen

- DES controverse
- Uitputtend zoeken
- Fysische methoden
  - foutinjectie
  - tijdsduur van operaties
  - analyse van stroomverbruik
- Time Memory Tradeoff
- Differentiële cryptoanalyse
- Lineaire cryptoanalyse

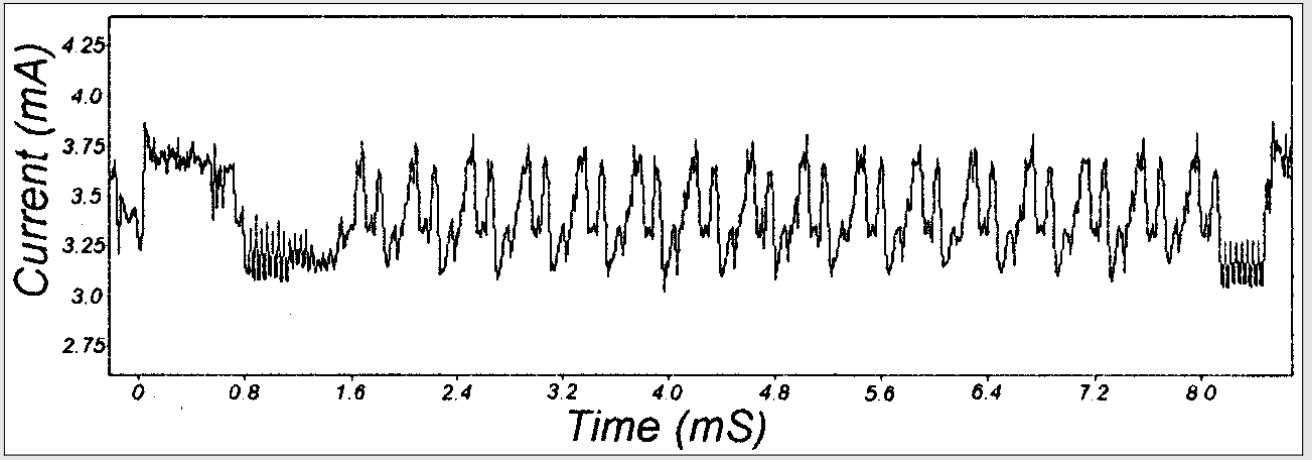
- National Security Agency (NSA) betrokken bij ontwikkeling
- Lucifer 128 bits vs. DES 56 bits: *verzwakt door NSA?*
  is 16 ronden te weinig?
- S-doos structuur: *valluik ingebouwd?*
- ontwikkelcriteria geheim: *verdacht?*
  veel later blijkt: vanwege differentiële cryptoanalyse
- US Senate Committee on Intelligence (1978) concludeert:
  - DES is more than adequate for its intended applications;
  - IBM invented and designed DES;
  - NSA did not tamper with the design;
  - NSA certified DES free of known statistical/mathematical weakness.

DES controverse

- *hardware*
  1984 256.000 encrypties sec^{-1}
  1998 Deep Crack machine, US$ 250.000
  2.500.000 sec^{-1}, 37.050 chips parallel, 9 dagen max
- *software*
  1997 Rocke Verser start internet programma
  78.000 deelnemers, 14.000 machines, 18 feb – 17 juni
- *sleutelherkenning*
  $DES^{-1}(C,K) \stackrel{?}{=} M$: door [azAZ09.,?!] 70 uit 256 plausibel
  DES-UD ≈ 16 bytes, $(70/256)^{16} \times 2^{56} \approx 70.000.000$ vals alarm
  known plaintext, UD ≈ 8 bytes, $\approx 2^{16}$ vals alarm

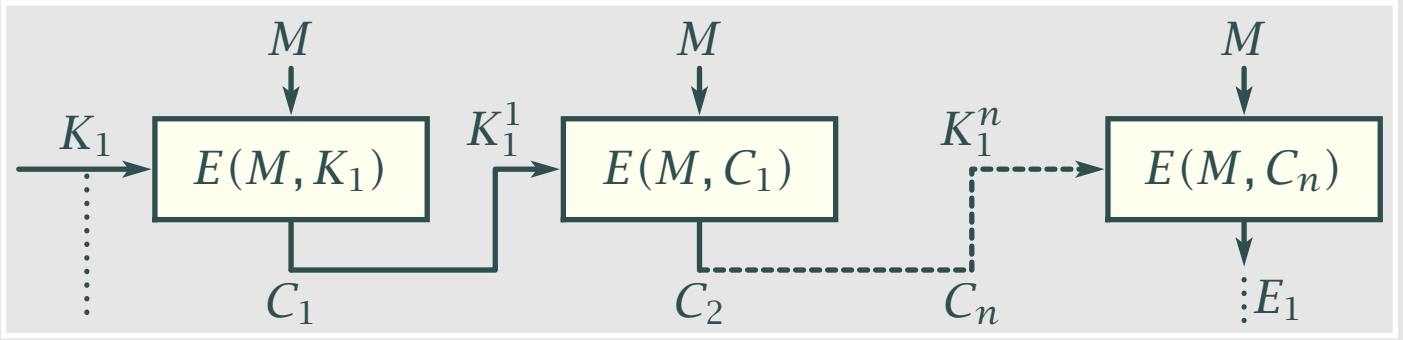
Uitputtend zoeken

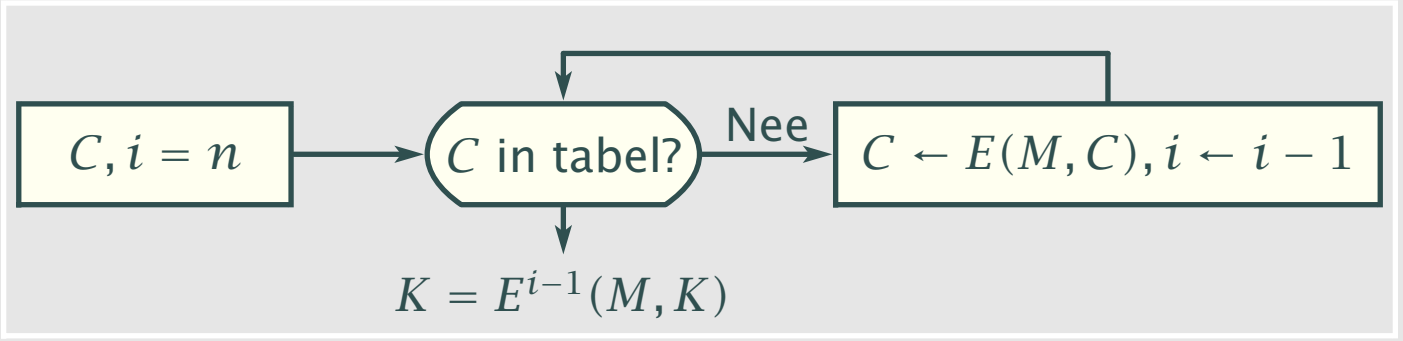
DES vercijfering



DPA = Differential Power Analysis

metingen middelen en vergelijken referentiewaarde: sleutelbits





Time Memory Tradeoff

1991 Biham en Shamir (chosen plaintext)

kies pt: $C = E(M,K)$ en $C^* = E(M^*,K)$ met $\Delta M = M \oplus M^*$
per ronde: $(R_{i-1} \oplus K_i) \oplus (R^*_{i-1} \oplus K_i) = R_{i-1} \oplus R^*_{i-1} = \Delta R$
onderzoek per S-doos combinaties (R_{i-1}, R^*_{i-1}) met $\Delta R = \text{const}$

Voorbeeld DES 1e substitutie van S_1:

$$\Delta_{in} = 1000_2 \begin{cases} (A,2)(2,A) \\ (6,E)(E,6) \end{cases} \xrightarrow{S_1} \Delta_{uit} = 1011_2 \begin{cases} (6,D)(D,6) \\ (B,0)(0,B) \end{cases}$$

omgekeerd: $(\Delta_{in}, \Delta_{uit}) = (8,B) \xrightarrow{in} (2,A)(A,2)(6,E)(E,6)$

B.v. 4-stap Feistel: $L_4, R_4 = R_3, \underbrace{L_1 \oplus f(R_1, K_2)}_{L_3 = R_2} \oplus f(R_3, K_4)$

$$\Delta = f(R_3, K_4) \oplus f(R_3^*, K_4) = L_1' \oplus \underbrace{f(R_1, K_2) \oplus f(R_1^*, K_2)}_{\text{uit speciale } \Delta M} \oplus R_4'$$

De speciale ΔM heet een *karakteristiek*.
Invoerverschil wordt over meerdere mogelijkheden verdeeld, dus per M slechts kans op gewenst verschil. Dan ook "bingo!"

Voor DES $p \leq 14/64$ per S-doos, karakteristiek 19600000_{16} op 3 dozen heeft $p = 0.004274$, na 13 ronden $p \approx 2^{-47}$.
Plus wat andere trucs → iets beter dan uitputtend zoeken.

- Precies genoeg (16) ronden gegeven beste karakteristiek.
- Permutatie na S-dozen blijkbaar zo gekozen dat kans op goede karakteristieken minimaal.
- Volgorde S-dozen bijna optimaal, met b.v. $\ldots S_1 S_7 S_4 \ldots$ karakteristiek met $p = 2^{-43}$ over 15 ronden.
- Substituties in S-dozen optimaal.
- Geen 4 substituties per S-doos verzwakt aanzienlijk.
- Eerst $R \oplus K_i$ en dan $32 \rightarrow 48$ verzwakt.
- Onafhankelijke subsleutels verbetert nauwelijks.

Conclusie: DES optimaal tegen differentiële cryptoanalyse.
Bevestiging door Coppersmith (lid IBM's DES-team).

1993 Matsui (known plaintext)

$$M[m_1, m_2, \ldots] \oplus C[c_1, c_2, \ldots] = K[k_1, k_2, \ldots] \text{ met kans } p$$

$$M[m_1, m_2, \ldots] = \vec{X}_M \cdot \vec{M} \quad (\vec{X}_M \text{ bit selector voor } M)$$

Itereerbare karakteristiek-combinatie van Matsui:

$$R[15] \oplus F(R,K)[7,18,24] = K[22] \quad p = 42/64$$

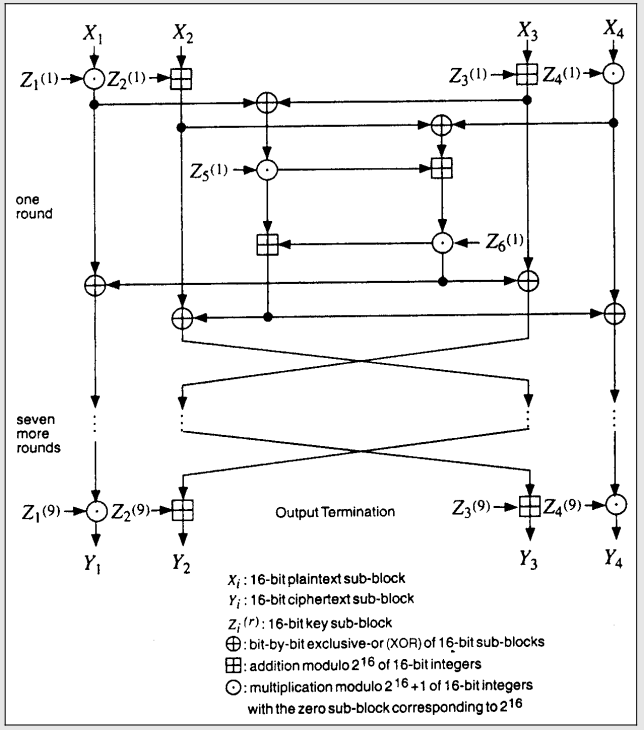
$$R[29] \oplus F(R,K)[15] = K[44] \quad p = 30/64$$

$$R[15] \oplus F(R,K)[7,18,24,29] = K[22] \quad p = 12/64$$

Totaal $p = 0,5 + 1,19 \times 2^{-22} \rightarrow \pm 2^{47}$ paren pt-ct nodig.

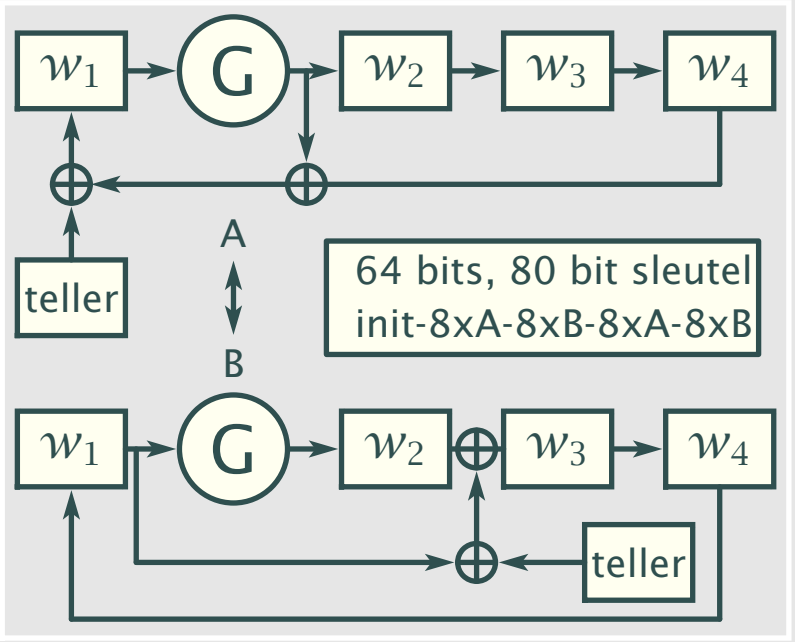
- newDES (Scott, 1985) (geen variant van DES)
- Feal (Shimizu en Miyaguchi, NTT Japan, 1987)
- IDEA (Lai en Massey, ETH Zürich, 1990)
- LOKI (Brown, Pieprzyk, Seberry, Australië, 1990)
- Skipjack (NSA, 1985–1990) *escrowed encryption standard*
- GOST (Gosudarstvennyi Standard Soyuza SSR, USSR)
- Blowfish (Schneier, Counterpane Inc, 1994)
- RC5 (Rivest, RSA Laboratories, 1994)
- TEA (Wheeler en Needham, Univ. Cambridge, 1994)
- enzovoorts, enzovoorts

Alternatieven voor DES

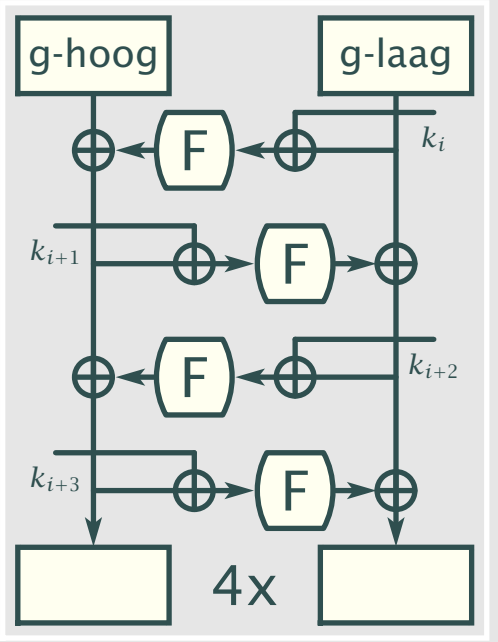


Lai en Massey, ETH Zürich (1990)

- Blok=64 bits, K=128 bits, R8+
- $\oplus$, $\boxplus \bmod 2^{16}$, $\odot \bmod (2^{16}+1)$
- 16 bit units – 16 bit processoren
- cryptoanalyse tot 4–5 rondes
- Daemen (1993) groepen met 2^{23}, 2^{51}, 2^{63} zwakke sleutels

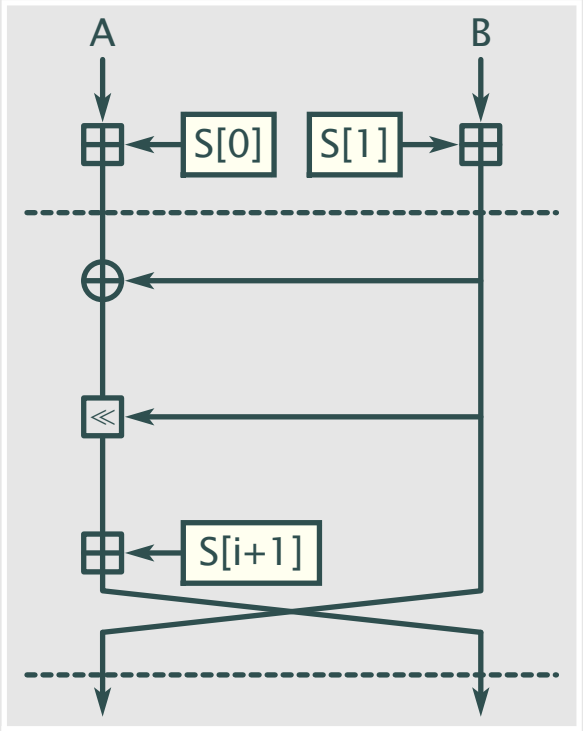


Declassificatie door NSA 1998



G-functie

Skipjack



Rivest, RSA Laboratories (1994)

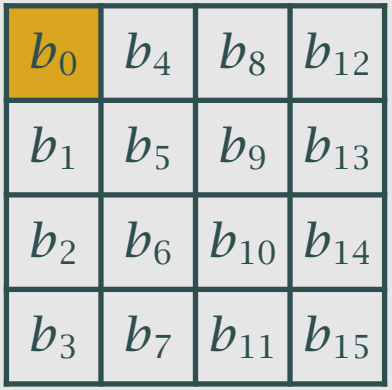
- Afgebeeld is een halve ronde
- RC5-w/r/b parametrisatie:
  blok 2w, 12 rondes, 16 byte sleutel
- $\boxplus / \boxminus$ = plus/minus $\bmod 2^{2w}$
- $\ll$ / $\gg$ = data afhankelijke rotaties
- $K = [0 \ldots b-1] \rightarrow S[0 \ldots 2r+1]$

NIST oproep voor AES 12 sept 1997, programma van eisen:

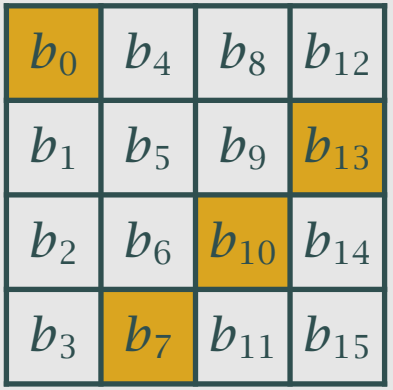
- ongeclassificeerde, publiekelijk bekende algoritme
- overal en zonder royalties beschikbaar
- symmetrisch 128 bits blokgeheimschrift
- sleutel 128, 192, 256 bits naar keuze gebruiker
- efficiënt te implementeren (smartcard b.v.)

Start finale 15 april 1999 met MARS (IBM, Coppersmith), RC6 (RSA Labs, Rivest), RIJNDAEL (Daemen, Rijmen), SERPENT (Anderson, Knudsen, Biham), Twofish (Schneier e.a.)
2 okt 2000 RIJNDAEL winnaar

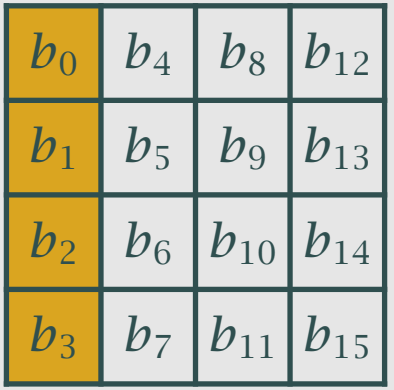
- voorloper is het SQUARE geheimschrift
- geen Feistel geheimschrift maar inverteerbaar door de gekozen (algebraïsche) operaties
- blok/sleutel naar keuze 128/192/256 bits
- whitening-stap voorafgaand aan vercijferrondes
- 10/12/14 rondes met elk 4 fasen:
  - ByteSub
  - ShiftRow
  - MixColumn
  - AddRoundKey



ByteSub



ShiftRow



MixColumn

AddRoundKey: $b'_i = b_i \oplus k_{i,r} \quad r = 1, \ldots, 10/12/14$

Rijndaelschema

- byte $B = (abcdefgh)$ in $GF(2^8)$ is
  $ax^7 + bx^6 + cx^5 + dx^4 + ex^3 + fx^2 + gx + h \quad a, \ldots \in \{0,1\}$
- $B_1 + B_2 = (a_1 + a_2 \bmod 2)x^7 + (b_1 + b_2 \bmod 2)x^6 \ldots$
- $B_1 \times B_2 = (a_1x^7 + \ldots)(a_2x^7 + \ldots) \bmod (x^8 + x^4 + x^3 + x + 1)$
- ByteSub operatie uit twee stappen opgebouwd:
  (1) inverse $B \rightarrow B^{-1}$ en
  (2) lineaire transformatie $M \cdot B + C$
- praktisch: implementeer tabel S[B=0–255] voor ByteSub

- kolommen zijn vectoren (b_0, b_1, b_2, b_3) etc.
- kolomvector als polynoom $b_0x^3 + b_1x^2 + b_2x + b_3$ etc.
- vermenigvuldig met $f = (3x^3 + x^2 + x + 2) \bmod (x^4 + 1)$
  praktisch: vermenigvuldig met (circulant) matrix

$$\begin{pmatrix} b'_0 \\ b'_1 \\ b'_2 \\ b'_3 \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{pmatrix}$$

- voor inverse $f^{-1} = (11x^3 + 13x^2 + 9x + 14) \bmod (x^4 + 1)$

MixColumn

- 128 bits en white + 10 rondes → 1408 subsleutel bytes
- kettingberekening maakt "on the fly" generatie mogelijk
- steeds 4 byte woord $w_i = w_{i-1} \oplus w_{vorige\ ronde}$
- per ronde aanvullende rotatie met ByteSub substitutie en combinatie met rondeteller
- extra bewerkingen bij 256 bit sleutel

AddRoundKey