Simplified Advanced Encryption Standard (S-AES)

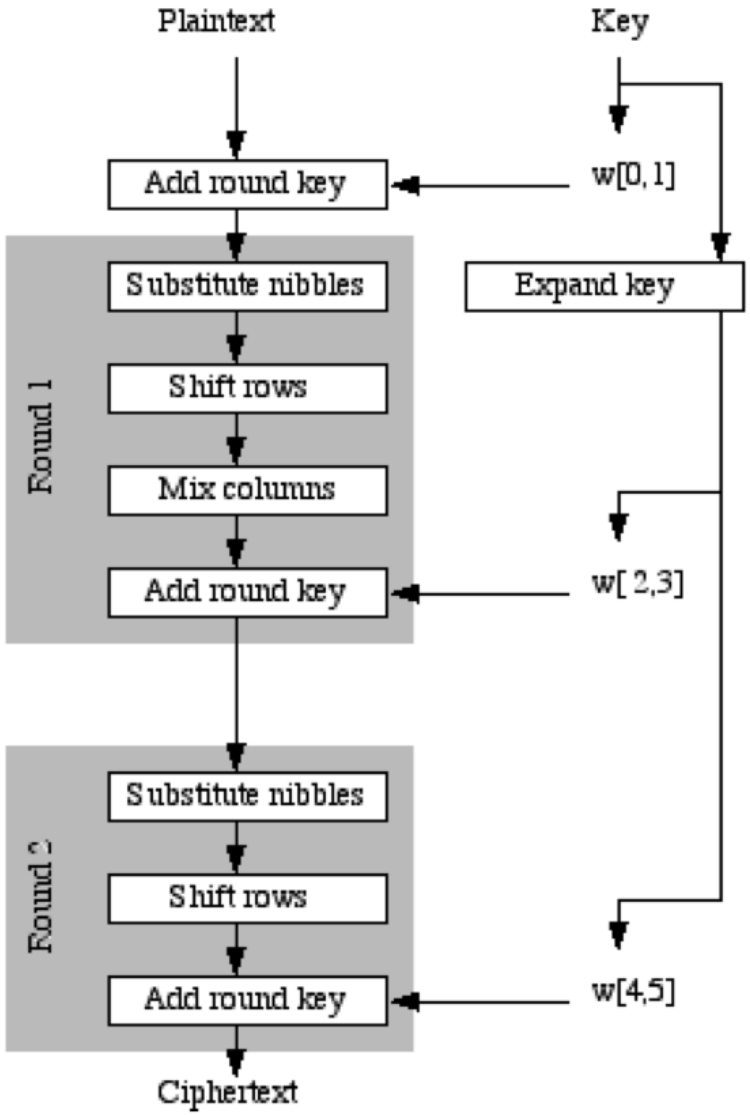
Math 4175

§4.6b. A Simplified Advanced Encryption Standard

Let us look at a simplifed AES whose structure is exactly same as AES with smaller size. Reference: Musa, Schaefer, and Wedig (2010), A simplified AES Algorithm and its Linear and Differential Cryptanalysis, *Cryptologia* 27(12), 148-177.

- Built on basic SPN architecture.
- Block size is 16 bits.
- Key length is also 16 bits.
- Number of rounds $N = 2$.
- From a key, 3 round keys are generated by a key schedule.

§4.6b. A Simplified Advanced Encryption Standard



S-AES Encryption Overview

§4.6b. A Simplified Advanced Encryption Standard

S-AES divides 16-bits block into two by two array of "nibbles", which are four bits long. So 1 nibble is equal to 4 bits.

This can be arranged in a 2×2 matrix:

$$A = \begin{bmatrix} a_{0,0} & a_{0,1} \\ a_{1,0} & a_{1,1} \end{bmatrix} = \begin{bmatrix} x_0 & x_2 \\ x_1 & x_3 \end{bmatrix}$$

§4.6b. A Simplified Advanced Encryption Standard

The S-box of S-AES carries each nibble in the current state matrix to a corresponding nibble in the next state matrix.

Here we are interested in a field with $2^4 = 16$ elements, because there are 16 possible nibbles. So we need an irreducible polynomial of degree 4 in $\mathbb{Z}_2[x]$.

Recall that $x^4 + x + 1$ is an irreducible polynomial in $\mathbb{Z}_2[x]$ and hence $F = \mathbb{Z}_2[x]/(x^4 + x + 1)$ is a field with 16 elements.

Let $a_3a_2a_1a_0$ be a nibble, that is, a binary string of length 4.
We can identify this nibble with an element in the field F as follows:

$$y = a_3\mathbf{x}^3 + a_2\mathbf{x}^2 + a_1\mathbf{x} + a_0.$$

§4.6b. A Simplified Advanced Encryption Standard

We now describe the construction of the permutation

$$\pi_S : \{0,1\}^4 \to \{0,1\}^4$$

The permutation π_S incorporates operations in the finite field

$$F = \mathbb{Z}_2[\mathbf{x}]/(\mathbf{x}^4 + \mathbf{x} + 1).$$

Let $a_3a_2a_1a_0$ be a binary string of length 4. We identify this byte with the field element

$$y = a_3\mathbf{x}^3 + a_2\mathbf{x}^2 + a_1\mathbf{x} + a_0.$$

Let $y^{-1} = b_3\mathbf{x}^3 + b_2\mathbf{x}^2 + b_1\mathbf{x} + b_0$ be the inverse of y in F when $y \neq 0$. (with $0^{-1} = 0$).

§4.6b. A Simplified Advanced Encryption Standard

Then, compute

$$\begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} b_3 \\ b_2 \\ b_1 \\ b_0 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} c_3 \\ c_2 \\ c_1 \\ c_0 \end{bmatrix}$$

We define $\pi_S(a_3a_2a_1a_0) = c_3c_2c_1c_0$.

§4.6b. A Simplified Advanced Encryption Standard

Recall that $(x^3 + x^2 + 1)^{-1} = x^2$, that is, $(1101)^{-1} = 0100$. Then

$$\begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

So we define $\pi_S(1101) = 1110$.

§4.6b. Substitute Nibbles

Substitute Nibbles: The S-box is given by the following table:

nibble	SN(nibble)	nibble	SN(nibble)
0000	1001	1000	0110
0001	0100	1001	0010
0010	1010	1010	0000
0011	1011	1011	0011
0100	1101	1100	1100
0101	0001	1101	1110
0110	1000	1110	1111
0111	0101	1111	0111

§4.6b. Shift Row

ShiftRow: Let the output of SubByte be:

$$B = \begin{bmatrix} b_{0,0} & b_{0,1} \\ b_{1,0} & b_{1,1} \end{bmatrix}$$

The second row of the matrix is left-shifted cyclically to yield:

$$\begin{bmatrix} b_{0,0} & b_{0,1} \\ b_{1,1} & b_{1,0} \end{bmatrix} = \begin{bmatrix} c_{0,0} & c_{0,1} \\ c_{1,0} & c_{1,1} \end{bmatrix} = C$$

C is the output of the ShiftRow.

§4.6b. MixColumn

MixColumn: Still viewing a nibble as an element of F, we perform the following matrix multiplication to get:

$$D = \begin{bmatrix} d_{0,0} & d_{0,1} \\ d_{1,0} & d_{1,1} \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 4 \\ 4 & 1 \end{bmatrix} \begin{bmatrix} c_{0,0} & c_{0,1} \\ c_{1,0} & c_{1,1} \end{bmatrix}$$

D is the output of the MixColumn Layer.

Note: 1 corresponds to 1 and 4 corresponds to x^2. Don't forget to reduce modulo $x^4 + x + 1$.

§4.6b. AddRoundKey

AddRoundKey: A round key is generated from the given 16 bit key, and bitwise XOR-ed with output D of MixColumn:

$$E = \begin{bmatrix} e_{0,0} & e_{0,1} \\ e_{1,0} & e_{1,1} \end{bmatrix}$$

$$= \begin{bmatrix} d_{0,0} & d_{0,1} \\ d_{1,0} & d_{1,1} \end{bmatrix} \oplus \begin{bmatrix} k_{0,0} & k_{0,1} \\ k_{1,0} & k_{1,1} \end{bmatrix}$$

§4.6b. Key Schedule

Key schedule for S-AES is done (very similarly to AES) as follows:

- We need 3 round keys, each of which consists of 16 bits.
- The key scheduling algorithm is word oriented, where a word consists of 2 nibbles (8-bits) here.
- The four nibbles in the key are grouped into two 8-bit words, $W(0)$ and $W(1)$, which will be expanded to 6 words.
- Supplied key provides $W(0)$ and $W(1)$ where $W(i)$ stands for i-th Word. This matrix is the round key for the 0th round.
- Then this matrix is expanded by adjoining 4 more columns, as follows.
- 16 bits of user supplied key: $\underbrace{1010\ 0111}_{W[0]}\ \underbrace{0011\ 1011}_{W[1]}$

§4.6b. Key Schedule

$W[0]$	$=$	1010		0111
$W[1]$	$=$	0011		1011
RN			$\times$	
		1011		0011
SN		$\downarrow$		$\downarrow$
		0011		1011
			$\oplus$	
Round constant		1000		0000
		1011		1011
			$\oplus$	
$W[0]$		1010		0111
$W[2]$	$=$	0001		1100
			$\oplus$	
$W[1]$		0011		1011
$W[3]$	$=$	0010		0111

§4.6b. Key Schedule

$W[2]$	$=$	0001		1100
$W[3]$	$=$	0010		0111
RN			$\times$	
		0111		0010
SN		$\downarrow$		$\downarrow$
		0101		1010
			$\oplus$	
Round constant		0011		0000
		0110		1010
			$\oplus$	
$W[2]$		0001		1100
$W[4]$	$=$	0111		0110
			$\oplus$	
$W[3]$		0010		0111
$W[5]$	$=$	0101		0001

§4.6b. Key Schedule

We get the round keys:

$$K_0 = 1010\ 0111\ 0011\ 1011$$
$$K_1 = 0001\ 1100\ 0010\ 0111$$
$$K_2 = 0111\ 0110\ 0101\ 0001$$

Now the encryption is done as follows:

$$PT \to A_{K_0} \to NS \to SR \to MC \to A_{K_1} \to NS \to SR \to A_{K_2} \to CT$$

Encrypt the plaintext: "ok" $= 0110\ 1111\ 0110\ 1011$

§4.6b. S-AES

$$PT = \begin{bmatrix} x_0 & x_2 \\ x_1 & x_3 \end{bmatrix} = \begin{bmatrix} 0110 & 0110 \\ 1111 & 1011 \end{bmatrix} \Longrightarrow$$

$$PT \oplus K_0 = \begin{bmatrix} 0110 & 0110 \\ 1111 & 1011 \end{bmatrix} \oplus \begin{bmatrix} 1010 & 0011 \\ 0111 & 1011 \end{bmatrix} = \begin{bmatrix} 1100 & 0101 \\ 1000 & 0000 \end{bmatrix}$$

Round 1:

$$\xrightarrow{NS} \begin{bmatrix} 1100 & 0001 \\ 0110 & 1001 \end{bmatrix} \xrightarrow{SR} \begin{bmatrix} 1100 & 0001 \\ 1001 & 0110 \end{bmatrix} \xrightarrow{MC^*} \begin{bmatrix} 1110 & 1010 \\ 1100 & 0010 \end{bmatrix}$$

$$\xrightarrow{\oplus K_1} \begin{bmatrix} 1110 & 1010 \\ 1100 & 0010 \end{bmatrix} \oplus \begin{bmatrix} 0001 & 0010 \\ 1100 & 0111 \end{bmatrix} \longrightarrow \begin{bmatrix} 1111 & 1000 \\ 0000 & 0101 \end{bmatrix}$$

(* see next slide for the details of MC part)

§4.6b. S-AES Mixcolumn

$$\begin{bmatrix} 1100 & 0001 \\ 1001 & 0110 \end{bmatrix} \xrightarrow{MC} \begin{bmatrix} 1 & x^2 \\ x^2 & 1 \end{bmatrix} \begin{bmatrix} x^3+x^2 & 1 \\ x^3+1 & x^2+x \end{bmatrix}$$

$$= \begin{bmatrix} 1(x^3+x^2)+x^2(x^3+1) & 1(1)+x^2(x^2+x) \\ x^2(x^3+x^2)+1(x^3+1) & x^2(1)+1(x^2+x) \end{bmatrix}$$

$$= \begin{bmatrix} x^3+x^2+x^5+x^2 & 1+x^4+x^3 \\ x^5+x^4+x^3+1 & x^2+x^2+x \end{bmatrix}$$

$$= \begin{bmatrix} x^5+x^3 & x^4+x^3+1 \\ x^5+x^4+x^3+1 & x \end{bmatrix}$$

$$= \begin{bmatrix} x(x^4+x+1)+x^3+x^2+x & 1(x^4+x+1)+x^3+x \\ (x+1)(x^4+x+1)+x^3+x^2 & x \end{bmatrix}$$

$$= \begin{bmatrix} x^3+x^2+x & x^3+x \\ x^3+x^2 & x \end{bmatrix} = \begin{bmatrix} 1110 & 1010 \\ 1100 & 0010 \end{bmatrix}$$

§4.6b. S-AES

Round 2:

$$\xrightarrow{NS} \begin{bmatrix} 0111 & 0110 \\ 1001 & 0001 \end{bmatrix} \xrightarrow{SR} \begin{bmatrix} 0111 & 0110 \\ 0001 & 1001 \end{bmatrix}$$

$$\xrightarrow{\oplus K_2} \begin{bmatrix} 0111 & 0110 \\ 0001 & 1001 \end{bmatrix} \oplus \begin{bmatrix} 0111 & 0101 \\ 0110 & 0001 \end{bmatrix} \longrightarrow \begin{bmatrix} 0000 & 0011 \\ 0111 & 1000 \end{bmatrix}$$

Cipher text: 0000 0111 0011 1000