RWTH AACHEN UNIVERSITY

5.2.1. AES Encryption

AES consists of r rounds, numbered $1, \dots, r$ and $r+1$ round keys $K_0, K_1, \dots, K_r$, each of length 128 bits. $K_0, \dots, K_r$ are derived from master key K, as described later.

The no of rounds depends on the key size

key size		no of rounds
128	$\rightarrow$	10
192	$\rightarrow$	12
256	$\rightarrow$	14

Plaintext m of 128 bits (otherwise chop) arranged as a 4x4 matrix of bytes

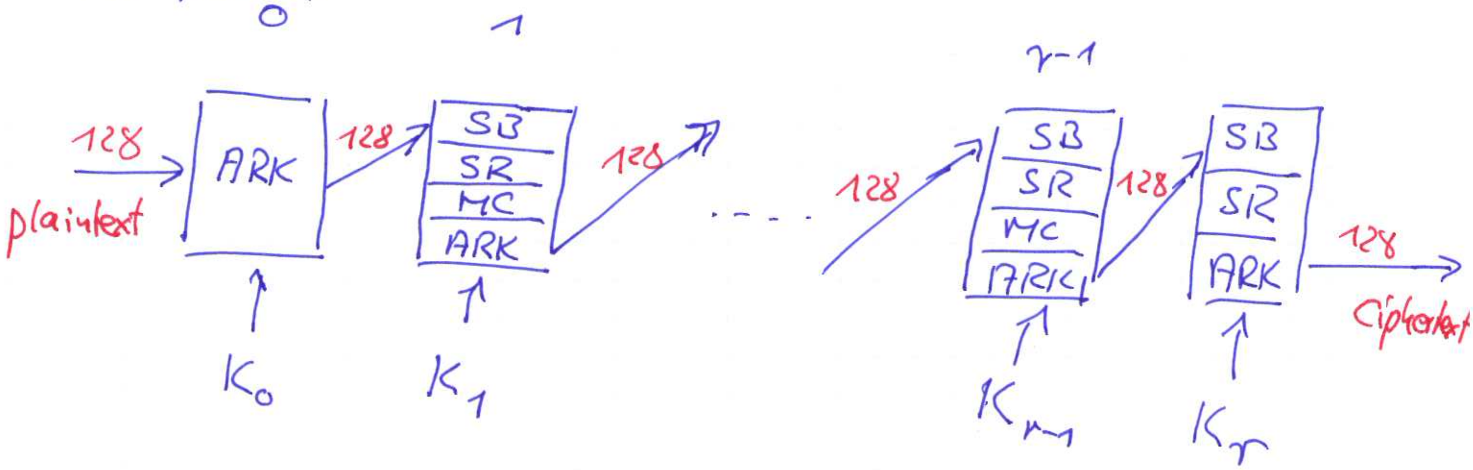
$$\begin{pmatrix} b_{0,0} & b_{0,1} & b_{0,2} & b_{0,3} \\ b_{10} & b_{11} & b_{12} & b_{13} \\ b_{20} & b_{21} & b_{22} & b_{23} \\ b_{30} & b_{31} & b_{32} & b_{33} \end{pmatrix}$$

The round keys are also arranged as 4x4 byte matrices.

Encryption uses the following operations

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

Graphically:



Description of the layers in detail.

RWTH AACHEN UNIVERSITY

SubBytes (Bytes substitution)

Each byte $f = (b_7, \ldots, b_0)$ is viewed as

$b_7 y^7 + b_6 y^6 + \ldots + b_0 \in \mathbb{F}_{2^8}$

1. Compute f^{-1} in $\mathbb{F}_{2^8}$, let $f^{-1} = (y_7, \ldots, y_0)$
(set $0^{-1} := 0$)

2. Affine transformation

$$\begin{pmatrix} z_0 \\ \vdots \\ z_7 \end{pmatrix} = \begin{pmatrix} 1 & 0 & \cdots & 1 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} \begin{pmatrix} y_0 \\ \vdots \\ y_7 \end{pmatrix} + \begin{pmatrix} 1 \\ \vdots \\ 0 \end{pmatrix}$$

Replace $(b_7, \ldots, b_0)$ by $(z_7, \ldots, z_0)$.

Implementation by a lookup table, so called

$$\text{S-Box} \quad \begin{array}{c|ccc|} & 0 & \cdots & 15 \\ \hline 0 & 99 & & 118 \\ \vdots & \vdots & & \vdots \\ 15 & 140 & - & 22 \\ \hline \end{array} = (s_{ij})_{0 \le i,j \le 15}$$

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

Output: $\mathrm{bin}\left(s_{(b_7 \ldots b_4),(b_3 \ldots b_0)}\right)$ (don't leave out leading zeros)

Ex. Input $(\underbrace{1000}_{8} \mid \underbrace{1011}_{11})$

Look up $s_{8,11} = 61$, output

$(z_7, \ldots, z_0) = \mathrm{bin}(61) = (0011\ 1101)$.

Thinking the Future
Zukunft denken

Shift Rows

Rows are cyclically shifted

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

Mix Columns

Regard each byte c_{ij}, $0 \le i,j \le 3$, as an element of $\mathbb{F}_{2^8}$.

Apply a lin. transformation by a fixed matrix

$$A \in \mathbb{F}_{2^8}^{4\times 4}$$

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

A may be written as a "circulant"

$$\begin{pmatrix} x & x+1 & 1 & 1 \\ 1 & x & x+1 & 1 \\ 1 & 1 & x & x+1 \\ x+1 & 1 & 1 & x \end{pmatrix}.$$

Thinking the Future
Zukunft denken

Add Roundkey

Bitwise addition mod 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 key length 128)

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

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

Expanded by 40 more columns

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

$i = 4, \ldots, 43$

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

1. Cyclic shift: $(w_0, w_1, w_2, w_3) \to (w_1, w_2, w_3, w_0) = (u_0, \ldots, u_3)$
2. Apply SubBytes to each $u_i \to (v_0, v_1, v_2, v_3)$
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: $k = 1, \ldots, 10$.

$$(W(4k), W(4k+1), W(4k+2), W(4k+3))$$

Thinking the Future
Zukunft denken

RWTH AACHEN UNIVERSITY

5.2.3. AES Decryption

Each of the steps SubBytes, ShiftRows, MixColumns, AddRoundKey

is invertible, giving transformations

- InvSubBytes (ISB)
- InvShiftRows (ISR)
- InvMixColumn (IMC)
- AddRoundKey (ARK) (its own inverse)

Keys are applied in reverse order.

Because of interchangeability there are implementations that look more symmetric, see Trap & Washington, p. 134, 135.

Thinking the Future
Zukunft denken