AES

Cryptography

AES

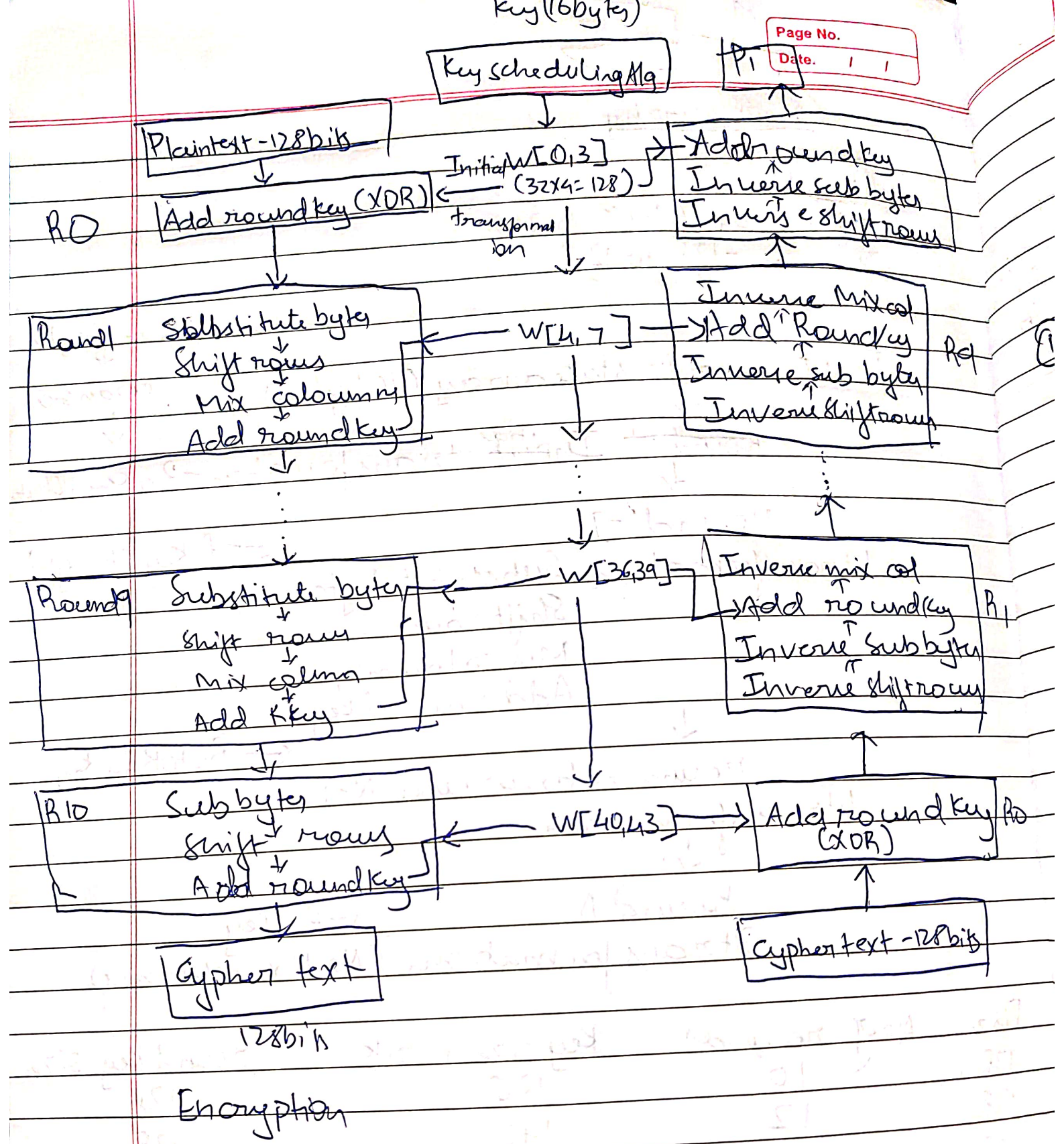
* found by NIST in 2001
* block - 128 to 128
  P C

Key - M bytes
↓
expansion
↓
← Rokey (16 bytes)

- Input stored in state array (16 bytes)
↓
~~Round~~ - 1 ~~Input~~ initial transformation
↓
round - 1
4 transformations: Substitute bytes
Shift rows
Mix columns
Add round key
← R1 key (16 bytes)
↓
round - 2 to round N-1
4 transformations
↓
Round N
3 transformations (No Mix columns)
← Rn key
← R2 to Rn-1 key

PT size	No of rounds	Key size in bits	Round key size
128	10	128	128
128	12	192	128
128	14	256	128

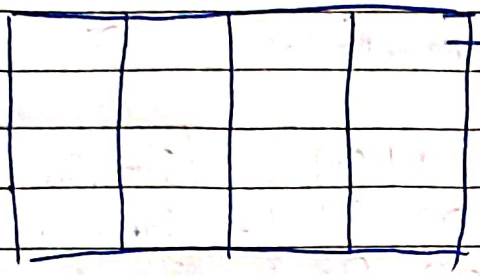
1 Word = 32 bits



Key size	No of words
AES ~~16 bytes~~ 128	44
AES 192	52
AES 256	60

Page No.
Date. / /

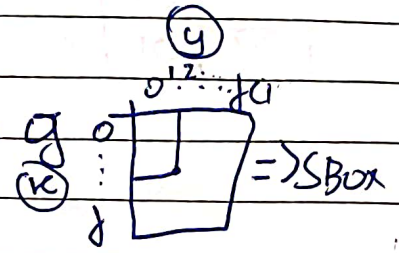
Transformations in each round



→ 8 bits each
eg: 1011 0110
x y

① **Substitute bytes**

SBox has values of



S_{00}	S_{01}	.	.
S_{10}	S_{11}	.	.
$S_{.}$	.	.	.
.	.	.	.

eg: Let $S_{00} = \underset{x}{1100}\ \underset{y}{0101}$

S'_{00} = Value where x & y intersect in Sbox

S'_{00}	S'_{01}	.	.
S'_{10}	S'_{11}	.	.
.	.	.	.
.	.	.	.

111^4 for all

② **Shift rows**

⟹

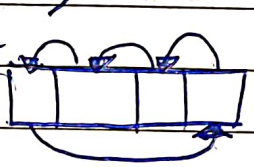
S_{00}	S_{01}	S_{02}	S_{03}
S_{10}	S_{11}	S_{12}	S_{13}
S_{20}	S_{21}	S_{22}	S_{23}
S_{30}	S_{31}	S_{32}	S_{33}

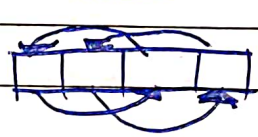
→ R_1 → No shift

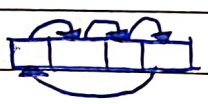
→ R_2 - LSL(1)

→ R_3 LSL(2)

→ R_4 [LSL(3)] same (RE1)







S_{00}	S_{01}	S_{02}	S_{03}
S_{11}	S_{12}	S_{13}	S_{10}
S_{22}	S_{23}	S_{20}	S_{21}
S_{33}	S_{30}	S_{31}	S_{32}

(3) Mix Columns

Multiply with predefined Matrix

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}

X

02	03	01	01
01	02	03	01
01	01	02	03
03	01	01	02

=

S'_{00}	S_{01}	S'_{02}	S'_{03}
S'_{01}	S_{11}	S'_{12}	S'_{13}
S'_{20}	S'_{21}	S'_{22}	S'_{23}
S'_{30}	S'_{31}	S'_{32}	S'_{33}

(4) Add round key

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}

$\oplus$

W_i	W_{i+1}	W_{i+2}	W_{i+3}

$\Rightarrow$

S'_{00}
S'_{33}

Columnwise ⊕ XOR

1 word = 32 bit

each column = 4 X 1 byte in each $S_{00} \ldots S_{33}$ = 4 X 8 = 32

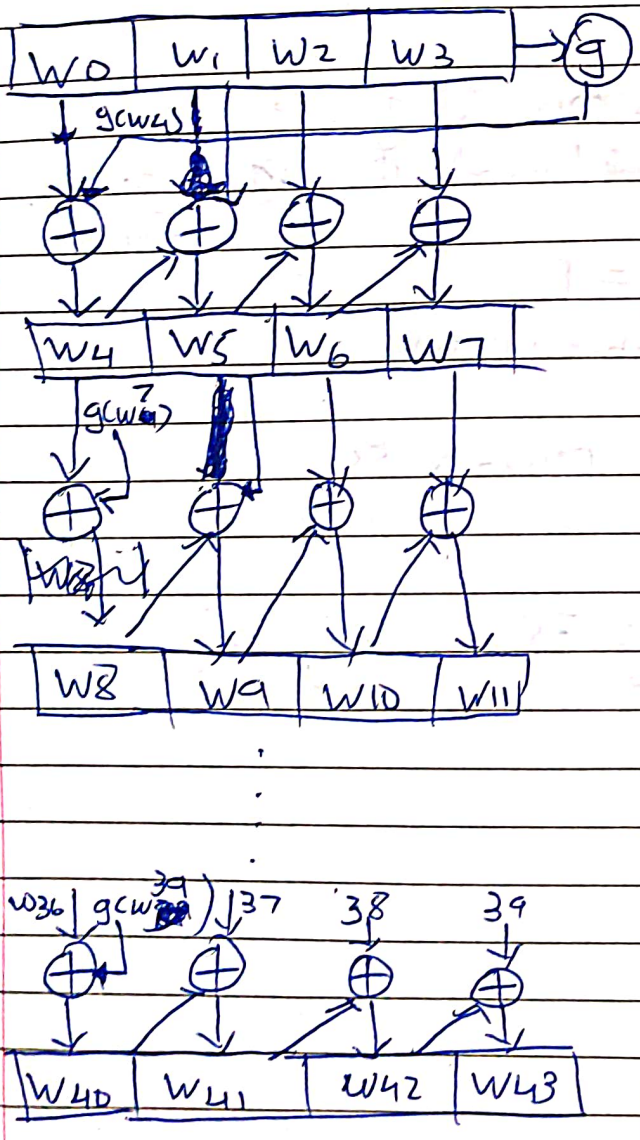
each word: 4 bytes
each byte: 8 bits
$k_0 \ldots k_{15}$ = 1 byte each

AES Key Expansion

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}

w_0 w_1 w_2 w_3

Key for R_0



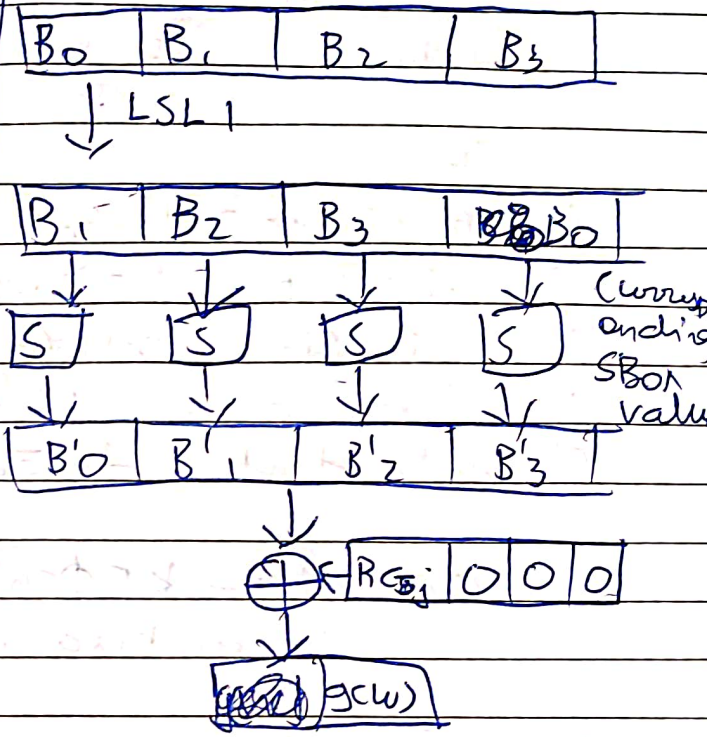
Key for R_1

Key for R_2

Key for R_{10}

g function

W → B = Byte



Rj	Round constant
0	$(00\ 00\ 00\ 00)_{16}$
1	$(01\ 00\ 00\ 00)_{16}$
2	$(02\ 00\ 00\ 00)_{16}$
3	$(04\ 00\ 00\ 00)_{16}$
4	$(08\ 00\ 00\ 00)_{16}$
5	$(10\ 00\ 00\ 00)_{16}$
6	$(20\ 00\ 00\ 00)_{16}$
7	$(40\ 00\ 00\ 00)_{16}$
8	$(80\ 00\ 00\ 00)_{16}$
9	$(1B\ 00\ 00\ 00)_{16}$
10	$(36\ 00\ 00\ 00)_{16}$

Initial round constant

RSA

If A has to send msg to B then A encrypts PT using B's Public key & B converts it to CPT back using B's private key (PRK). Both A&B have their own public & private keys.

Steps

1. choose 2 large random prime nos p & q
2. calculate $n = p*q$
3. Calc $\phi(n) = (p-1)*(q-1)$
4. choose e st $1 < e < \phi n$ & $\gcd(e, \phi(n)) = 1$ [coprime]
5. calc d st: $de \equiv 1 \mod \phi n$

$\Rightarrow de - k[\phi(n)] = 1$

where k is a positive integer

6. e = public key d = private key

* $p = 13$, $q = 17$, $p(A) = 35$ (e), $pr(A) = ?$ (d)

$pq = 221$

$\phi(n) = 192$

$e = 35$

$d = ?$

$35d - 192k = 1$

$d = \frac{1 + 192k}{35}$ (Note: d should be whole no. No Decimals)

k=0 X
k=1 X
k=2 ✓ d=11

∴ private key of A = 11

DHKE

~~XA = Private~~ X - Private
Y - Public

used to exchange key follows asymetric key

Steps

1. consider prime no q
2. Select α st α < q & α is primitive root of q

α is primitive root of q iff

$\alpha^1 \mod q$
$\alpha^2 \mod q$
⋮
$\alpha^{q-1} \mod q$

Should have values in {1, 2 ... q-1} byfree of
eg: q=7 α=3 , q-1=6 {1, 2, 3, 4, 5, 6}

$3^1 \mod 7 = 3$
$3^2 \mod 7 = 2$
$3^3 \mod 7 = 6$
$3^4 \mod 7 = 4$
$3^5 \mod 7 = 5$
$3^6 \mod 7 = 1$

all values from 1 to 6 are covered

∴ 3 is primitive root of 7

③ Assume X_A where $X_A < q$

Calc $Y_A = \alpha^{X_A} \bmod q$

④ Assume X_B st $X_B < q$

Calc $Y_B = \alpha^{X_B} \bmod q$

⑤ Calculate K_1 & K_2

$K_1 = (Y_B)^{X_A} \bmod q$

$K_2 = (Y_A)^{X_B} \bmod q$

if $K_1 = K_2$ then key exchange successful

eg: $q = 7$

$\alpha = 5$

$Y_A = 3 \quad X_A = 6$

$Y_A = 5^3 \bmod 7 = 6$ $\quad \alpha^{X_A} \bmod q$

$Y_B = 4 \quad X_B = 2$

$X_A = 5^4 \bmod 7 =$ $\quad \alpha^{X_B} \bmod q$

$K_1 = Y_B^{X_A} \bmod q = 4$

eg: ① $q = 7$
② $\alpha = 5$ calc k_1 & k_2

③ $X_A = 3$

$Y_A = \alpha^{(XA)} \bmod q$
$Y_A = 5^3 \bmod 7 = 6$

$\boxed{X_A = 3 \quad Y_A = 6}$

④ $X_B = 4$
$Y_B = \alpha^{(XB)} \bmod q$
$Y_B = 5^4 \bmod 7$
~~$Y_B = 2$~~
$\boxed{Y_B = 4, \; Y_B = 2}$

⑤ $k_1 = (Y_B)^{XA} \bmod q$
$k_1 = 4^3 \bmod 7$
$k_1 = 8 \bmod 7$

$\boxed{k_1 = 1}$

$k_2 = (Y_A)^{YB} \bmod q$
$k_2 = 6^4 \bmod 7$
$k_2 = 1296 \bmod 7$
$\boxed{k_2 = 1}$

$k_1 = k_2$

Key exchange successfully

ELGAMAL

- Asymetric

3 steps
1. Key generation
2. Encryption
3. decryption

1. Key generation

1. large prime number p
2. Select decryption key (private key) d
3. Select second part of encryption key (e_1)
4. Calculate third part of encryption key (e_2)

~~$e_2 = (e_1)^d \bmod p$~~

$$e_2 = (e_1)^d \bmod p$$

5. public key = (e_1, e_2, p), private key = d

Page No.
Date. / /

(2) Encryption

1. Select random integer r

2. Calculate c1 & c2

$$c1 = (e1)^r \bmod p$$

$$c2 = (PT \times (e2)^r) \bmod p$$

3. Ciphertext = (c1, c2)

(3) $$PT = [c2 \times ((c1)^p)^{-1}] \bmod p$$ Decryption

remember $ab \bmod n = (a \bmod n \times b \bmod n) \bmod n$

and $a^{-1} \bmod b = x$ where $ax \bmod b = 1$

eg: PT = 7

(1) Key generation

Let p = 11

d = 3

$e_1 = 2$

$e_2 = (e_1)^d \bmod p$

$e_2 = 2^3 \bmod 11 = 8 \bmod 11$

$e_2 = 8$

private key = 3

public key = (2, 8, 11)

Page No.
Date. / /

② Enc

$r = 4$

$C_1 = (\varepsilon_1)^r \bmod p$

$C_1 = (16)\ 2^4 \bmod 11 = 16 \bmod 11$

$C_1 = 5$

$C_2 = (PT \times \varepsilon_2^r) \bmod p$

$C_2 = (7 \times 8^4) \bmod 11$

$C_2 = 6$

~~Encrypted~~

Ciphertext = $(5, 6)$ $[(C_1, C_2)]$

③ Dec

$PT = [C_2 \times (((C_1)^d)^{-1})] \bmod p$

$PT = ((6 \times ((5)^3)^{-1}) \bmod 11) \bmod 11$

$PT = (6 \bmod 11 \times (125)^{-1} \bmod 11) \bmod 11$

↓

to find $(125)^{-1} \Rightarrow 125 \times k \bmod 11 = 1$

by calc: $k = 3$

$\therefore (125)^{-1} = 3$

~~PT = 6 X 3~~

$PT = (6 \bmod 11 \times 3 \bmod 11) \bmod 11$

$= (6 \times 3) \bmod 11$

$= 18 \bmod 11$

$= 7$

DISCRETE LOGS

- $g^x \bmod p$ where g is primitive root of p

eg $2^x \bmod 7$ if k can be ~~extracted~~. so to find exact value eg k can be hard

Solve $\log_2 9 \bmod 11$

$p = 11, g = 2, X = 9$ $\quad 2^9 \bmod 11$