5.2. The Advanced Encryption Standard (AES)

Sept. 1997: NIST put out a call for a succ. of DES

Requirements: Block length 128 bits, support of key length 128, 192, 256 bits

Deadline: June 98

21 submitted proposals. After 3 AES-conferences Rijndael (authors Daemen & Rijmen, Leuven, Belgium) was chosen.

The ~~fin~~ 5 finalists were

MARS (IBM), RC6 (RSA), Rijndael (s.a.)

Serpent (Biham et. al.), Twofish (Schneier et. al.)

All are very strong.

Computations are mainly in the field $\mathbb{F}_{2^8} = GF(2^8)$.

[see ff. pages: A, B, C, -2-]

5.2.1. AES encryption

AES has r rounds, numbered $1, \ldots, r$,

and needs $r+1$ round keys $K_0, K_1, \ldots, K_r$,

each of length 128 bits.

$K_0, \ldots, K_r$ are derived from master key K. → later

The no. of rounds depends on the key size

key size	128	→	10	rounds
	192	→	12	
	256	→	14	

Fields

A triple $(\mathcal{X}, +, \cdot)$ with operations $+, \cdot : \mathcal{X} \times \mathcal{X} \to \mathcal{X}$ is called a *field* if the following conditions hold:

- $\mathcal{X}$ with operation "+" forms an Abelian group, i.e.,

  $\exists$ *neutral element* "0": $a + 0 = 0 + a = a$ for all $a \in \mathcal{X}$

  $\exists$ *inverse elements:* $a + (-a) = (-a) + a = 0$ for all $a \in \mathcal{X}$

  Associativity: $a + (b + c) = (a + b) + c$ for all $a, b, c \in \mathcal{X}$

  Commutativity: $a + b = b + a$ for all $a, b \in \mathcal{X}$

- $\mathcal{X} \setminus \{0\}$ with operation "$\cdot$" forms an Abelian group with neutral element "1".

- *Distributivity* holds:

$$(a + b) \cdot c = a \cdot c + b \cdot c \text{ for all } a, b, c \in \mathcal{X}$$

Fields

Example GF(2): $\mathcal{X} = \{0, 1\}$

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Example GF(4): $\mathcal{X} = \{x_1, x_2, x_3, x_4\}$

$+$	x_0	x_1	x_2	x_3
x_0	x_0	x_1	x_2	x_3
x_1	x_1	x_0	x_3	x_2
x_2	x_2	x_3	x_0	x_1
x_3	x_3	x_2	x_1	x_0

$\cdot$	x_0	x_1	x_2	x_3
x_0	x_0	x_0	x_0	x_0
x_1	x_0	x_1	x_2	x_3
x_2	x_0	x_2	x_3	x_1
x_3	x_0	x_3	x_1	x_2

Theorem. There exists a finite field of order m if and only if $m = p^t$ for some prime p and power $t \in \mathbb{N}$.
Construction by polynomials over GF(p).

AES - Encryption

Most computations are in the field

$$\begin{aligned} F_{2^8} &= GF(2^8) \\ &= \{b_7x^7 + b_6x^6 + \cdots + b_1x + b_0 \mid b_i \in GF(2)\} \\ &= \{(b_7, b_6, \ldots, b_1, b_0) \mid b_i \in GF(2)\} \end{aligned}$$

Set of polynomials with coefficients from $F_2 = GF(2)$.

Addition:

Addition of polynomial coefficients.

Multiplication:

Multiplication of polynomials and taking the remainder modulo $q(x) = (x^8 + x^4 + x^3 + x + 1)$.

RWTH AACHEN UNIVERSITY

Example.

$$(1101\,0101)\cdot(1100\,0001) = (10111101)$$

$$= (y^7+y^6+y^4+y^2+1)(y^7+y^6+1)$$

$$\cancel{=}(y^{14}+y^{12}+y^{11}+y^{10}+y^9+y^8+y^4+y^2+1) : (y^8+y^4+y^3+y+1) = y^6+y^4+y^3$$

$$\begin{array}{l} y^{14}+ \quad y^{10}+y^9 \quad +y^7+y^6 \\ \hline y^{12}+y^{11} \quad +y^8+y^7+y^6+y^4+y^2+1 \\ \quad \ddots \\ \hline y^7+y^5+y^4+y^3+y^2+1 \end{array}$$

Thinking the Future
Zukunft denken

Plaintext of 128 bits, arranged as a 4x4 byte matrix (columnwise)

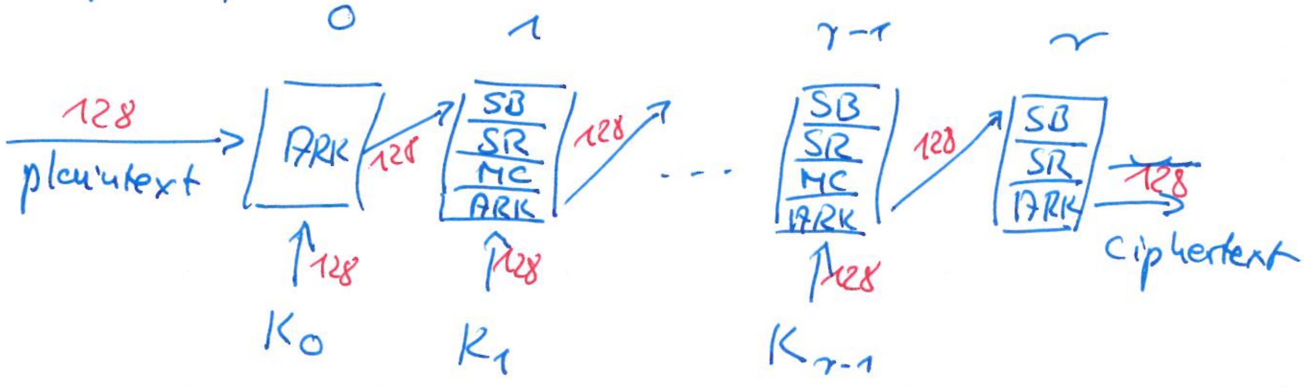
$$\begin{pmatrix} b_{00} & \cdots & b_{03} \\ \vdots & & \vdots \\ b_{30} & \cdots & b_{33} \end{pmatrix}$$

The round keys are also organized as 4x4 byte matrix.

Encryption uses the following operations

- AddRoundKey (ARK)
- Round $1, \ldots, r-1$, consists of "layers"
  - SubBytes (SB)
  - ShiftRows (SR)
  - MixColumns (MC)
  - AddRoundKey (ARK)
- Round r: SB, SR, ARK

Graphically



SubBytes

Each byte $f = (b_7, \dots, b_0) \triangleq b_7 x^7 + \dots + b_1 x + b_0 \in \mathbb{F}_{2^8}$

1. Compute f^{-1} in $\mathbb{F}_{2^8}$, let $f^{-1} = (y_7, \dots, y_0)$
2. Affine transformation

$$\begin{pmatrix} z_0 \\ \vdots \\ \vdots \\ z_7 \end{pmatrix} = \begin{pmatrix} 1 & 0 & \cdots & 1 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} \begin{pmatrix} y_0 \\ \vdots \\ y_7 \end{pmatrix} + \begin{pmatrix} 1 \\ \vdots \\ 0 \end{pmatrix}$$ (see lect. notes)

Replace $(b_7, \dots, b_0)$ by $(z_7, \dots, z_0)$

Implementation by a look-up table, the S-box

Input: $(b_7, \dots, b_0)$

Output: $\mathrm{bin}\left(S_{(b_7 \dots b_4)(b_3 \dots b_0)} \right)$

Example: Input $(\underbrace{1\,0\,0\,0}_{8} | \underbrace{1\,0\,1\,1}_{11})$

$$S_{8,11} = 61_z = (0\,0\,1\,1\;1\,1\,0\,1)$$

ShiftRows

Rows are cyclically shifted as

$$\begin{pmatrix} b_{00} & \cdots & b_{03} \\ \vdots & & \vdots \\ b_{30} & \cdots & b_{33} \end{pmatrix} \to \begin{pmatrix} b_{00} & b_{01} & b_{02} & b_{03} \\ b_{11} & b_{12} & b_{13} & b_{10} \\ b_{22} & b_{23} & b_{20} & b_{21} \\ b_{33} & b_{30} & b_{31} & b_{32} \end{pmatrix} = \begin{pmatrix} c_{00} & \cdots & c_{03} \\ \vdots & & \vdots \\ c_{30} & \cdots & c_{33} \end{pmatrix}$$

MixColumns

Regard each c_{ij} as an element of $\mathbb{F}_{2^8}$.

Apply a linear transformation

$$\underbrace{\begin{pmatrix} 00\,00\,00\,10 & \cdots & 00\,00\,00\,01 \\ \vdots & & \vdots \\ 00\,00\,00\,11 & \cdots & 00\,00\,00\,10 \end{pmatrix}}_{A} \begin{pmatrix} c_{00} & \cdots & c_{03} \\ \vdots & & \vdots \\ c_{30} & \cdots & c_{33} \end{pmatrix} = \begin{pmatrix} d_{00} & \cdots & d_{03} \\ \vdots & & \vdots \\ d_{30} & \cdots & d_{33} \end{pmatrix}$$

A may be written as a "circulant"

$$A = \begin{pmatrix} x & x+1 & 1 & 1 \\ 1 & x & x+1 & 1 \\ 1 & 1 & x & x+1 \\ x+1 & 1 & 1 & x \end{pmatrix}$$

AddRoundKey

Bitwise addition modulo 2

$$\begin{pmatrix} d_{00} & \cdots & d_{03} \\ \vdots & & \vdots \\ d_{30} & \cdots & d_{33} \end{pmatrix} \oplus \begin{pmatrix} k_{00} & \cdots & k_{03} \\ \vdots & & \vdots \\ k_{30} & \cdots & k_{33} \end{pmatrix} = \begin{pmatrix} e_{00} & \cdots & e_{03} \\ \vdots & & \vdots \\ e_{30} & \cdots & e_{33} \end{pmatrix}.$$

5.2.2. AES Key Expansion

(only for length 128, similar for 192, 256 bits)

Master key $K = K_0$, 128 bits, 4x4 matrix of bytes

columns $W(0), W(1), W(2), W(3)$

Expanded by 40 more columns

$$W(i) = \begin{cases} W(i-4) \oplus W(i-1), & \text{if } i \not\equiv 0 \pmod 4 \\ W(i-4) \oplus T(W(i-1)), & \text{if } i \equiv 0 \pmod 4 \end{cases}$$

$i = 4, \dots, 43$

Transformation $T(W(i-1))$, $W(i-1) = \begin{pmatrix} w_0 \\ w_1 \\ w_2 \\ w_3 \end{pmatrix}$:

1. Cyclic shift: $(w_0, w_1, w_2, w_3) \to (w_1, w_2, w_3, w_0) = (u_0, \dots, u_3)$
2. Apply SubBytes to each $u_i \mapsto (v_0, v_1, v_2, v_3)$
3. Compute $p(i) = (00\ 00\ 00\ 10)^{i/4 - 1}$ in $\mathbb{F}_{2^8}$.
4. $T(W(i-1)) = (v_0 \oplus p(i), v_1, v_2, v_3)$

Round key for round k:

$$(W(4k), W(4k+1), W(4k+2), W(4k+3)), \quad k = 1, \dots, 10$$

5.2.3. AES Decryption

Each of the steps SB, SR, MC, ARK is invertible, giving the transformation

- InvSubBytes (ISB)
- Inv ShiftRows (ISR)
- InvMixColumns (IMC)
- AddRoundKey (ARK)

These operations are applied in reverse order.