Cryptografie

http://www.michielstaessen.be/cryptografie

7 mei 2007

Wat is . . .

Codeertheorie coderen om maximale leesbaarheid te garanderen

Cryptografie coderen om boodschap geheim te houden

Enkele begrippen

Plaintext niet-gecodeerd bericht

Ciphertext gecodeerd bericht

symmetrische cryptografie (of conventionele cryptografie)

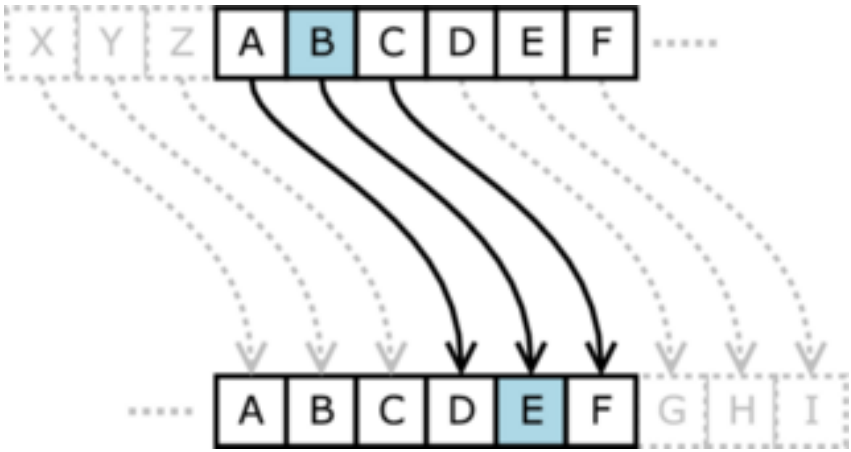
- encyptie = decryptie
- 1 sleutel

asymmetrische cryptografie (of public-key cryptografie)

- encyptie $\neq$ decryptie
- 2 sleutels

Caesarvercijfering

Simpele verschuiving van letters



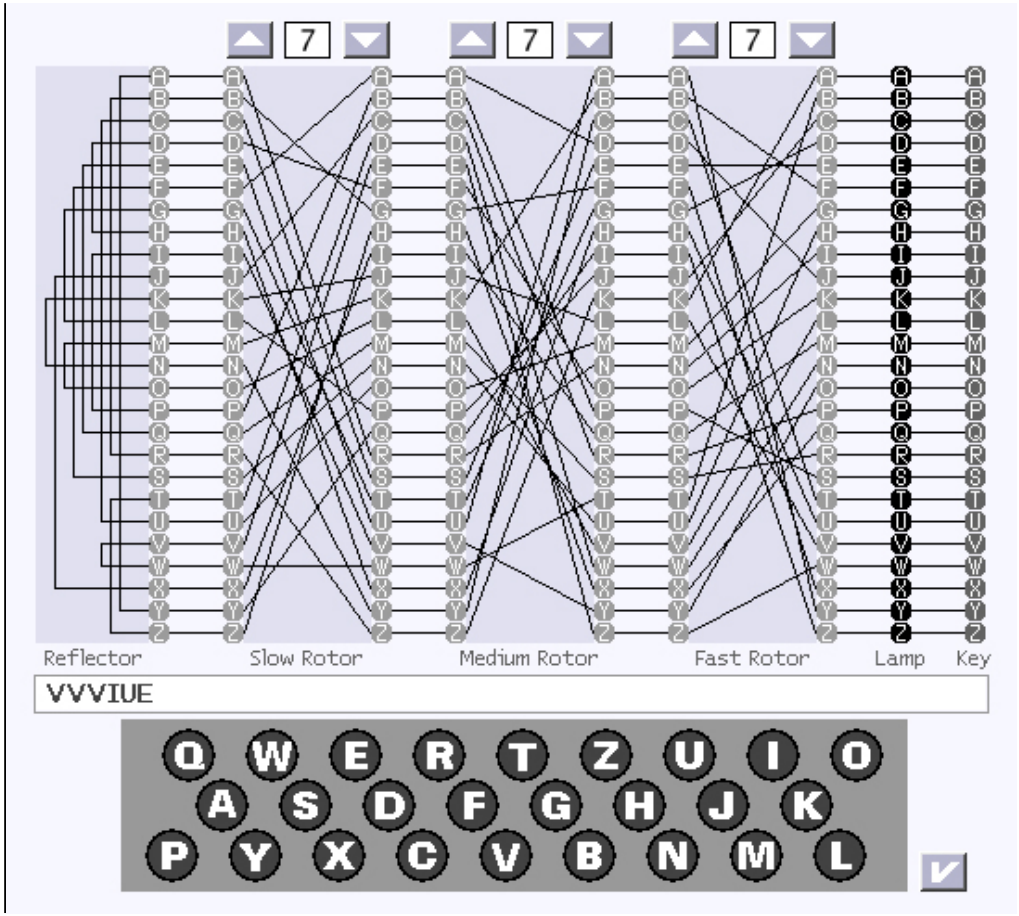
ROT13 Caesarvercijfering met 13 plaatsen

Enkelvoudige substitutie

Elke letter wordt vervangen door een andere letter
$26!$ $(4 \cdot 10^{26})$ mogelijkheden bij gebruik van enkel letters

Enigma

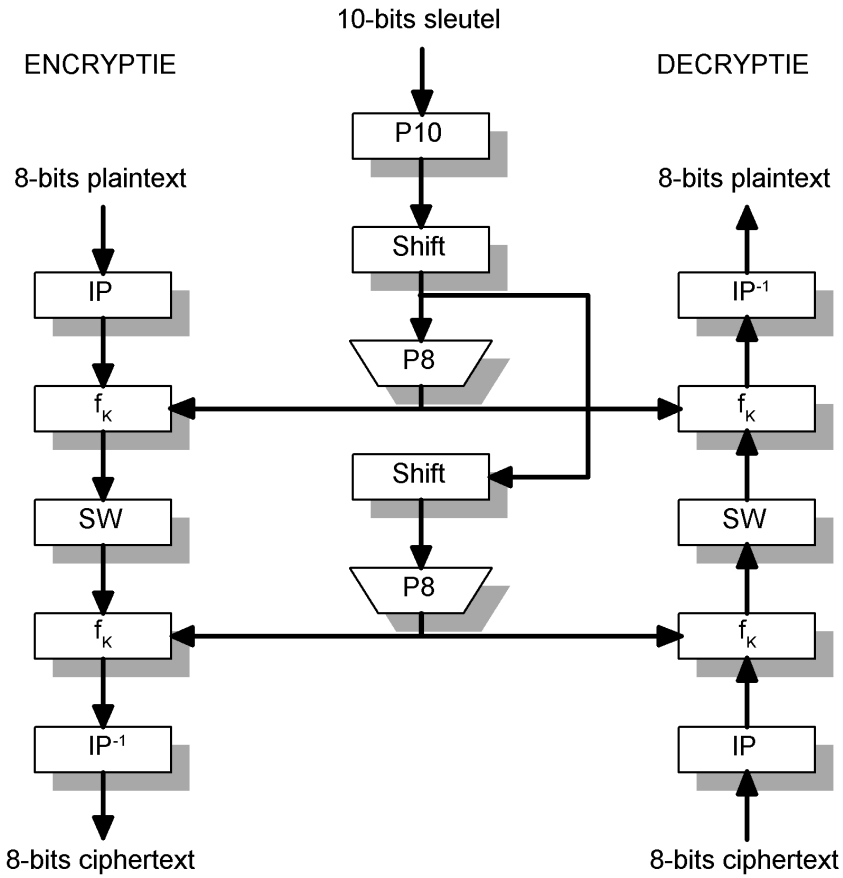

Zur Beachtung!
Q W E R T Z U I O
A S D F G H J K
P Y X C V B N M L

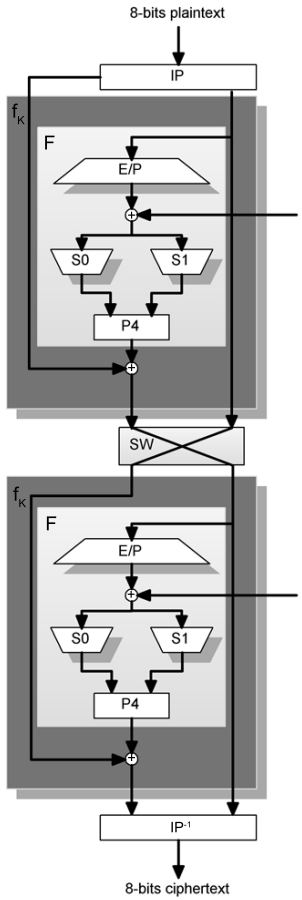

Reflector
Slow Rotor
Medium Rotor
Fast Rotor
Lamp
Key
VVVIUE
Q W E R T Z U I O
A S D F G H J K
P Y X C V B N M L

S-DES, simpele variant van DES

- educatieve variant van DES
- codeert in blokken (8 bits)
- Binaire codering
- 10-bits sleutel (niet veilig!)

Het algoritme





S-DES ontleed: Sleutelgeneratie

1. P10 (Permutatie)
2. Enkele verschuiving naar links per 5 bits
    1. Tweevoudige verschuiving naar links per 5 bits
    2. P8 (Permutatie)
    3. Resultaat: Sleutel 2
3. P8 (Permutatie)
4. Resultaat: Sleutel 1

S-DES ontleed: Sleutelgeneratie

1. P10 (Permutatie)
2. Enkele verschuiving naar links per 5 bits
    1. Tweevoudige verschuiving naar links per 5 bits
    2. P8 (Permutatie)
    3. Resultaat: Sleutel 2
3. P8 (Permutatie)
4. Resultaat: Sleutel 1

S-DES ontleed: Sleutelgeneratie

1. P10 (Permutatie)
2. Enkele verschuiving naar links per 5 bits
    1. Tweevoudige verschuiving naar links per 5 bits
    2. P8 (Permutatie)
    3. Resultaat: Sleutel 2
3. P8 (Permutatie)
4. Resultaat: Sleutel 1

S-DES ontleed: Sleutelgeneratie

1. P10 (Permutatie)
2. Enkele verschuiving naar links per 5 bits
    1. Tweevoudige verschuiving naar links per 5 bits
    2. P8 (Permutatie)
    3. Resultaat: Sleutel 2
3. P8 (Permutatie)
4. Resultaat: Sleutel 1

S-DES ontleed: Sleutelgeneratie

1. P10 (Permutatie)
2. Enkele verschuiving naar links per 5 bits
    1. Tweevoudige verschuiving naar links per 5 bits
    2. P8 (Permutatie)
    3. Resultaat: Sleutel 2
3. P8 (Permutatie)
4. Resultaat: Sleutel 1

S-DES ontleed: Sleutelgeneratie

1. P10 (Permutatie)
2. Enkele verschuiving naar links per 5 bits
    1. Tweevoudige verschuiving naar links per 5 bits
    2. P8 (Permutatie)
    3. Resultaat: Sleutel 2
3. P8 (Permutatie)
4. Resultaat: Sleutel 1

S-DES ontleed: Sleutelgeneratie

1. P10 (Permutatie)
2. Enkele verschuiving naar links per 5 bits
    1. Tweevoudige verschuiving naar links per 5 bits
    2. P8 (Permutatie)
    3. Resultaat: Sleutel 2
3. P8 (Permutatie)
4. Resultaat: Sleutel 1

S-DES ontleed: Codering

1. Beginpermutatie
2. functie f_K met substituties en permutaties
3. splits de invoer in eerste 4 bits (L) en laatste 4 bits (R)
4. Afbeelding F
    1. Expansie/Permutatie
    2. XOR met Sleutel 1
    3. P4 (Permutatie)
5. XOR met L (eerste 4 bits)
6. Verwissel L met R (Switch)
7. herhaal stap 1 tot 5

S-DES ontleed: Codering

1. Beginpermutatie
2. functie f_K met substituties en permutaties
3. splits de invoer in eerste 4 bits (L) en laatste 4 bits (R)
4. Afbeelding F
    1. Expansie/Permutatie
    2. XOR met Sleutel 1
    3. P4 (Permutatie)
5. XOR met L (eerste 4 bits)
6. Verwissel L met R (Switch)
7. herhaal stap 1 tot 5

S-DES ontleed: Codering

1. Beginpermutatie
2. functie f_K met substituties en permutaties
3. splits de invoer in eerste 4 bits (L) en laatste 4 bits (R)
4. Afbeelding F
    1. Expansie/Permutatie
    2. XOR met Sleutel 1
    3. P4 (Permutatie)
5. XOR met L (eerste 4 bits)
6. Verwissel L met R (Switch)
7. herhaal stap 1 tot 5

S-DES ontleed: Codering

1. Beginpermutatie
2. functie f_K met substituties en permutaties
3. splits de invoer in eerste 4 bits (L) en laatste 4 bits (R)
4. Afbeelding F
    1. Expansie/Permutatie
    2. XOR met Sleutel 1
    3. P4 (Permutatie)
5. XOR met L (eerste 4 bits)
6. Verwissel L met R (Switch)
7. herhaal stap 1 tot 5

S-DES ontleed: Codering

1. Beginpermutatie
2. functie f_K met substituties en permutaties
3. splits de invoer in eerste 4 bits (L) en laatste 4 bits (R)
4. Afbeelding F
   1. Expansie/Permutatie
   2. XOR met Sleutel 1
   3. P4 (Permutatie)
5. XOR met L (eerste 4 bits)
6. Verwissel L met R (Switch)
7. herhaal stap 1 tot 5

S-DES ontleed: Codering

1. Beginpermutatie
2. functie f_K met substituties en permutaties
3. splits de invoer in eerste 4 bits (L) en laatste 4 bits (R)
4. Afbeelding F
   1. Expansie/Permutatie
   2. XOR met Sleutel 1
   3. P4 (Permutatie)
5. XOR met L (eerste 4 bits)
6. Verwissel L met R (Switch)
7. herhaal stap 1 tot 5

S-DES ontleed: Codering

1. Beginpermutatie
2. functie f_K met substituties en permutaties
3. splits de invoer in eerste 4 bits (L) en laatste 4 bits (R)
4. Afbeelding F
   1. Expansie/Permutatie
   2. XOR met Sleutel 1
   3. P4 (Permutatie)
5. XOR met L (eerste 4 bits)
6. Verwissel L met R (Switch)
7. herhaal stap 1 tot 5

S-DES ontleed: Codering

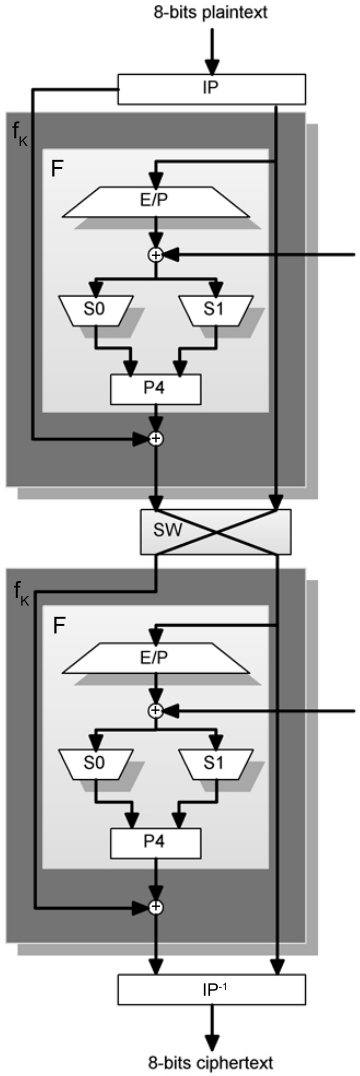
1. Beginpermutatie
2. functie f_K met substituties en permutaties
3. splits de invoer in eerste 4 bits (L) en laatste 4 bits (R)
4. Afbeelding F
   1. Expansie/Permutatie
   2. XOR met Sleutel 1
   3. P4 (Permutatie)
5. XOR met L (eerste 4 bits)
6. Verwissel L met R (Switch)
7. herhaal stap 1 tot 5

S-DES ontleed: Codering

1. Beginpermutatie
2. functie f_K met substituties en permutaties
3. splits de invoer in eerste 4 bits (L) en laatste 4 bits (R)
4. Afbeelding F
   1. Expansie/Permutatie
   2. XOR met Sleutel 1
   3. P4 (Permutatie)
5. XOR met L (eerste 4 bits)
6. Verwissel L met R (Switch)
7. herhaal stap 1 tot 5

S-DES ontleed: Codering

1. Beginpermutatie
2. functie f_K met substituties en permutaties
3. splits de invoer in eerste 4 bits (L) en laatste 4 bits (R)
4. Afbeelding F
   1. Expansie/Permutatie
   2. XOR met Sleutel 1
   3. P4 (Permutatie)
5. XOR met L (eerste 4 bits)
6. Verwissel L met R (Switch)
7. herhaal stap 1 tot 5


8-bits plaintext
IP
f_K
F
E/P
S0
S1
P4
SW
f_K
F
E/P
S0
S1
P4
IP^{-1}
8-bits ciphertext

Verschillen met DES

S-DES	DES
blokken van 8 bits	blokken van 64 bits
10-bits sleutel	56-bits sleutel
2 ronden ($2 \times f_K$)	16 ronden

Priem/Relatief Priem

Een getal is een priemgetal als het slechts twee delers heeft: 1 en zichzelf.

Twee getallen zijn relatief priem ten opzichte van elkaar als en slechts als ze grootste gemene deler 1 hebben.

Definitie

We bekijken de deling: $\frac{A(X)}{D(X)}$

We verkrijgen bij deze deling:

- quotiënt $Q(X)$
- rest $R(X)$

Een modulobewerking geeft de rest na deling door de modulo.

Voorbeeld: $10 \equiv 3 \bmod 7$

Stelling van Fermat

$\forall\ a \in \mathbb{N}$ en p een priemgetal:

$$a^{p-1} \equiv 1 \bmod p \tag{1}$$

De Phi-functie

$\phi(n)$ geeft het **aantal** getallen, kleiner dan n, die relatief priem zijn met n.

Voor priemgetallen:

$$\phi(p) = p - 1 \tag{2}$$

Eigenschap

Voor twee priemgetallen p en q:

$$\begin{aligned} \phi(pq) &= \phi(p) \times \phi(q) && (3) \\ &= (p-1) \times (q-1) && (4) \end{aligned}$$

Stelling van Euler

$\forall\ a,\ n > 0$:

$$a^{\phi(n)} \equiv 1 \bmod n \tag{5}$$

Sleuteluitwisseling

Hash-functies

RSA-codering: werking

Enkele waarheden:

- $e \cdot \frac{1}{e} = e \cdot e^{-1} = 1$
- $M^{e \cdot e^{-1}} = M^1 = M$
- $M^{e \cdot e^{-1}} \bmod n = M^1 \bmod n = M \bmod n$

Stel $d = e^{-1}$

$M = M^{ed} \bmod n$

RSA-codering: werking

Enkele waarheden:

- $e \cdot \frac{1}{e} = e \cdot e^{-1} = 1$
- $M^{e \cdot e^{-1}} = M^1 = M$
- $M^{e \cdot e^{-1}} \bmod n = M^1 \bmod n = M \bmod n$

Stel $d = e^{-1}$

$M = M^{ed} \bmod n$

RSA-codering: werking

Enkele waarheden:

- $e \cdot \frac{1}{e} = e \cdot e^{-1} = 1$
- $M^{e \cdot e^{-1}} = M^1 = M$
- $M^{e \cdot e^{-1}} \bmod n = M^1 \bmod n = M \bmod n$

Stel $d = e^{-1}$

$M = M^{ed} \bmod n$

RSA-codering: Waarom werkt het?

RSA-codering: samenvatting

Ingrediënten

- Twee priemgetallen p en q (Privaat)
- $n = pq$ (Publiek)
- e zodat ggd$(e, \phi(n)) = 1$ en $1 < e < \phi(n)$ (Publiek)
- $d \equiv e^{-1} \bmod n$ (Privaat)