[CS304] **Introduction to Cryptography and Network Security**

Course Instructor: Dr. Dibyendu Roy | Winter 2022-2023
Scribed by: Akshay (202051018) | Lecture (Week 6)

1 AES ....cnt'd

We have to understand the followings:

- Round function
- Key scheduling algorithm

Round functions of AES-128

$$f_1, f_2, \ldots\ldots, f_{10}$$

1. $f_1 = f_2 = f_3 = \ldots. = f_9$
2. f_{10} is different from f_i, $i = 1, 2, \ldots., 9$

   (In each version of AES, all round functions are equal except the last round function)

The first nine round functions are based on the following functions:

1. Subbytes
2. Shift rows
3. Mix column

The 10th round function is based on:

1. Subbytes
2. Shift rows

$$f_i : \{0,1\}^{128} \rightarrow \{0,1\}^{128}$$

In each round function, on input we apply subbytes first, whatever the output we get is passed to shift-rows and output from shift rows will be served as input to Mix Column.

$$\text{MixColumn(ShiftRows(Subbytes(x)))} = f_i(x)$$

$$128 \text{ bit} \rightarrow \boxed{f_i} \rightarrow 128 \text{ bit} \qquad i = 1, 2, \ldots., 9$$

$$128 \text{ bit} \rightarrow \boxed{\text{Subbytes}} \xrightarrow{128 \text{ bit}} \boxed{\text{Shift rows}} \xrightarrow{128 \text{ bit}} \boxed{\text{Mix column}} \rightarrow 128 \text{ bit}$$

1.1 Subbytes

$$\text{Subbytes}: \{0,1\}^{128} \rightarrow \{0,1\}^{128}$$

s : input

$$s = \begin{bmatrix} s_{00} & s_{01} & s_{02} & s_{03} \\ s_{10} & s_{11} & s_{12} & s_{13} \\ s_{20} & s_{21} & s_{22} & s_{23} \\ s_{30} & s_{31} & s_{32} & s_{33} \end{bmatrix}_{4\times 4} \qquad s_{ij} =: \text{8-bit} \qquad (8*(16) = 128 \text{ (total bits)})$$

Plaintext (P, 128-bit) is xored with the round key (128-bit) to get input (s) of subbyte functions.

$P = P_0 P_1 .... P_{15}$

$$P \oplus K_1 = \begin{bmatrix} P_0 & P_4 & P_8 & P_{12} \\ P_1 & P_5 & P_9 & P_{13} \\ P_2 & P_6 & P_{10} & P_{14} \\ P_2 & P_7 & P_{11} & P_{15} \end{bmatrix} \oplus K_1 = \begin{bmatrix} s_{00} & s_{01} & s_{02} & s_{03} \\ s_{10} & s_{11} & s_{12} & s_{13} \\ s_{20} & s_{21} & s_{22} & s_{23} \\ s_{30} & s_{31} & s_{32} & s_{33} \end{bmatrix}$$

We have a pre-defined S-box which maps 8-bit to 8-bit.
$S : \{0,1\}^8 \rightarrow \{0,1\}^8$

1. $(C_7 C_6 C_5 C_4 C_3 C_2 C_1 C_0) = (01100011) = (63)_{16}$ (constant)
2. S(s_{ij}) $= (a_7 a_6 a_5 a_4 a_3 a_2 a_1 a_0)$
3. For i=0 to 7
   $b_i = (a_i + a_{(i+4)\%8} + a_{(i+5)\%8} + a_{(i+6)\%8} + a_{(i+7)\%8} + C_i) mod 2$
4. $(b_7 b_6 b_5 b_4 b_3 b_2 b_1 b_0)$
5. $s'_{ij} = (b_7 b_6 \ .... \ b_0)$

$$\begin{bmatrix} s_{00} & s_{01} & s_{02} & s_{03} \\ s_{10} & s_{11} & s_{12} & s_{13} \\ s_{20} & s_{21} & s_{22} & s_{23} \\ s_{30} & s_{31} & s_{32} & s_{33} \end{bmatrix} \rightarrow \begin{bmatrix} s'_{00} & s'_{01} & s'_{02} & s'_{03} \\ s'_{10} & s'_{11} & s'_{12} & s'_{13} \\ s'_{20} & s'_{21} & s'_{22} & s'_{23} \\ s'_{30} & s'_{31} & s'_{32} & s'_{33} \end{bmatrix}$$

Now, we have to learn the working of S-box:
S(0) = 0
$X \neq 0 \in \{0,1\}^8$
S(X) = Y $\in \{0,1\}^8$
X = $(a_7 a_6 a_5 a_4 a_3 a_2 a_1 a_0)$ $\qquad a_i \in \{0,1\}$
P(x) = $a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4 + a_5 x^5 + a_6 x^6 + a_7 x^7 \in \mathbb{F}_2[x]$
deg(P(x)) ≤ 7 $\qquad P(x) \in \mathbb{F}_2[x]$
$(\mathbb{F}_2[x], +, *)$: Field
$g(x) = x^8 + x^4 + x^3 + x + 1$
g(x) is a primitive polynomial

$$(\mathbb{F}_2[x]/ < g(x) >, +, *)$$

Find the multiplicative inverse of P(x) under modulo $(x^8 + x^4 + x^3 + x + 1)$
P(x).q(x) $\equiv$ 1 mod$(x^8 + x^4 + x^3 + x + 1)$
$\implies P(x).q(x) - 1 = h(x).(x^8 + x^4 + x^3 + x + 1)$
$\implies 1 = P(x).q(x) + h(x).(x^8 + x^4 + x^3 + x + 1)$
gcd$(P(x), (x^8 + x^4 + x^3 + x + 1)) = 1$
How to find q(x) ?
We use Extended Euclidean Algo to find q(x).
q(x): Polynomial of degree 7.
q(x) = $r_0 + r_1x + r_2x^2 + r_3x^3 + r_4x^4 + r_5x^5 + r_6x^6 + r_7x^7$
$q(x) \to (r_7r_6r_5 \ .... \ r_0) \in \{0, 1\}^8$
S(X) = Y = $(r_7r_6r_5 \ .... \ r_0)$
Example:
$P(x) = x^6 + x^4 + x + 1$
$g(x) = x^8 + x^4 + x^3 + x + 1$

$$
\begin{array}{rl}
x^6 + x^4 + x + 1 \big) & x^8 + x^4 + x^3 + x + 1 \quad \big(x^2 + 1 \\
 & \underline{x^8 + x^6 + x^3 + x^2} \\
 & x^6 + x^4 + x^2 + x + 1 \\
 & \underline{x^6 + x^4 + x + 1} \\
 & x^2 \big) \, x^6 + x^4 + x + 1 \, \big(x^4 + x^2 \\
 & \quad \underline{x^6} \\
 & \quad x^4 + x + 1 \\
 & \quad \underline{x^4} \\
 & \quad x + 1 \big) \, x^2 \quad \big(x + 1 \\
 & \qquad \underline{x^2 + x} \\
 & \qquad x \\
 & \qquad \underline{x + 1} \\
 & \qquad 1
\end{array}
$$

Aim: $1 = q(x).P(x) + h(x).g(x)$
where 1 is gcd of P(x) and g(x). Inverse of g(x) is q(x).
We go from bottom to up in the search of aim equation.
Here:

$$remainder = dividend + divisor \times quotient$$

$$1 = x^2 + (x + 1)(x + 1)$$

$$= x^2 + (x + 1)[(x^6 + x^4 + x + 1) + x^2(x^4 + x^2)]$$

$$= x^2 + (x + 1)(x^6 + x^4 + x + 1) + (x + 1)x^2(x^4 + x^2)$$

$$= (x + 1)(x^6 + x^4 + x + 1) + x^2[1 + (x + 1)(x^4 + x^2)]$$

$$= (x + 1)(x^6 + x^4 + x + 1) + (1 + x^5 + x^3 + x^4 + x^2)x^2$$

Now replace x^2:

$$= (x+1)(x^6+x^4+x+1)+(1+x^5+x^4+x^3+x^2)[(x^8+x^4+x^3+x+1)+(x^6+x^4+x+1)(x^2+1)]$$

$$= (1+x^5+x^4+x^3+x^2)(x^8+x^4+x^3+x+1)+(x^6+x^4+x+1)[(x+1)+(1+x^5+x^4+x^3+x^2)(x^2+1)]$$

$$= h(x).g(x) + (x^6 + x^4 + x + 1)[x + 1 + x^2 + x^7 + x^6 + x^5 + x^4 + 1 + x^5 + x^4 + x^3 + x^2$$

$$= h(x).g(x) + (x^6 + x^4 + x + 1)(x^7 + x^6 + x^3 + x)$$

$$q(x) = x^7 + x^6 + x^3 + x$$

Which is the multiplicative inverse of $(x^6 + x^4 + x + 1)$
S(01010011) = (11001010) = $(a_7a_6a_5a_4a_3a_2a_1a_0)$
C = (01100011)
$b_i = (a_i + a_{(i+4)\%8} + a_{(i+5)\%8} + a_{(i+6)\%8} + a_{(i+7)\%8} + C_i) mod\ 2$
$(b_7b_6b_5b_4b_3b_2b_1b_0)$ = (11101101)
So, Subbytes(0101 0011) = (1110 1101)
In hexadecimal:
Subbytes(5 3) = E D
For programming we have outputs corresponding to each inputs already precomputed and stored.
Input = (X Y)
Subbyte(Input) = element present in the row number X and column number Y.

	Y															
X	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Source: Stinson Book