I. AES— Rijndael

Rijndael - Internal Structure

Rijndael is an iterated block cipher with variable length block and variable key size. The number of rounds is defined by the table:

	Nb = 4	Nb = 6	Nb = 8
Nk = 4	10	12	14
Nk = 6	12	12	14
Nk = 8	14	14	14

Nb = length of data block in 32-bit words

Nk = length of key in 32-bit words

Rijndael - Internal Structure

- First Initial Round Key Addition
- 9 rounds, numbered 1-9, each consisting of
  - Byte Substitution transformation
  - Shift Row transformation
  - Mix Column transformation
  - Round Key Addition
- A final round (round 10) consisting of
  - Byte Substitution transformation
  - Shift Row transformation
  - Final Round Key Addition

Rijndael - Inverse Structure

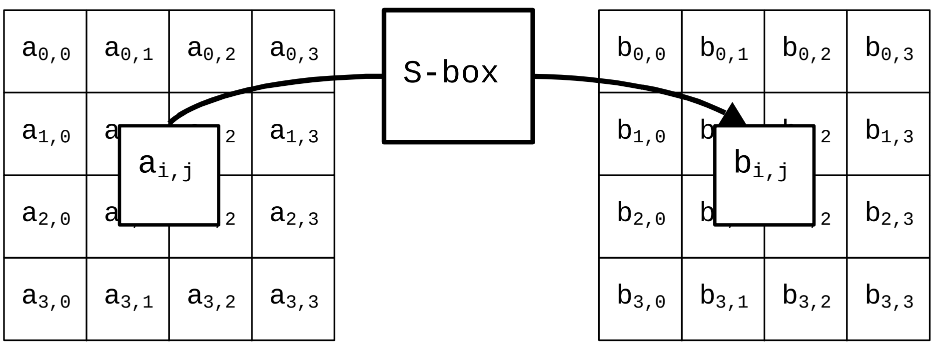
ENCRYPT (2 rounds)	DECRYPT (2 rounds)	→ INV ENCRYPT (2 rounds)
Initial Round Key Add	Final Round Key Add	Inv Initial Round Key Add
Byte Substitution	Inv Shift Row	Inv Byte Substitution
Shift Row	Inv Byte Substitution	Inv Shift Row
Mix Column	Round Key Addition	Inv Mix Column
Round Key Addition	Inv Mix Column	Inv Round Key Addition
Byte Substitution	Inv Shift Row	Inv Byte Substitution
Shift Row	Inv Byte Substitution	Inv Shift Row
Final Round Key Add	Initial Round Key Add	Inv Final Round Key Add

Rijndael-128 State and 128 Cipher Key

$a_{0,0}$	$a_{0,1}$	$a_{0,2}$	$a_{0,3}$
$a_{1,0}$	$a_{1,1}$	$a_{1,2}$	$a_{1,3}$
$a_{2,0}$	$a_{2,1}$	$a_{2,2}$	$a_{2,3}$
$a_{3,0}$	$a_{3,1}$	$a_{3,2}$	$a_{3,3}$

$k_{0,0}$	$k_{0,1}$	$k_{0,2}$	$k_{0,3}$
$k_{1,0}$	$k_{1,1}$	$k_{1,2}$	$k_{1,3}$
$k_{2,0}$	$k_{2,1}$	$k_{2,2}$	$k_{2,3}$
$k_{3,0}$	$k_{3,1}$	$k_{3,2}$	$k_{3,3}$

Byte Substitution



Rijndael S-box

Sbox[256] = {

```
 99,124,119,123,242,107,111,197, 48,  1,103, 43,254,215,171,118,
202,130,201,125,250, 89, 71,240,173,212,162,175,156,164,114,192,
183,253,147, 38, 54, 63,247,204, 52,165,229,241,113,216, 49, 21,
  4,199, 35,195, 24,150,  5,154,  7, 18,128,226,235, 39,178,117,
  9,131, 44, 26, 27,110, 90,160, 82, 59,214,179, 41,227, 47,132,
 83,209,  0,237, 32,252,177, 91,106,203,190, 57, 74, 76, 88,207,
208,239,170,251, 67, 77, 51,133, 69,249,  2,127, 80, 60,159,168,
 81,163, 64,143,146,157, 56,245,188,182,218, 33, 16,255,243,210,
 96,129, 79,220, 34, 42,144,136, 70,238,184, 20,222, 94, 11,219,
224, 50, 58, 10, 73,  6, 36, 92,194,211,172, 98,145,149,228,121,
231,200, 55,109,141,213, 78,169,108, 86,244,234,101,122,174,  8,
186,120, 37, 46, 28,166,180,198,232,221,116, 31, 75,189,139,138,
112, 62,181,102, 72,  3,246, 14, 97, 53, 87,185,134,193, 29,158,
225,248,152, 17,105,217,142,148,155, 30,135,233,206, 85, 40,223,
140,161,137, 13,191,230, 66,104, 65,153, 45, 15,176, 84,187, 22};
```


Rijndael S-box Design View

Galois field GF(2^8) with polynomial

$$m(x) = x^8 + x^4 + x^3 + x + 1$$

The Rijndael S-box is the composition $f \circ g$ where

$g(x) = x^{-1}$, $x \in GF(2^8)$, $x \neq 0$, and

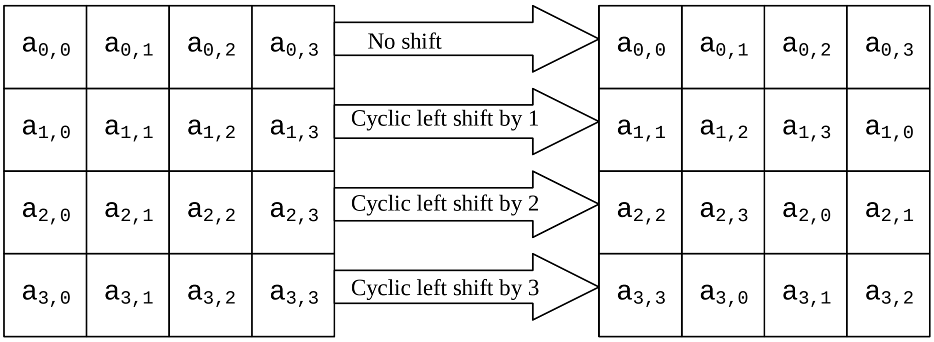
$g(0) = 0$

Inv ($f \circ g$) = $g \circ$ (Inv f)

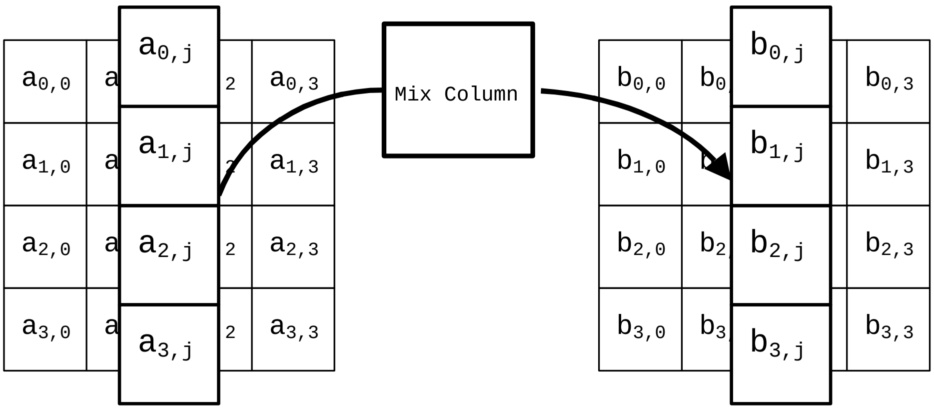
and f is the affine transformation defined by y = f(x)

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

Shift Row



Mix Column



Mix Column - Implemented

The mix column transformation mixes one column of the state at a time.

Column j:

$$
\begin{aligned}
b_{0,j} &= T_2(a_{0,j}) \oplus T_3(a_{1,j}) \oplus a_{2,j} \oplus a_{3,j}\\
b_{1,j} &= a_{0,j} \oplus T_2(a_{1,j}) \oplus T_3(a_{2,j}) \oplus a_{3,j}\\
b_{2,j} &= a_{0,j} \oplus a_{1,j} \oplus T_2(a_{2,j}) \oplus T_3(a_{3,j})\\
b_{3,j} &= T_3(a_{0,j}) \oplus a_{1,j} \oplus a_{2,j} \oplus T_2(a_{3,j})
\end{aligned}
$$

where:

$$
\begin{aligned}
T_2(a) &= 2*a && \text{if } a < 128\\
T_2(a) &= (2*a) \oplus 283 && \text{if } a \geq 128\\
T_3(a) &= T_2(a) \oplus a.
\end{aligned}
$$

Mix Column - Design view

The columns of the State are considered as polynomials over $GF(2^8)$.

They are multiplied by a fixed polynomial $c(x)$ given by

$$c(x) = \text{'03'}\, x^3 + \text{'01'}\, x^2 + \text{'01'}\, x + \text{'02'}$$

The product is reduced modulo $x^4 + \text{'01'}$.

Matrix form

$$
\begin{bmatrix} b_{0,j}\\ b_{1,j}\\ b_{2,j}\\ b_{3,j} \end{bmatrix} =
\begin{bmatrix} 02 & 03 & 01 & 01\\ 01 & 02 & 03 & 01\\ 01 & 01 & 02 & 03\\ 03 & 01 & 01 & 02 \end{bmatrix}
\begin{bmatrix} a_{0,j}\\ a_{1,j}\\ a_{2,j}\\ a_{3,j} \end{bmatrix}
$$

The Inverse Mix Column polynomial is $c(x)^{-1} \bmod (x^4 + \text{'01'}) = d(x)$ given by

$$d(x) = \text{'0B'}\, x^3 + \text{'0D'}\, x^2 + \text{'09'}\, x + \text{'0E'}$$

AES salaamisfunktio

tila $x^{(r)} = (x_{ij}^{(r)}), \quad i,j = 0,1,2,3, \quad r = 1,2,\ldots,10, \quad x_{ij}^{(r)} \in GF(2^8)$

avain $k^{(r)} = (k_{ij}^{(r)}), \quad i,j = 0,1,2,3, \quad r = 0,1,2,\ldots,10, \quad k_{ij}^{(r)} \in GF(2^8)$

AES operaatio:

$$x^{(1)} = p \oplus k^{(0)}$$

$$x^{(r+1)} = M(S(F(G(x^{(r)}))) \oplus k^{(r)}, \ r = 1,2,\ldots,9$$

$$c = S(F(G(x^{(10)}))) \oplus k^{(10)}$$

missä

M, S ovat lineaarisia funktioita kerroinkunnan $GF(2^8)$ suhteen

$G = (g)$ missä $g : GF(2^8) \to GF(2^8), \ g(x) = x^{-1}, \ g(0) = 0$

$F = (f)$ missä $f - \lambda_0$ on additiivinen funktio kunnassa $GF(2^8)$

Linearisoitu polynomi

Murphy-Robshaw 2002:

f :n esitys linearisoituna polynomina

$$f(x) = \lambda_0 + \sum_{l=0}^{7} \lambda_{l+1} x^{2^l}$$

missä kertoimet λ_l ja kaikki laskutoimitukset kunnassa $GF(2^8)$

Murphy ja Robshaw upottivat AES:n kahdeksan kertaa suurempaan BES algoritmiin, jonka tilavektorissa 8×16 tavua, upotuskuvauksella

$$\phi(x) = (x, x^2, x^{2^2}, \ldots, x^{2^7}), \quad x \in GF(2^8)$$

Eräs AES yhtälösysteemi

$$0 = x_{ij}^{(1)} + p_{ij} + k_{ij}^{(0)}$$

$r = 1,2,\ldots,10:$

$$0 = y_{ij}^{(r)} x_{ij}^{(r)} + 1$$

$$0 = y_{ij0}^{(r)} + y_{ij}^{(r)}$$ (merkintä!)

$$0 = y_{ijl}^{(r)} + (y_{ij,l-1}^{(r)})^2, \quad l = 1,\ldots,7$$ konjugointi

$$0 = z_{ij}^{(r)} + \sum_{l=0}^{7} \lambda_{l+1} y_{ijl}^{(r)} + \lambda_0$$

$r \neq 10:$

$$0 = x_{ij}^{(r+1)} + \sum_{m,n=0}^{3} \alpha_{ij,mn} z_{mn}^{(r)} + k_{ij}^{(r)}$$

$$0 = c_{ij} + \sum_{m,n=0}^{3} \beta_{ij,mn} z_{mn}^{(10)} + k_{ij}^{(10)}$$

AES yhtälösysteemit

Tässä yhtälöryhmässä

- $80 \times 16 = 1280$ kvadraattista yhtälöä
- $21 \times 16 = 336$ lineaarista yhtälöä
- yhteensä 1616 yhtälöä
- 1600 tuntematonta tilamuuttujaa
- 176 tuntematonta avainmuuttujaa (johdettu 16 perusmuuttujasta)
- avainten johtaminen kuvattavissa samanlaisella yhtälöryhmällä
- ei näyttäisi olevan ylimääritelty (overdefined)

Murphy-Robshaw yhtälöryhmä:

- yhteensä 5280 yhtälöä, joista 3840 kvadraattista
- 2560 tilamuuttujaa ja 1408 ($= 8 \times 176$) avainmuuttujaa
- avainsysteemissä 2560 yhtälöä, joista 960 kvadraattista ja siinä on yhteensä 2048 tuntematonta
- ylimääritelty

Yhtälöryhmän ratkaisusta

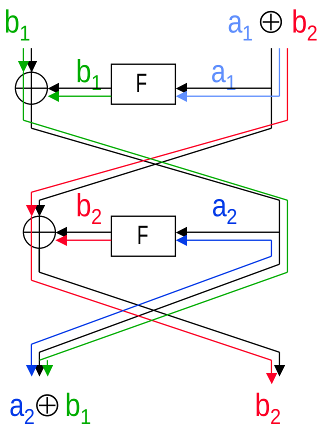
Laskennallinen algebra

- Uusia tehokkaita menetelmiä polynomiyhtälöryhmien ratkaisemiseksi
- Gröbnerin kannat
- Algoritmeja
  - Buchberger 1965, 1979, 1985
  - Faugère-Gianni-Lazard-Mora (FGLM) 1993
  - F4, F5,...
- Algoritmien kompleksisuus ei tunnettu
- Jos ratkaisua ei löydy, niin ratkaisun kompleksisuutta ei pystytä määrittämään.
- Useita jonosalausalgoritmeja ratkaistu (murrettu).
- AES ei ole ratkennut.

Uusi testi ja suunnittelukriteeri symmetrisille salaamisalgoritmeille.

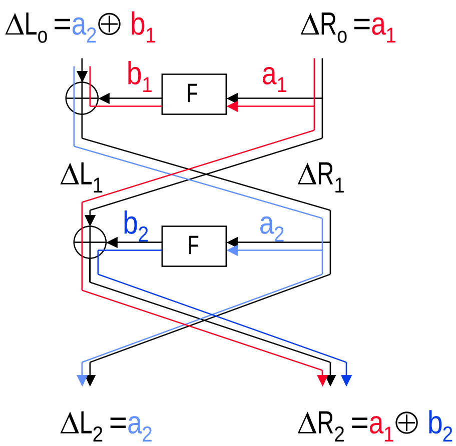
2. Linear and differential cryptanalysis for Feistel ciphers

Principles of Linear Cryptanalysis 4



Next we shall determine the probability of the two round linear approximation given the probabilities $r(a_1,b_1)$ and $r(a_2,b_2)$. For that purpose we prove the following result.

Feistel salaajan differentiaalinen kryptoanalyysi



Todennäköisyys $\approx p(a_1,b_1)\, p(a_2,b_2)$,

Tällainen todennäköinen relaatio on *differentiaalinen karakteristika*.

Feistel salaaja – Bijektiivinen kierrosfunktio:
Viiden kierroksen mahdoton differentiaalinen karakteristika

F bijektio

$\alpha \neq 0$

$\Downarrow$

$\beta \neq 0$

$\Downarrow$

$\gamma \neq 0$