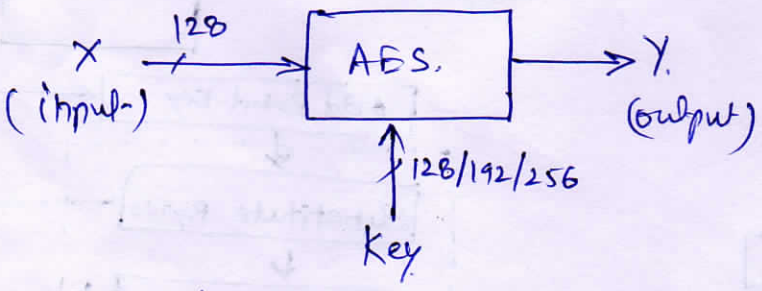
AES Origins

i) A replacement for DES was needed. (key search attacks).
ii) Can use triple DES - but slow.
iii) US NIST issued call for ciphers in 1997.
iv) 15 candidates accepted → 5 were shortlisted in Aug-99.
v) Rijndael was selected as the AES in Oct-2000.
vi) Designed by Rijmen-Daemen in Belgium.
vii) Has 128/192/256 bit key, 128 bit data.
viii) An iterative rather than feistel cipher.
   → processes data as block of 4 columns of 4 bytes.
   → operates on entire data block in every round.

AES Structure

i) Data block of 4 columns of 4 bytes is a state.
ii) Key is expanded to array of words.
iii) Has 9/11/13 rounds in which state undergoes:
   → Byte substitution (1 S-box used on every byte).
   → Shift rows
   → Mix columns
   → Add round key (XOR state with key material)

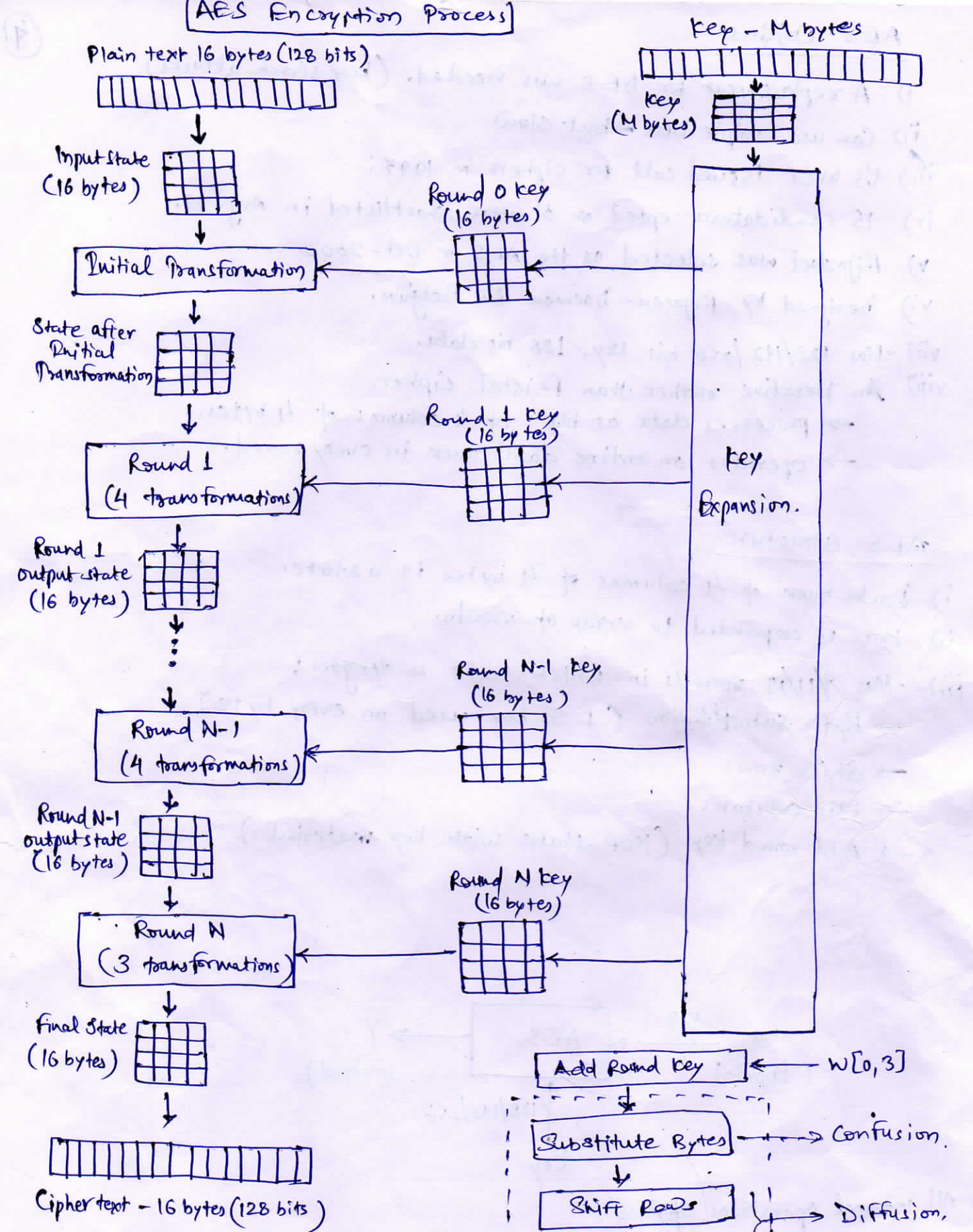


All internal operations of AES are based on finite field.

	Key length N_k words	Block Size (N_b words)	Rounds
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14.
	(Columns)	(Rows)	

P.T.O.

AES Encryption Process



No. of Rounds	key length (bytes)
10	16. (128 bits)
12	24 (192 bits)
14	32 (256 bits)

Substitute Bytes Transformation

EA	04	65	85
83	45	5D	96
5C	33	98	B0
F0	2D	AD	C5

→

87	F2	4D	97
EC	6E	4C	90
4A	C3	46	E7
8C	D8	95	A6

Shift Row Transformation

87	F2	4D	97
6E	4C	90	EC
46	E7	4A	C3
A6	8C	D8	95

Mix Columns Transformations

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \cdot \begin{bmatrix} 87 & F2 & 4D & 97 \\ 6E & 4C & 90 & EC \\ 46 & E7 & 4A & C3 \\ A6 & 8C & D8 & 95 \end{bmatrix} = \text{New State.}$$

$$\begin{bmatrix} 47 & 40 & A3 & 4C \\ 37 & D4 & 70 & 9F \\ 94 & E4 & 3A & 42 \\ ED & A5 & A6 & BC \end{bmatrix}$$

Add Round key Transformations

47	40	A3	4C
37	D4	70	9F
94	E4	3A	42
ED	A5	A6	EC

⊕

AC	19	28	57
77	FA	D1	5C
66	DC	29	00
F3	21	41	6A

=

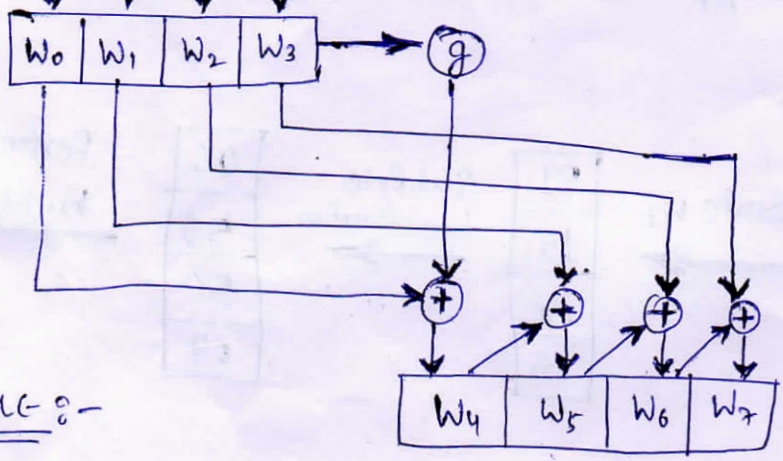
EB	59	8B	1B
40	2E	A1	C3
F2	38	13	42
1E	84	E7	D2

AES KEY EXPANSION :-

1) Takes 128-bit (16 byte) key and expands into array of 44/52/60 32-bit words.
2) Start by copying key into first 4 words.
3) Then loop creating words that depend on values in previous & 4 places back:
   → In 3 of 4 cases just XOR these together.
   → 1st word in 4 has rotate + S-box + XOR round constant on previous, before XOR 4th back.

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}

Key Size (Bytes)	Block Size (Bytes)	Expansion Rounds	Round key Copy	Expanded key (Bytes)
16	16	44	4	176
24	16	52	6	208
32	16	60	8	240.



RCON((Round/(KeySize/4))-1)

Ex:- For a 16 byte key Rcon is first called in the 4th round:
(4/(16/4))-1 = 0 ∴
Rcon(0) = 01000000.

For a 24 byte key Rcon is first called in the 6th round
(6/(24/4))-1 = 0.

EXAMPLE :-

key →

0F	47	0C	AF
15	D9	B7	7F
71	E8	AD	67
C9	59	00	98

W_0 = 0F 15 71 C9
W_1 = 47 D9 E8 59
W_2 = 0C B7 AD 00
W_3 = AF 7F 67 98

RCON (ROUND CONSTANT)

01	02	04	08	10	20	40	80	1B	36	6C	D8	AB	4D	9A
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

OPERATION :-

i) ROTATE WORD _ W3. = X1
ii) SUB-WORD USING S-BOX. = Y1
iii) RCON(a)
iv) Y1 ⊕ RCON(a)

0F	47	0C	AF
15	D9	B7	7F
71	E8	AD	67
C9	59	00	98

W_0 W_1 W_2 W_3

Rotate W_3.

0F	47	0C	7F
15	D9	B7	67
71	E8	AD	98
C9	59	00	AF

$X_1 =$

7F
67
98
AF

Perform SubByte transformation

$X_1 =$

D2
85
46
79

Perform X-OR with W_0, RCON(1)

DC	←	0F	⊕	01	⊕	D2	
90		15		00		85	
37		71		00		46	
B0		C9		00		79	
W_4		W_0		RCON(1)		X_1	

$W_5 = W_4 \oplus W_1 = 9B\ 49\ DF\ E9$

$W_6 = W_5 \oplus W_2 = 97\ FF\ 72\ 3F$

$W_7 = W_6 \oplus W_3 = 38\ 81\ 15\ AF$

Step (2)

0F	47	0C	AF	DC	9B	97	38
15	D9	B7	7F	90	49	FF	81
71	E8	AD	67	37	DF	72	15
C9	59	00	98	B0	E9	3F	AF

W_0 W_1 W_2 W_3 W_4 W_5 W_6 W_7

Rotate W_7

81
15
AF
38

SubByte transformation

0C
59
5C
07

Perform X-OR with W_4, RCON(2)

D2
C9
6B
B7

W_8

$W_9 = W_8 \oplus W_5 = 49\ 80\ B4\ 5E$

$W_{10} = W_9 \oplus W_6 = DE\ 7E\ C6\ 61$

$W_{11} = W_{10} \oplus W_7 = E6\ FF\ D3\ C6.$

Similarly we can compute for all (upto 44 words)

$W_{40} = Z_{10} \oplus W_{36}$

$W_{41} = W_{40} \oplus W_{37}$

$W_{42} = W_{41} \oplus W_{38}$

$W_{43} = W_{42} \oplus W_{39}$

Where Z_{10}

$$\left[RCON(10) \oplus \left\{ SubByte\left[Rotate\ Word\ (W_{39}) \right] \right\} \right]$$

A value is a polynomial of degree at most 8 with coefficients in GF(2).

For example, 0xB2 (10110010) really represents:

$$v = X^7 + X^5 + X^4 + X.$$

The coefficients are always 0 or 1.

Addition is done for each coefficient independently, and in GF(2), so 1+1=0.

In practice, this means that addition of two elements in GF(256) really is bitwise XOR.

For multiplication, this is again done with polynomials, and a modular reduction, using a specific degree-8 polynomial, which happens to be:

$$P = X^8 + X^4 + X^3 + X + 1$$

which corresponds to 0x11B (100011011)

[multiplication by the polynomial X, followed by reduction modulo P]

$$v \times X = (X^7 + X^5 + X^4 + X)\,X = X^8 + X^6 + X^5 + X^2$$

In the binary representation, this is a left shift by 1. However, the result must be reduced modulo polynomial P.

In this specific case, $v \times X$ is a degree-8 polynomial, which is one too many (Since P has degree 8, all polynomials modulo P must have degree 7 or less).

Modulo reduction really is subtracting a multiple of P such that the result will have degree 7 or less.

(Note: subtraction & addition are the same thing : a bit wise - XOR)

In this case :

$$v \times X \pmod P = (X^8 + X^6 + X^5 + X^2) + (X^8 + X^4 + X^3 + X + 1)$$

$$= X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$$

So the result is ⇒ 01111111 (0x7F)

0xB2 ⇒ 2 * B2 ⇒ 10110010 ⇒ 101100100 ⇒ 0x164

0164 XOR 11B ⇒

```
  101100100
XOR 100011011
-------------
  001111111
```

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} * \begin{bmatrix} 87 & F2 & 4D & 97 \\ 6E & 4C & 90 & EC \\ 46 & E7 & 4A & C3 \\ A6 & 8C & D8 & 95 \end{bmatrix} = \begin{bmatrix} 47 & 40 & A3 & 4C \\ 37 & D4 & 70 & 9F \\ 94 & E4 & 3A & 42 \\ ED & A5 & A6 & BC \end{bmatrix}$$

DETAILS OF MIX-COLUMN TRANSFORMATION STEP OF AES

FIRST ROW * SECOND COLUMN

1

02 * F2 = 11110010 ⇒ 11110100 XOR 00011011 ⇒ 11111111

03 * 4C ⇒ 02 * 4C + 4C ⇒ 01001100 ⇒ 01001100 + 01001100 = 11010100

01 * E7 ⇒ 11100111

01 * 8C XOR 10001100

01101011

11010100

10111111

11111111

01000000

40

2

02 * 4D = 01001101 ⇒ 01001101 0 ⇒ 10011010

03 * 90 = 10010000 ⇒ 10010000 XOR 00011011

00111011

10010000

10101011

01 * 4A = 01001010 → 01001010

11100001

01 * D8 = 11011000 → 11011000

00111001

10011010

10100011

A3

3

01 * 97 = 10010111

01 * EC = 11101100 XOR

01111011

02 * C3 ⇒ 11000011 0 XOR 10001101 1 (11B)

10011101

01111011

11100110

10100100

01000010

4 2

03 * 95 = 10010101 0 XOR 10001101 1 (11B)

00110001

10010101

10100100

FIRST ROW* THIRD COLUMN

THIRD ROW * FOURTH COLUMN

(1) FIRST ROW * FIRST COLUMN

02 * 87 ⇒ 10000111 ⇒ 100001110 (10E)

XOR 100011011 (11B)

000010101 ⇒ 0x15

03 * 6E ⇒ 02 * 6E + 6E ⇒

⇒ 01101110 ⇒ 011011100

01101110

10110010 ⇒

46 ⇒ 0100 0110

A6 ⇒ 1010 0110

11100000

10110010

(47)

01010010

00010101

01000111

(4) (7)

(2) SECOND ROW* FIRST COLUMN

87 ⇒ 1000 0111

02 * 6E ⇒ 01101110 ⇒ 011011100

03 * 46 ⇒ 02 * 46 + 46 ⇒ 01000110 ⇒ 010001100

01000110

11001010

A6 ⇒ 1010 0110

~~10000111~~ 10000111

~~01~~ 11011100

01011011

11001010

10010001

10100110

00110110

(3) (7)

(3) THIRD ROW * FIRST COLUMN

87 = 10000111

6E = 01101110

---

19 10 1001

02 * 46 = 01000110 => 01000 1100

03 * A6 = 02 * A6 + A6

= 10100110 => 1 01001100

XOR 1 0001 1011 (11B)

0 0101 0111

10100110

1111 0001

1000 1100

0111 1101

1110 1001

1001 0100

---

(9) (4)

---

(4) 03 * 87 => 10000111 => 1 0000 1110

02 * 87 + 87

XOR 1 0001 1011 (11B)

0 0001 0101

87 10000111

10010010

FOURTH ROW* FIRST COLUMN

6E => 01101110 → D1101110

11111100

46 => 01000110 → 01000110

10111010

02 * A6 => 10100110 → 0101 0111

10100 1100

XOR 1 0001 1011 (11B)

---

0 0101 0111

1110 1101

(E) (D)

(4)

$3*97 \oplus 1*EC \oplus 1*C3 \oplus 2*95$

↓

$2*97 \oplus 97$

10010111 → 100101110

XOR 100010011 (11B)

00110101

10010111

10100010

$1*EC \rightarrow$ 11101100

01001110

$1*C3 \rightarrow$ 11000011

10001101

00110001

$2*95$ → 100101010

10001011

00011000 1

01111100

BC