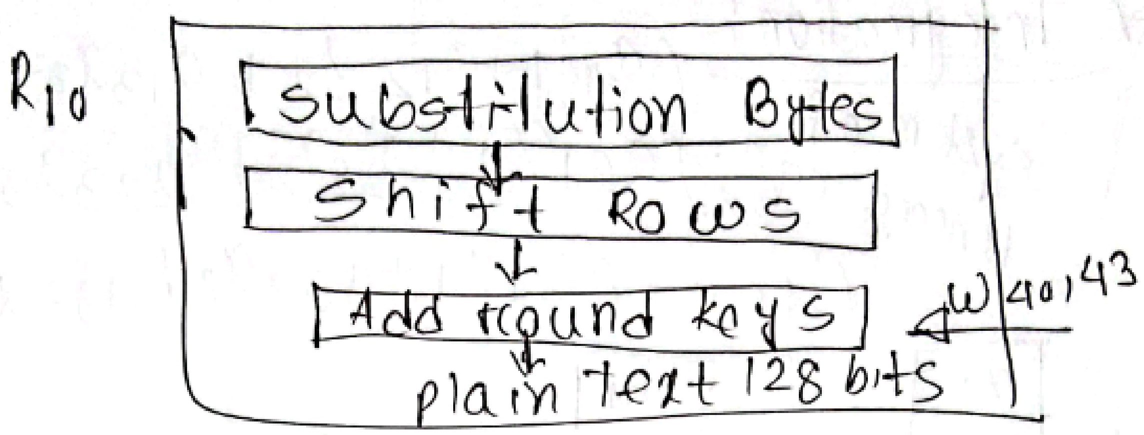
TOPIC NAME :

DAY :

TIME : DATE : / /



TOPIC NAME : S.P.L DAY :

TIME : DATE : / /

A.E.S. Algorithm

Advance encryption standard:

symmetric key block cipher.

(same key used for encryption + decryption)

* established in 2001 by US NSIT (National Institute of standards and Technology).

* fixed block size: 128 bits.

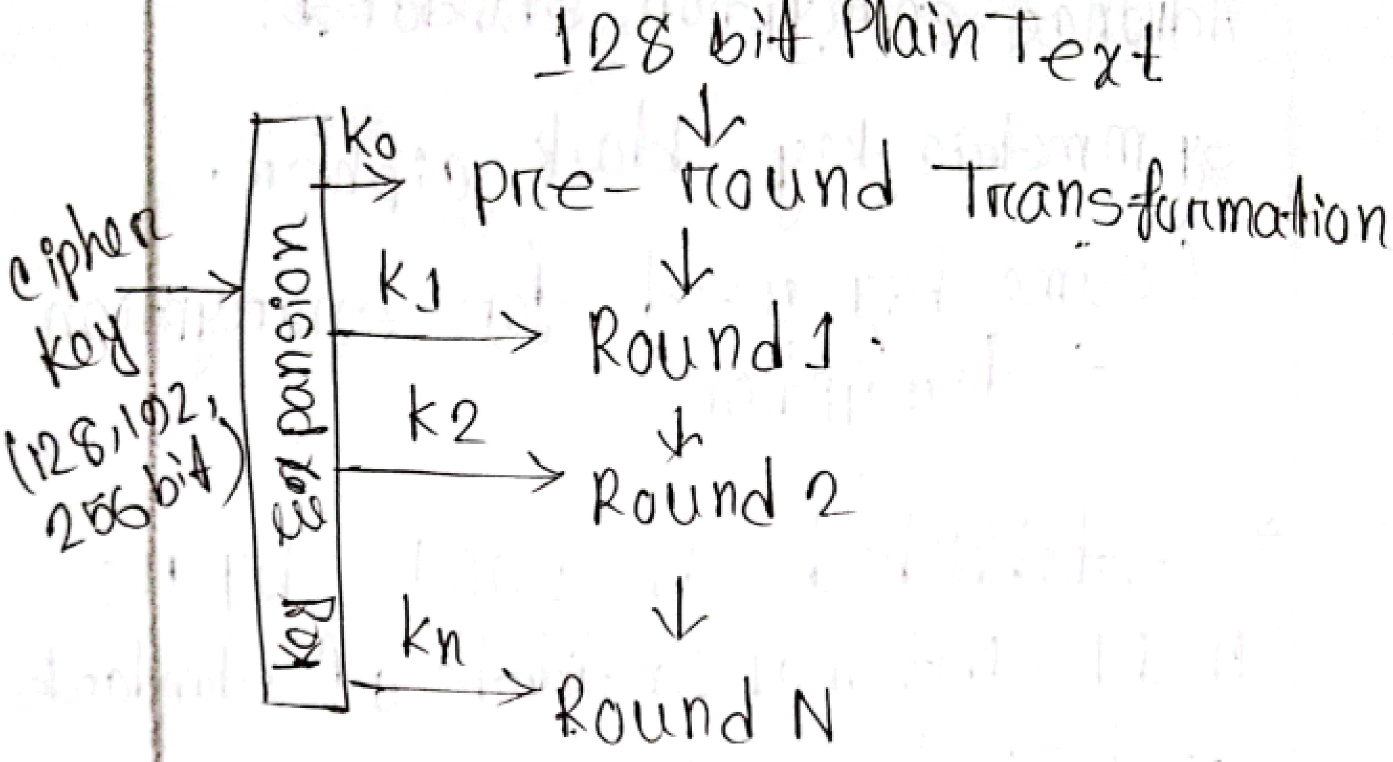
Rounds: no. of bits

10 → 128 AES - 128 version

12 → 192 AES - 192 version

14 → 256 AES - 256 version

1 word = 32 bits.



General design of AES Encryption.

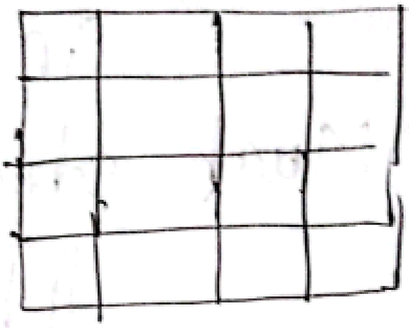
* no of keys generated by key expanssion algorithm is =(no of rounds+1)

*state → 16 bytes (4x4)

stores the intermediate results.

* input will be in 4x4 matrix

input array:



4x 4byte = 128 bits

state array:

$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,3}$
$S_{1,0}$	$S_{1,1}$	$S_{1,2}$	$S_{1,3}$
$S_{2,0}$	$S_{2,1}$	$S_{2,2}$	$S_{2,3}$
$S_{3,0}$	$S_{3,1}$	$S_{3,2}$	$S_{3,3}$

[W_0, W_1, W_2, W_3]

1st byte of 0th word

3nd byte of 1st word

~~set~~array[byte][state]

key:

W_0	W_1	W_2	W_3
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}

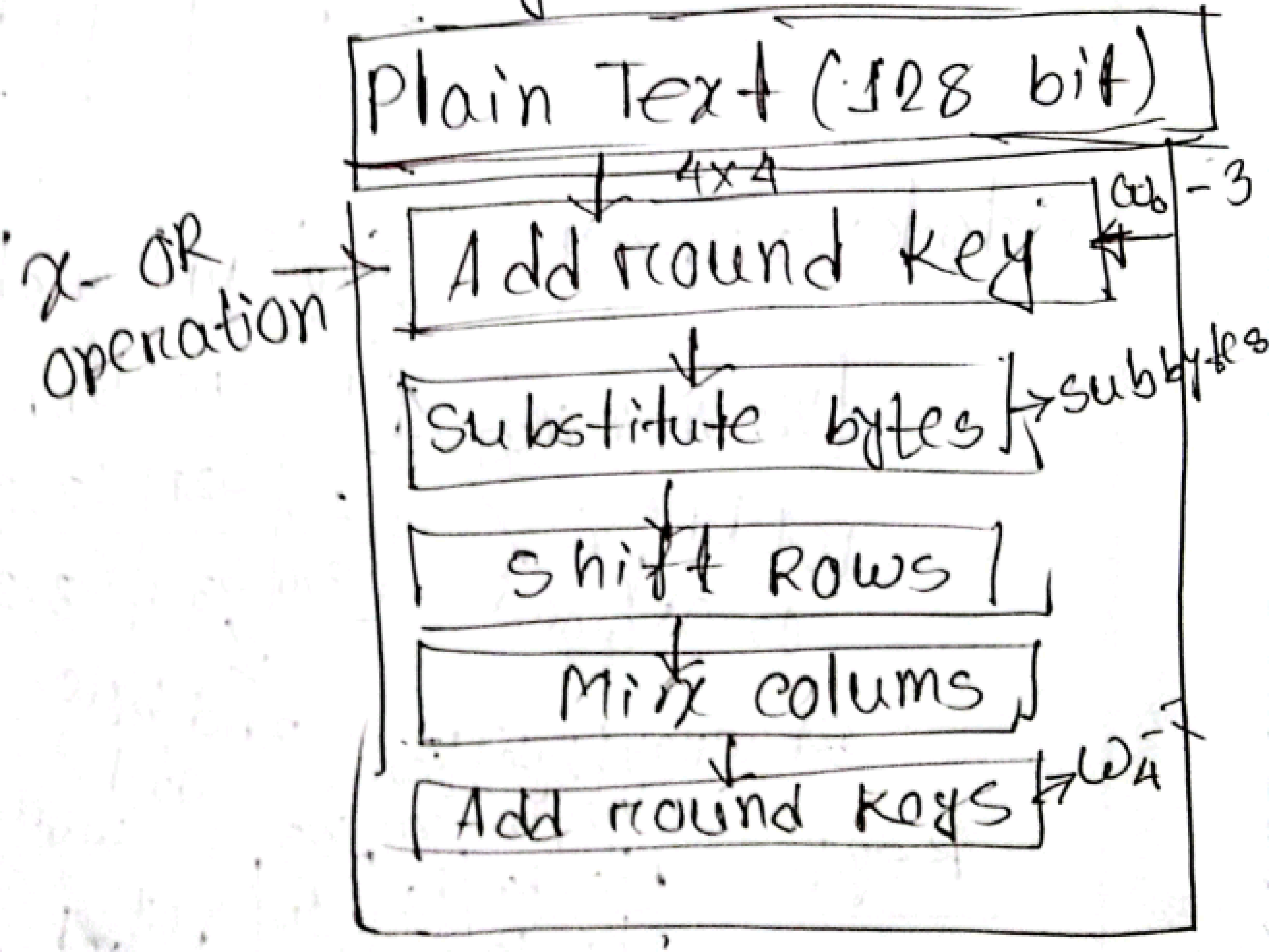
key expand algo →

44 words

W_0	W_1	W_2	. . .	W_{43}

* encryption algorithm → cipher.
* decryption algorithm → reverse cipher.
↓
round keys applied in reverse keys.

* Much stronger than DES


Plain Text (128 bit)
4x4
x- OR operation
Add round key
ω_0 -3
Substitute bytes
subbytes
Shift Rows
Mix colums
Add round keys
ω_4