[CS304] Introduction to Cryptography and Network Security

Course Instructor: Dr. Dibyendu Roy | Winter 2022-2023
Scribed by : Pallikonda Sai Teja | Lecture (Week 06)
Student ID : 202011052

1 Advance Encryption Standard AES

$\rightarrow$ It is a block cipher.
$\Rightarrow$ Round function in AES should be invertable.

• We have understand the following.

1. Round Function.
2. Key Scheduling Algorithm.

1.1 Round Function of AES - 128 bit

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

(A) $f_1 = f_2 = f_3 = \ldots. = f_9$

(B) f_{10} is different from f_i, i = 1, 2, 3,.., 9.

First 9 round functions are exactly same and 10^{th} round function is different from other 9 round functions.

• The first 9 round functions (i.e., $f_1, f_2, \ldots, f_9$) are based on the following.

i. Sub bytes. $\boxed{f_i : \{0, 1\}^{128} \rightarrow \{0, 1\}^{128}}$

ii. Shift rows.

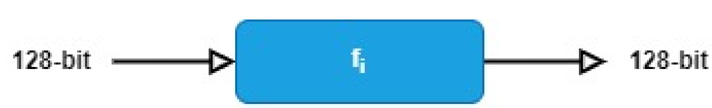
iii. Mix columns.

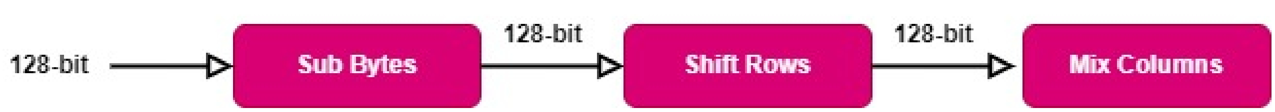
• The 10^{th} round function (i.e., f_{10}) is based on the following.

i. Sub bytes. $\boxed{f_{10} : \{0, 1\}^{128} \rightarrow \{0, 1\}^{128}}$

ii. Shift rows.

$f_i(X)$ = Mix Column(Shift Row(Sub Bytes(X)))





1.2 Sub bytes

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

S $\rightarrow$ input.

$$S \rightarrow \begin{vmatrix} S_{00} & S_{01} & S_{02} & S_{03} \\ S_{10} & S_{11} & S_{12} & S_{13} \\ S_{20} & S_{21} & S_{22} & S_{23} \\ S_{30} & S_{31} & S_{32} & S_{33} \end{vmatrix}$$

$$S_{ij} \rightarrow 8 \text{ bit.}$$

P $\rightarrow$ Plain text 128 bit.

$$P \rightarrow \begin{vmatrix} P_0 & P_4 & P_8 & P_{12} \\ P_1 & P_5 & P_9 & P_{13} \\ P_2 & P_6 & P_{10} & P_{14} \\ P_3 & P_7 & P_{11} & P_{15} \end{vmatrix} + K_1 \rightarrow (S_{ij})_{4x4} \qquad \text{len}(P_i) = 8 \text{ bit}$$

$K_1 \rightarrow$ 128 bit. K_0, K_1,..., K_{15}

$$K_1 \rightarrow \begin{vmatrix} K_0 & K_4 & K_8 & K_{12} \\ K_1 & K_5 & K_9 & K_{13} \\ K_2 & K_6 & K_{10} & K_{14} \\ K_3 & K_7 & K_{11} & K_{15} \end{vmatrix}$$

1.3 Sub bytes

$S = (S_{ij})_{4x4}$
$S : \{0, 1\}^8 \rightarrow \{0, 1\}^8 \qquad S(0) = 0$

i. $(c_7c_6c_5c_4c_3c_2c_1c_0) = (01100011) = (63)_{16}$

ii. $S(S_{ij}) = (a_7a_6a_5a_4a_3a_2a_1a_0)$

iii. For i = 0 to 7
$b_i = (a_i + a_{(i+4)\%8} + a_{(i+5)\%8} + a_{(i+6)\%8} + a_{(i+7)\%8} + c_i) \bmod 2$

iv. $(b_7b_6b_5b_4b_3b_2b_1b_0)$

v. $S^1{}_{ij} = (b_7b_6b_5b_4b_3b_2b_1b_0)$

• $S : \{0, 1\}^8 \rightarrow \{0, 1\}^8 \qquad S(0) = 0$
$X \neq 0 \in \{0, 1\}^8$
$S(X) = Y \in \{0, 1\}^8$
$X = (a_7a_6a_5a_4a_3a_2a_1a_0)$, $a_i \in \{0, 1\}$
$P(x) = a_0 + a_1x + a_2x^2 + ... + a_7x^7$
$\deg(P(x)) \leq 7$
$P(x) \in F_2[x]$

$g(x) = x^8 + x^4 + x^3 + x + 1$
g(x) is a primitive polynomial.

$(F_2[x]/< g(x) >, +, *) \rightarrow$ Field.
Find the multiplicative inverse of P(x) under modulo $(x^8 + x^4 + x^3 + x + 1)$

$p(x).q(x) = 1 \bmod (x^8 + x^4 + x^3 + x + 1)$

$\Rightarrow$ p(x).q(x) - 1 = h(x).(x^8 + x^4 + x^3 + x + 1)
1 = p(x).q(x) + h_1(x).(x^8 + x^4 + x^3 + x + 1)

gcd(a, b) = as + bt
gcd(P(x), x^8 + x^4 + x^3 + x + 1) = 1

How to find g(x) ?
$\Rightarrow$ Extended Euclidean Algorithm finds q(x)
q(x) $\rightarrow$ deg(q(x)) $\leq$ 7
q(x) = r_0 + $r_1 x$ + $r_2 x^2$ + ... + $r_7 x^7$
q(x) $\rightarrow$ ($r_7r_6r_5r_4r_3r_2r_1r_0$) $\in \{0, 1\}^8$
S(x) = Y = ($r_7r_6r_5r_4r_3r_2r_1r_0$)

Example

Find S(01010011) = ?
p(x) = x^6 + x^4 + x + 1
g(x) = x^8 + x^4 + x^3 + x + 1

x^6 + x^4 + x + 1) x^8 + x^4 + x^3 + x + 1 (x^2 + 1
$x^2 + x + 1$

---

x^6 + x^4 + x^2 + x + 1
x^6 + x^4 + x + 1

---

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

---

x^4 + x + 1
x^4

---

x + 1) x^2 (x + 1
x^2 + x

---

x
$x + 1$

1

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

Co-efficient of (x^6 + x^4 + x + 1) is multiplicative inverse of p(x) (i.e., q(x))
So, q(x) = $(x^2 + 1)(x^5 + x^4 + x^3 + x^2 + 1) + (x + 1)$
$= (x^7 + x^6 + x^5 + x^4 + x^2 + x^5 + x^4 + x^3 + x^2 + 1) + (x + 1)$

$= x^7 + x^6 + x^3 + x$
(11001010) $\rightarrow$ output.
c = (01100011)
$b_i = (a_i + a_{(i+4)\%8} + a_{(i+5)\%8} + a_{(i+6)\%8} + a_{(i+7)\%8} + c_i) \bmod 2$
$b_0 = (a_0 + a_4 + a_5 + a_6 + a_7 + c_0) \bmod 2$
$= (0 + 0 + 0 + 1 + 1 + 1) \mathrm{mod} 2$
$= 1$
$b_1 = (a_1 + a_5 + a_6 + a_7 + a_0 + c_1) \bmod 2$
$= (1 + 0 + 1 + 1 + 0 + 1) \mathrm{mod} 2$
$= 0$
$b_2 = 1$
$b_3 = 1$
$b_4 = 0$
$b_5 = 1$
$b_6 = 1$
$b_7 = 1$
Output of Sub bytes (1110 1101)
E D
Subbytes (0101 0011) = (1110 1101)
Subbytes (53) = (ED)

1.4 AES S-Boxes

	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

(a) S-box

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

(b) Inverse S-box