Triple

cipher algorithm

TA&M CIPHER

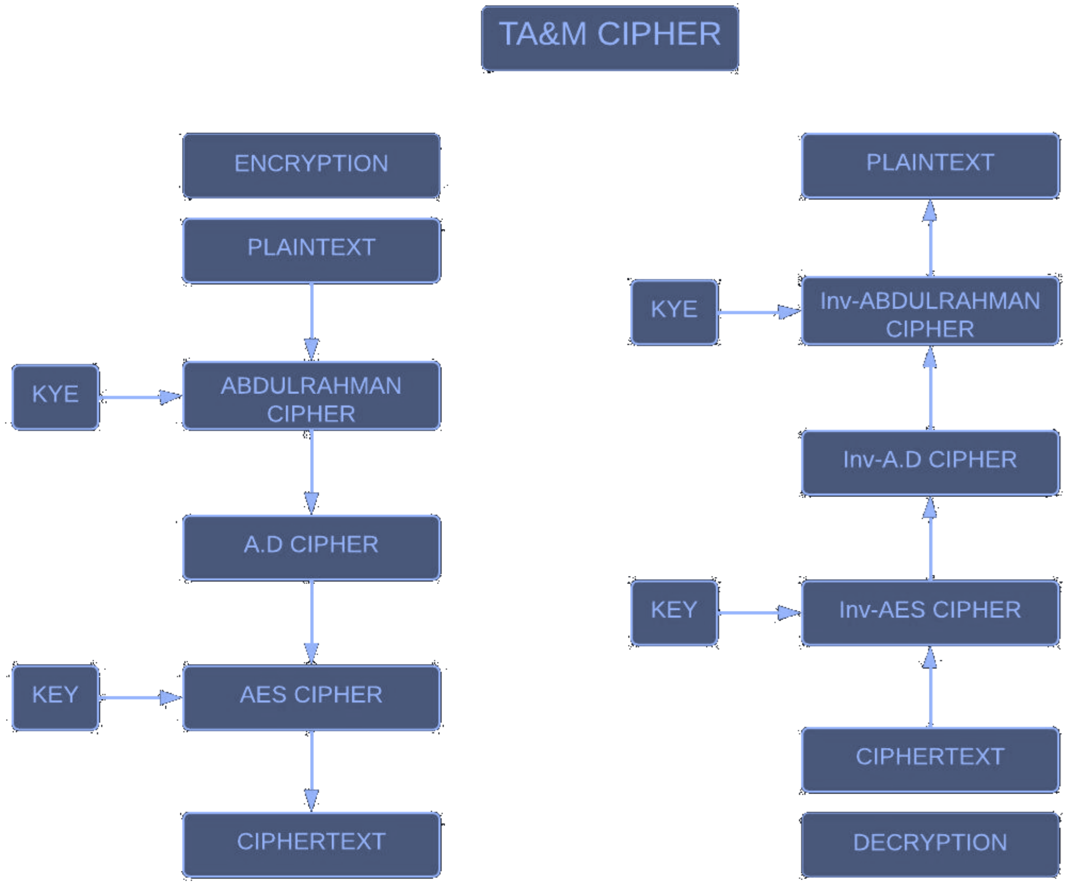
Steps of encryption

The first step we take the plaintext to Abdulrahman cipher and encryption. The second step we take the cipher text from Abdulrahman cipher to A.D Cipher and encryption. The last step take the ciphertext from A.D Cipher to AES Cipher and encryption. finally, we have the Ciphertext.

Steps of decryption

The first step we take the ciphertext to AES Cipher and decryption. The second step we take the ciphertext to A.D cipher and decryption. The last step we take the ciphertext to Abdulrahman cipher and decryption. Finally, we have the plaintext.

the diagram of TA&M Cipher



Cipher

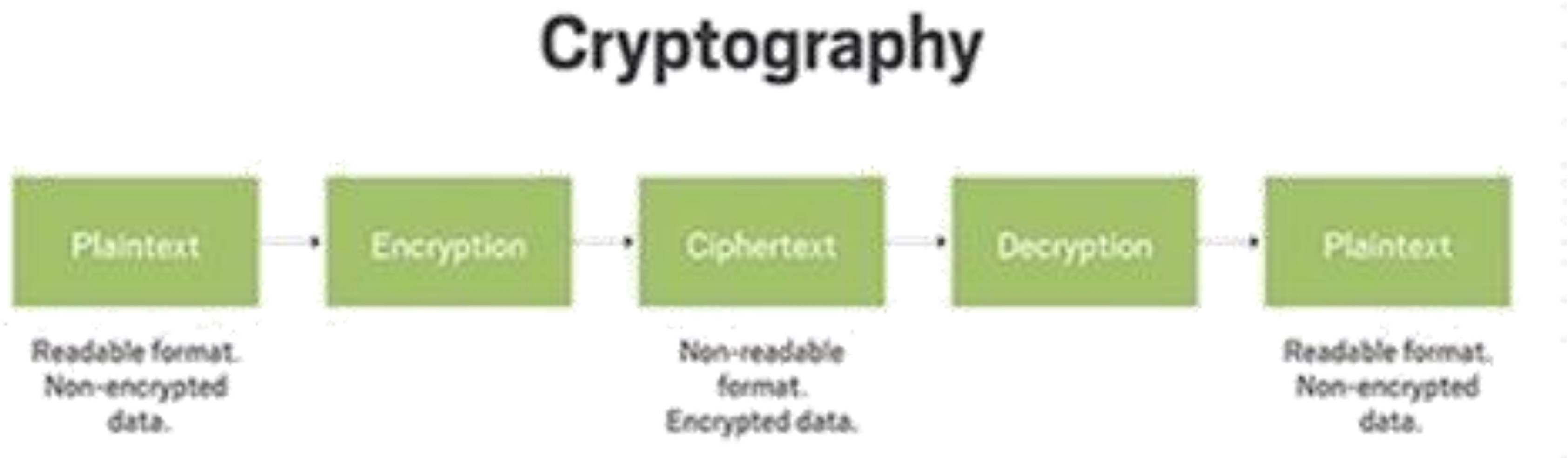
What is a cipher?

In cryptology, the discipline concerned with the study of cryptographic algorithms, a cipher is an algorithm for encrypting and decrypting data.

Ciphers used these two main types of transformation:

1. Transposition ciphers keep all the original bits of data in a byte but mix their order.

2. Substitution ciphers replace specific data sequences with other data sequences. For example, one type of substitution would be to transform all bits with a value of 1 to a value of 0, and vice versa.

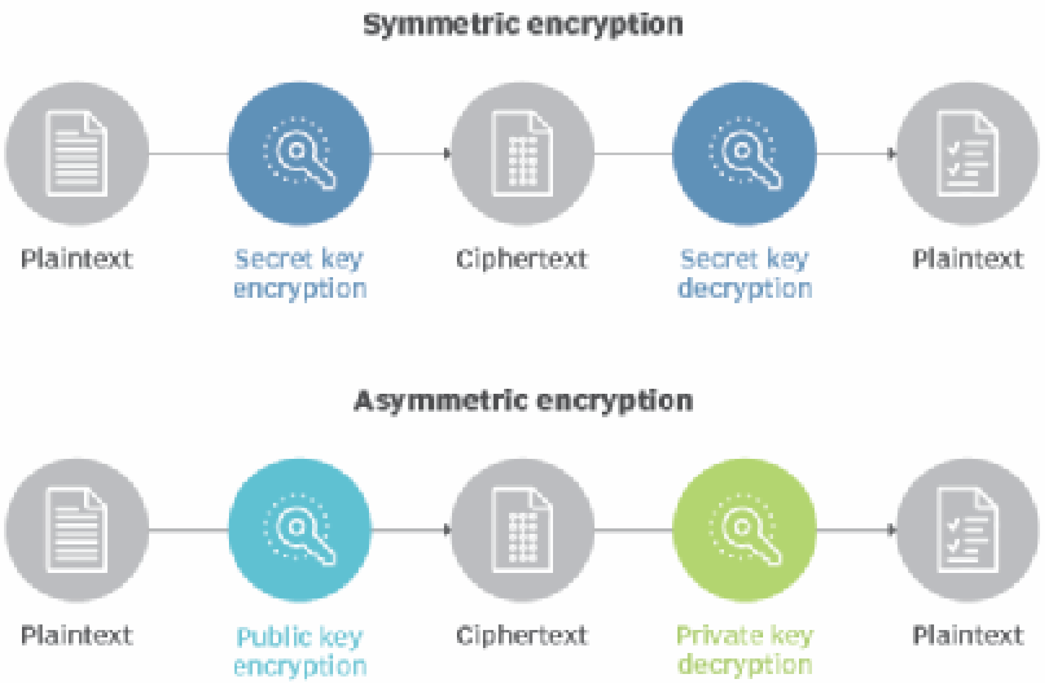


Cryptography
Plaintext
Encryption
Ciphertext
Decryption
Plaintext
Readable format. Non-encrypted data.
Non-readable format. Encrypted data.
Readable format. Non-encrypted data.

With symmetric key algorithms, the same key is used for the encryption and decryption of data.
Asymmetric key algorithms use public keys and private keys to encrypt and decrypt data.

- The public key can be shared with everyone.
- The private, or secret key, is kept secret.

Symmetric vs. asymmetric encryption



Symmetric encryption

Plaintext → Secret key encryption → Ciphertext → Secret key decryption → Plaintext

Asymmetric encryption

Plaintext → Public key encryption → Ciphertext → Private key decryption → Plaintext

What are ciphers used for?

Symmetric ciphers are most commonly used to secure online communications.

Types of ciphers

Ciphers can be characterized in different ways, including the following:

- Block ciphers encrypt uniformly sized blocks of data.
- Stream ciphers can be applied to streams of data that are often received and sent over a network.

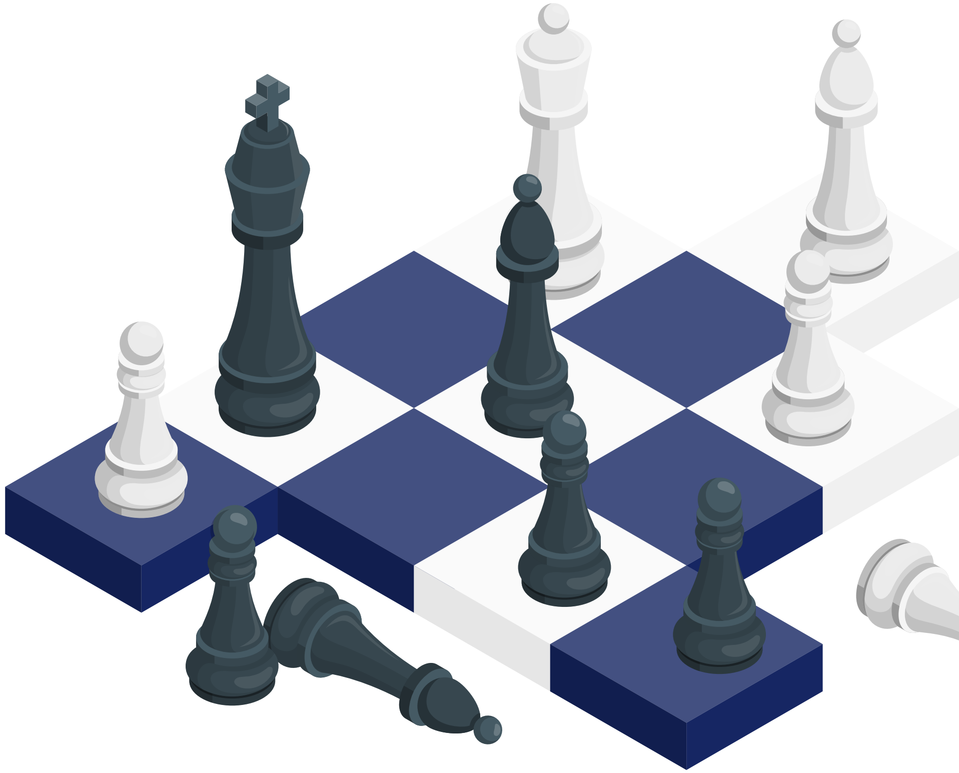
ABDULRAHMAN CIPHER

ABDULRAHMAN CIPHER IS DERIVED FROM

The Abdulrahman cipher derived from the Playfair cipher
and chess
Playfair
We derived from the Playfair:
Generate the key Square (5×5)

Chess
We derived from the chess

We choose A Knight
A knight moves to any of the closest squares that are not on the same rank, file, or diagonal. (Thus, the move forms an "L"-shape: two squares vertically and one square horizontally, or two squares horizontally and one square vertically.)
And we just choose one move , the move is two steps up and one step right



Rules for

encryption and decryption

Encryption

In encryption we have two steps
Step 1) tow steps up
Step 2) one step right

Decryption

In decryption we have two steps:
Step 1) one step left
Step 2) two steps down

Example of encryption

Find the encryption massage = " ALI", and the key = "FOOD".

for encryption.

1. Construction the Matrix, for Construction the matrix take the key without character repetition

F	**O**	**D**	**A**	**B**
C	E	G	H	I/J
K	L	M	N	P
Q	R	S	T	U
V	W	X	Y	Z

2. Every letter be single.

A

L

I

3. We take every single letter and encryption.

F	**O**	**D**	**A**	**B**
C	**E**	**G**	**H**	**I/J**
K	**L**	**M**	**N**	**P**
Q	**R**	**S**	**T**	**U**
V	**W**	**X**	**Y**	**Z**

To encryption use the rules encryption

A = U L = D I = V

The ciphertext = "UVD".

Encryption

Example for decryption

Find the decryption massage = "UVD", and the key = "FOOD".

1. Construction the Matrix, for Construction the matrix takes the key without character repetition.

F	O	D	A	B
C	E	G	H	I/J
K	L	M	N	P
Q	R	S	T	U
V	W	X	Y	Z

2. Every letter be single.

U
V
D

3. We take every single letter and decryption.

F	O	D	A	B
C	E	G	H	I/J
K	L	M	N	P
Q	R	S	T	U
V	W	X	Y	Z

To decryption use the rules decryption

U = A D = L V = I

The plaintext ="ALI".

Decryption

A.D CIPHER

A.D CIPHER

A.D CIPHER IS DERIVED FROM

The A.D Cipher derived from the playfair cipher and AES Cipher

Playfair

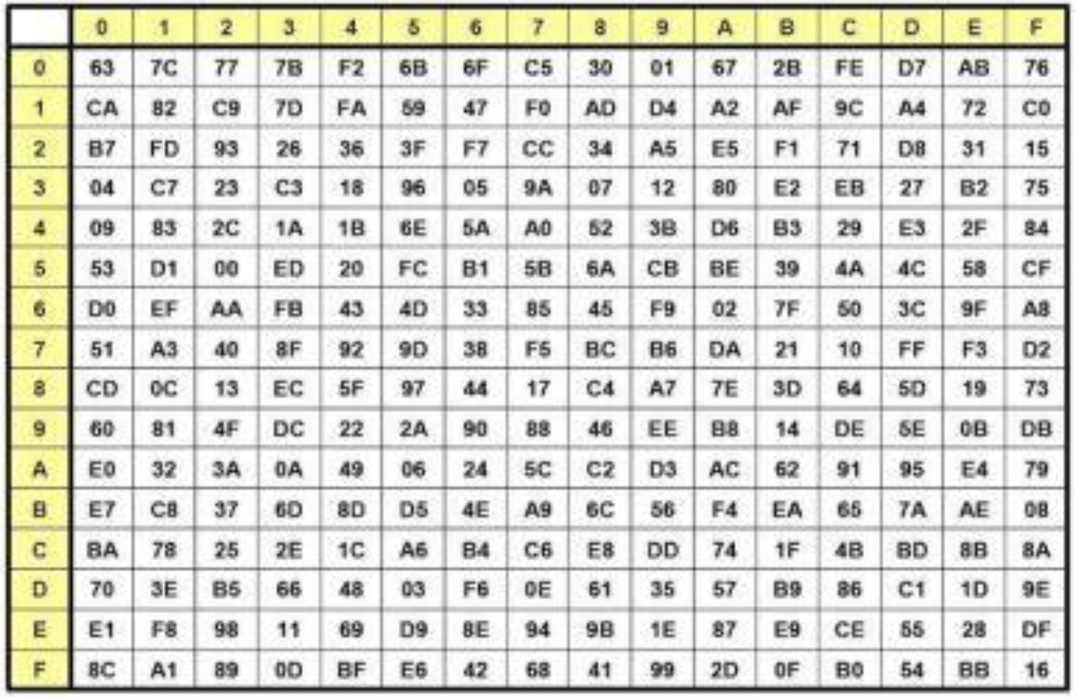
We derived from the playfair:

Ruled for encryption, decryption, and encryption the plaintext.

AES Cipher

We derived from the AES:

S-box table



	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

Rules for

encryption and decryption

Encryption

1. Letters in the same raw, shift to right one step.
2. Letters in the same column, shift to down one step.
3. Different, take letters on the horizontal opposite corner of the rectangle.

Decryption

1. Letters in the same raw, shift to lift one step.
2. Letters in the same column, shift to up one step.
3. Different, take letters on the horizontal opposite corner of the rectangle.

Encryption the plaintext

1. The plaintext is split into pairs of two letters.
2. Pair can not be made with same letter, break the letter in single and add "X" to the previous letter.
3. If the letter is standing alone, then add "Z" to it.
4. Change the plaintext to hex.

Example of encryption

The massage = " NETWORK "

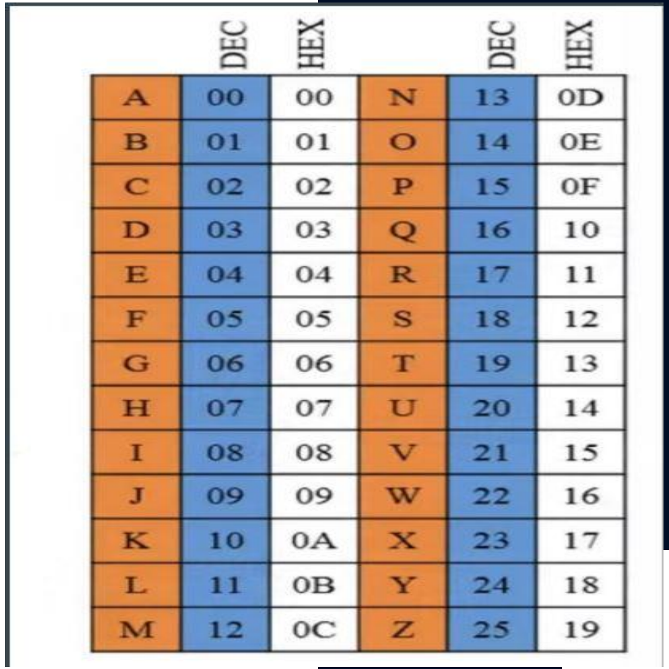
Steps for encryption:

1. Split into pairs

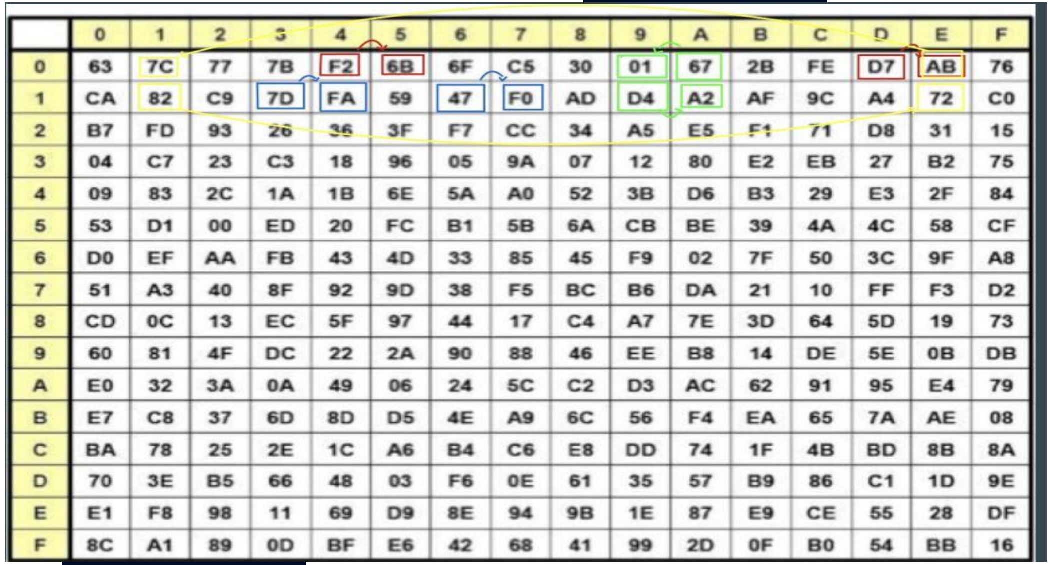
- NE – TW – OR – KZ   -

1. Change the plaintext to hex

- N = 0D – E = 04 – T = 13 – W = 16 – O = 0E – R = 11 – K = 0A – Z = 19 –
- then use S-box and rules of encryption:



	DEC	HEX		DEC	HEX
A	00	00	N	13	0D
B	01	01	O	14	0E
C	02	02	P	15	0F
D	03	03	Q	16	10
E	04	04	R	17	11
F	05	05	S	18	12
G	06	06	T	19	13
H	07	07	U	20	14
I	08	08	V	21	15
J	09	09	W	22	16
K	10	0A	X	23	17
L	11	0B	Y	24	18
M	12	0C	Z	25	19



	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

N = 0D = 0E   E = 04 = 05   T = 13 = 14   W = 16 = 17   O = 0E = 01

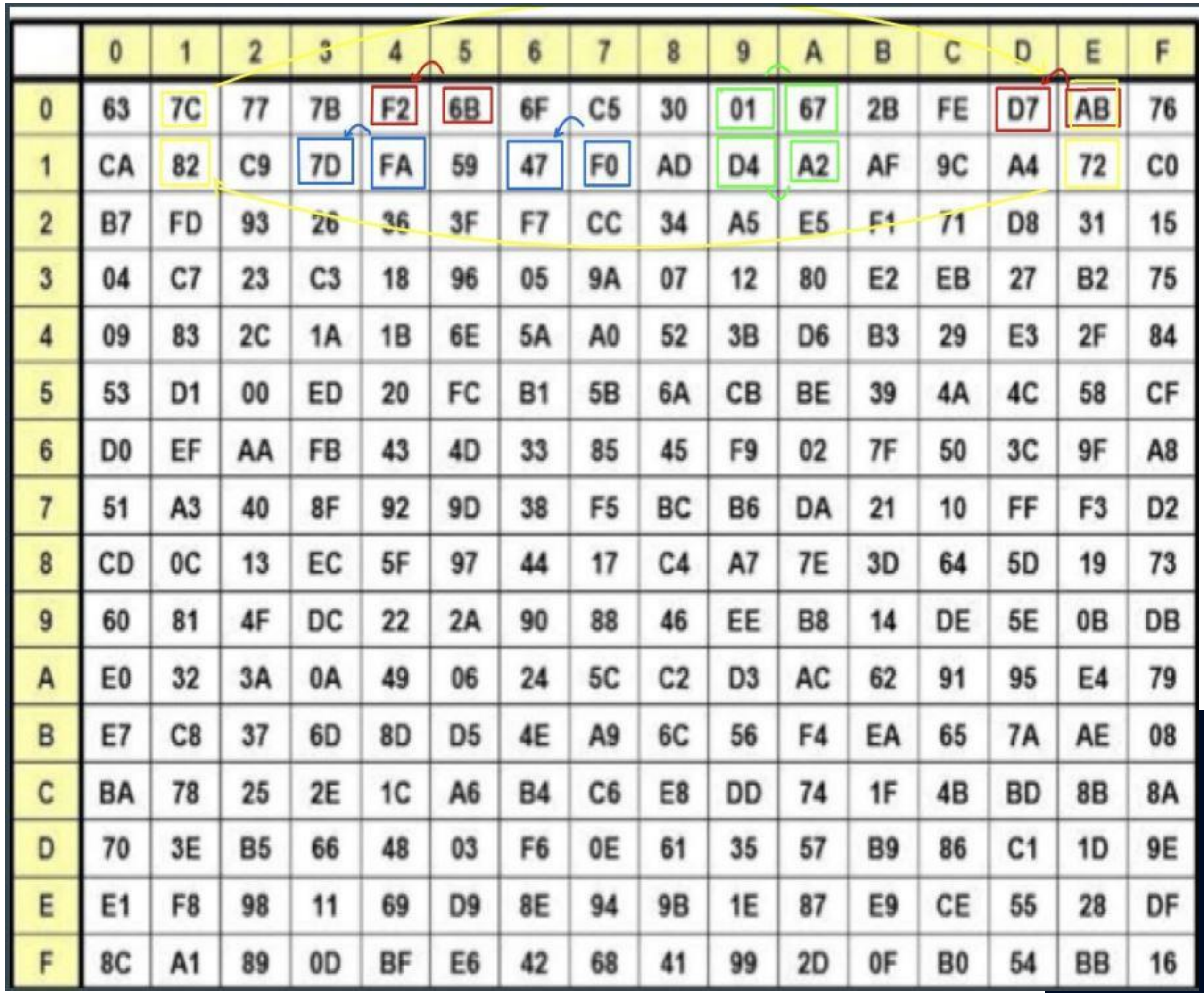
R = 11 = 1E   K = 0A = 09   Z = 19 = 1A

The ciphertext =" 03 05 14 17 01 1E 09 1A".

Example of decryption

Decryption:

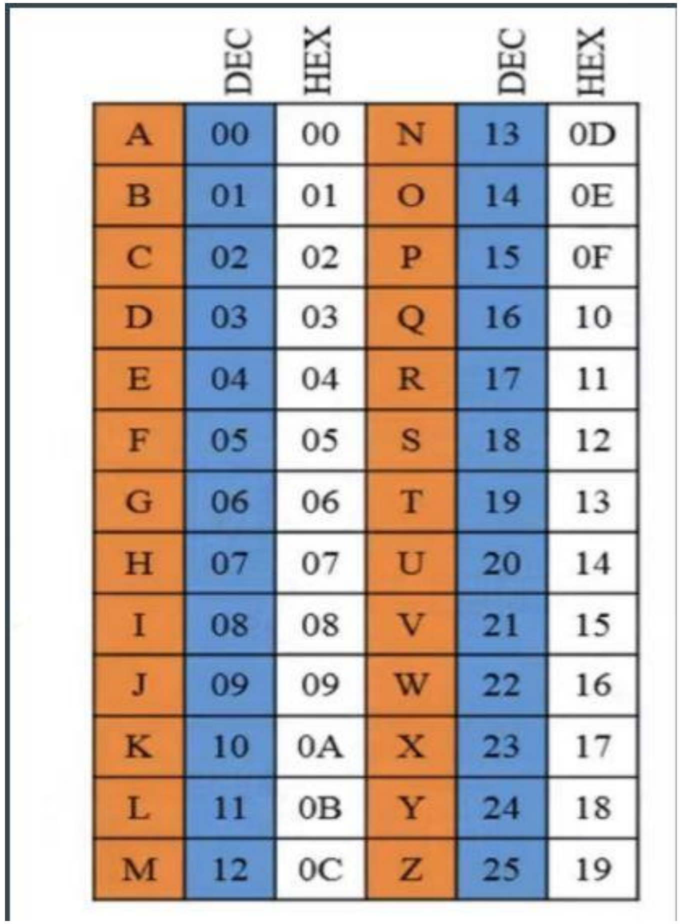
The ciphertext =" 03 05 14 17 01 1E 09 1A".



	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

The plaintext ="0D 04 13 16 0E 11 0A 19".

Plaintext after change



	DEC	HEX		DEC	HEX
A	00	00	N	13	0D
B	01	01	O	14	0E
C	02	02	P	15	0F
D	03	03	Q	16	10
E	04	04	R	17	11
F	05	05	S	18	12
G	06	06	T	19	13
H	07	07	U	20	14
I	08	08	V	21	15
J	09	09	W	22	16
K	10	0A	X	23	17
L	11	0B	Y	24	18
M	12	0C	Z	25	19

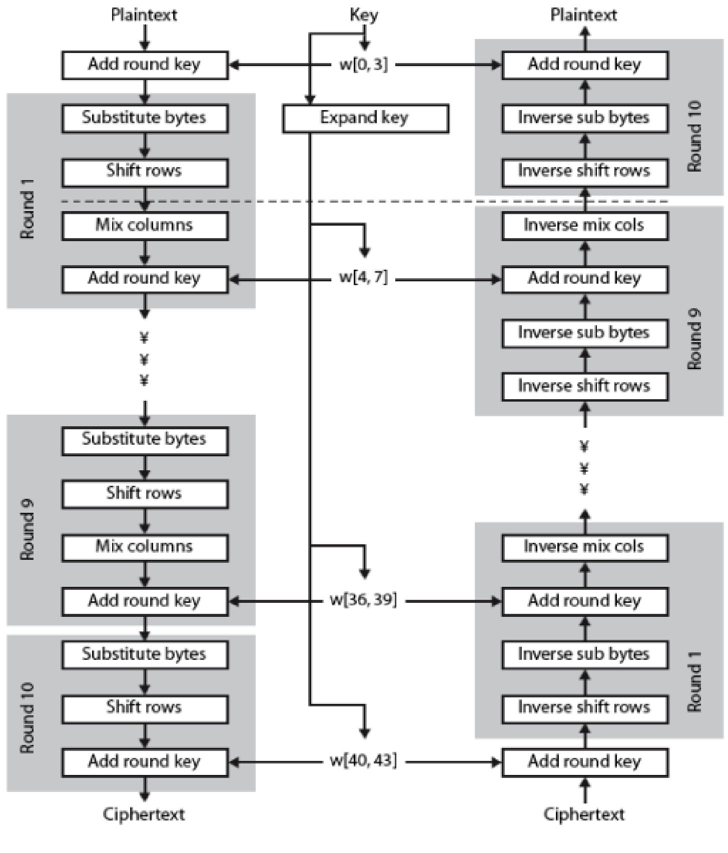
Plaintext ="NETWORKZ".

AES CIPHER

Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data

ENCRYPTION PROCESS

Encryption is a popular techniques that plays a major role to protect data from intruders. AES algorithm uses a particular structure to encrypt data to provide the best security. To do that it relies on a number of rounds and inside each round comprise of four sub-process. Each round consists of the following four steps to encrypt 128 bit block



(a) Encryption

(b) Decryption

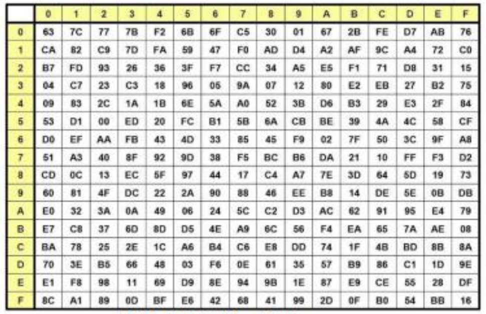
Fig. 1 Basic Structure of AES

A. Substitute Bytes Transformation

The first stage of each round starts with Sub-Bytes transformation. This stage is depends on nonlinear S-box to substitute a byte in the state to another byte.

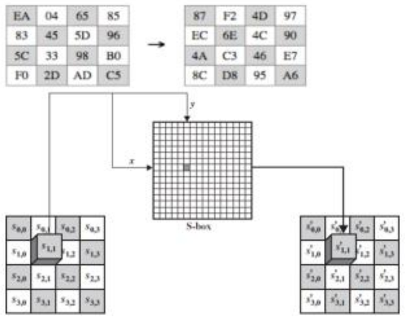
B. Shift-Rows Transformation

The next step after Sub-Byte that perform on the state is Shift-Row. The main idea behind this step is to shift bytes of the state cyclically to the left in each row rather than row number zero



	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

Table 1 AES S-box Table



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

→

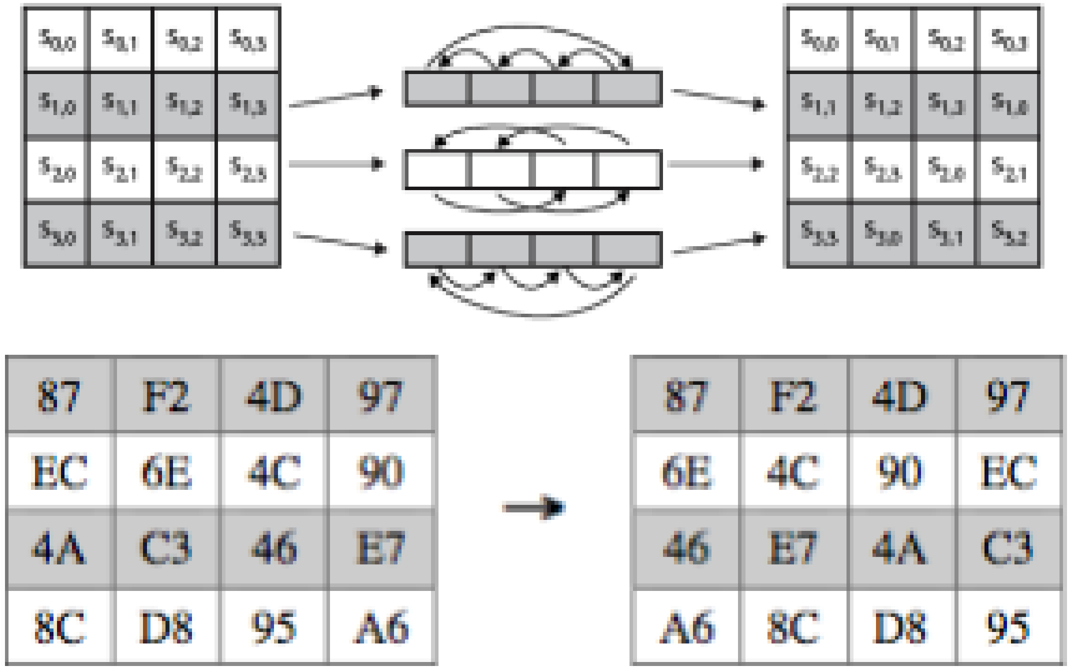
87	F2	4D	97
EC	6E	4C	90
4A	C3	46	E7
8C	D8	95	A6

y
x
S-box
$s_{0,0}$ $s_{0,1}$ $s_{0,2}$ $s_{0,3}$
$s_{1,0}$ $s_{1,1}$ $s_{1,2}$ $s_{1,3}$
$s_{2,0}$ $s_{2,1}$ $s_{2,2}$ $s_{2,3}$
$s_{3,0}$ $s_{3,1}$ $s_{3,2}$ $s_{3,3}$
$s'_{0,0}$ $s'_{0,1}$ $s'_{0,2}$ $s'_{0,3}$
$s'_{1,0}$ $s'_{1,1}$ $s'_{1,2}$ $s'_{1,3}$
$s'_{2,0}$ $s'_{2,1}$ $s'_{2,2}$ $s'_{2,3}$
$s'_{3,0}$ $s'_{3,1}$ $s'_{3,2}$ $s'_{3,3}$

Fig. 3 Substitute byte transformation

C. Mix-Columns Transformation

Another crucial step occurs of the state is Mix-Column. The multiplication is carried out of the state. Each byte of one row in matrix transformation multiply by each value (byte) of the state column.



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

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

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

→

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

Fig.4 Shift Rows

2	3	1	1
1	2	3	1
1	1	2	3
3	1	1	2

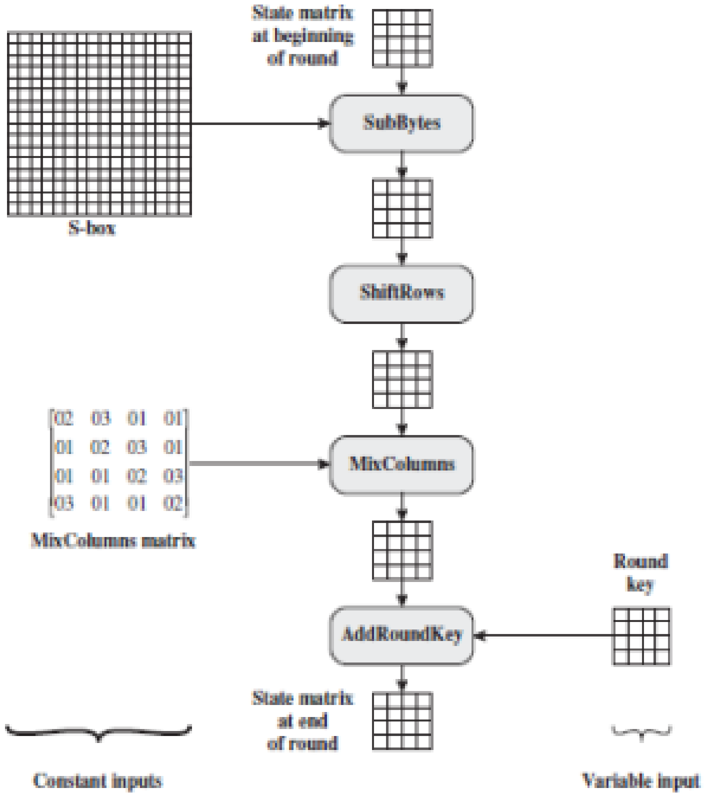
16 byte State

b1	b5	b9	b13
b2	b6	b10	b14
b3	b7	b11	b15
b4	b8	b12	b16

Fig. 5 Multiplication Matrix

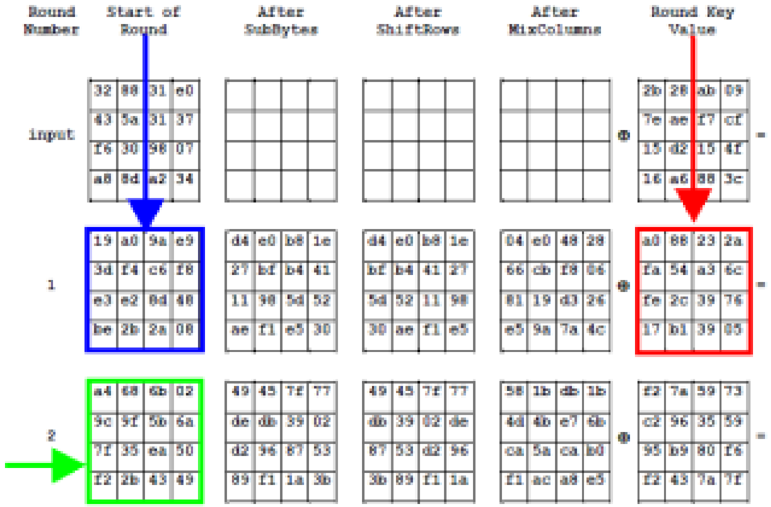
D. Add-Round-Key Transformation

Add-Round-Key is the most vital stage in AES algorithm. Both the key and the input data (also referred to as the state) are structured in a 4x4 matrix of bytes



$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}$$

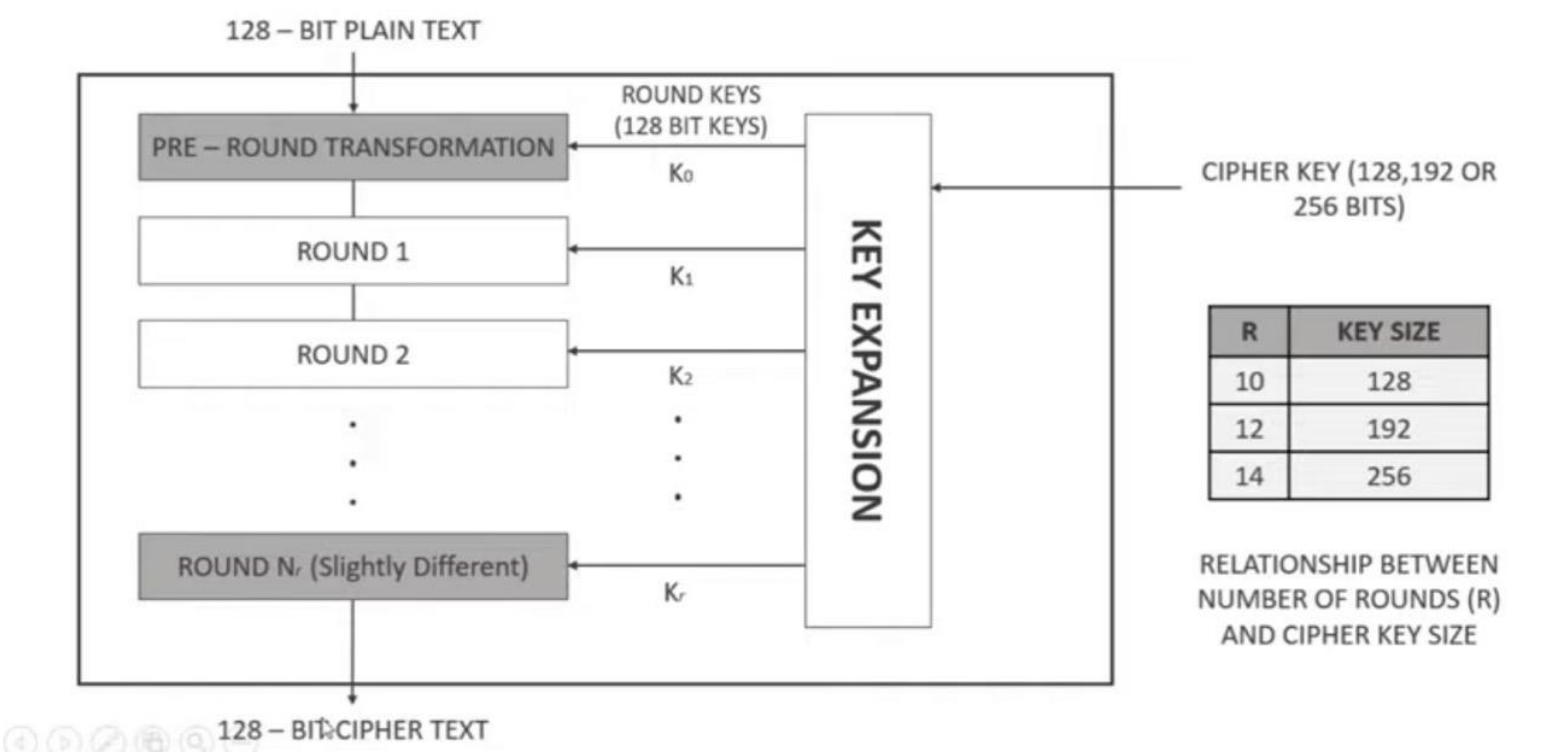
Fig.7 Inputs for Single AES Round



Round Number	Start of Round	After SubBytes	After ShiftRows	After MixColumns		Round Key Value	
input	32 88 31 e0				⊕	2b 28 ab 09	=
	43 5a 31 37					7e ae f7 cf	
	f6 30 98 07					15 d2 15 4f	
	a8 8d a2 34					16 a6 88 3c	
1	19 a0 9a e9	d4 e0 b8 1e	d4 e0 b8 1e	04 e0 48 28	⊕	a0 88 23 2a	=
	3d f4 c6 f8	27 bf b4 41	bf b4 41 27	66 cb f8 06		fa 54 a3 6c	
	e3 e2 8d 48	11 98 5d 52	5d 52 11 98	81 19 d3 26		fe 2c 39 76	
	be 2b 2a 08	ae f1 e5 30	30 ae f1 e5	e5 9a 7a 4c		17 b1 39 05	
2	a4 68 6b 02	49 45 7f 77	49 45 7f 77	58 1b db 1b	⊕	f2 7a 59 73	=
	9c 9f 5b 6a	de db 39 02	db 39 02 de	4d 4b e7 6b		c2 96 35 59	
	7f 35 ea 50	d2 96 87 53	87 53 d2 96	ca 5a ca b0		95 b9 80 f6	
	f2 2b 43 49	89 f1 1a 3b	3b 89 f1 1a	f1 ac a8 e5		f2 43 7a 7f	

Fig. 6 Add Round Key

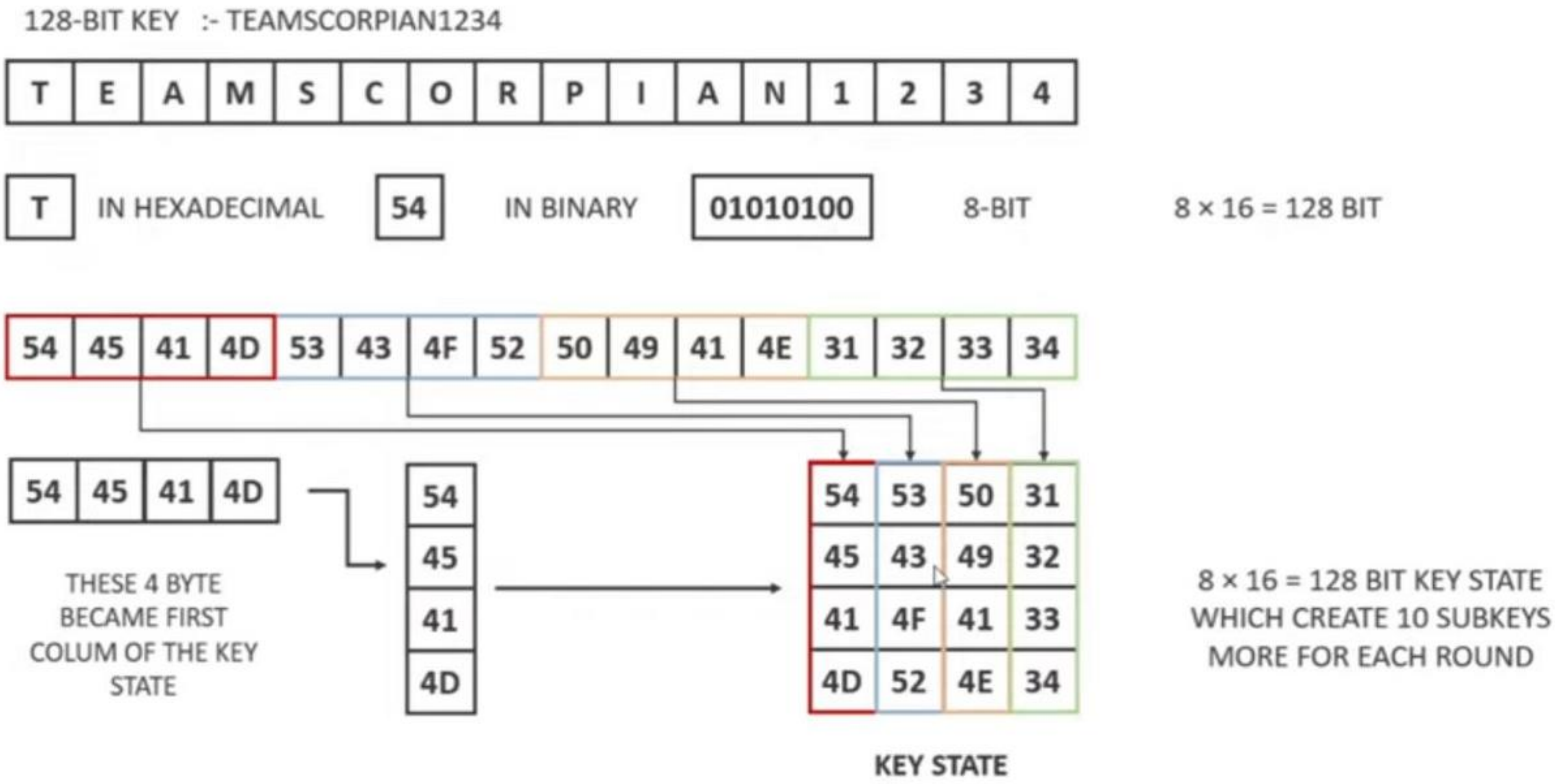
AES ENCRYPTION



R	KEY SIZE
10	128
12	192
14	256

RELATIONSHIP BETWEEN NUMBER OF ROUNDS (R) AND CIPHER KEY SIZE

KEY GENERATION



128-BIT KEY :- TEAMSCORPIAN1234

T	E	A	M	S	C	O	R	P	I	A	N	1	2	3	4

T IN HEXADECIMAL 54 IN BINARY 01010100 8-BIT 8 × 16 = 128 BIT

54	45	41	4D	53	43	4F	52	50	49	41	4E	31	32	33	34

54	45	41	4D

54
45
41
4D

THESE 4 BYTE BECAME FIRST COLUM OF THE KEY STATE

54	53	50	31
45	43	49	32
41	4F	41	33
4D	52	4E	34

KEY STATE

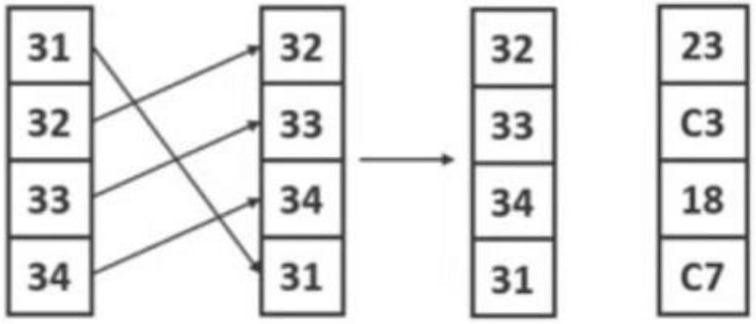
8 × 16 = 128 BIT KEY STATE WHICH CREATE 10 SUBKEYS MORE FOR EACH ROUND

SUB – KEY GENERATION

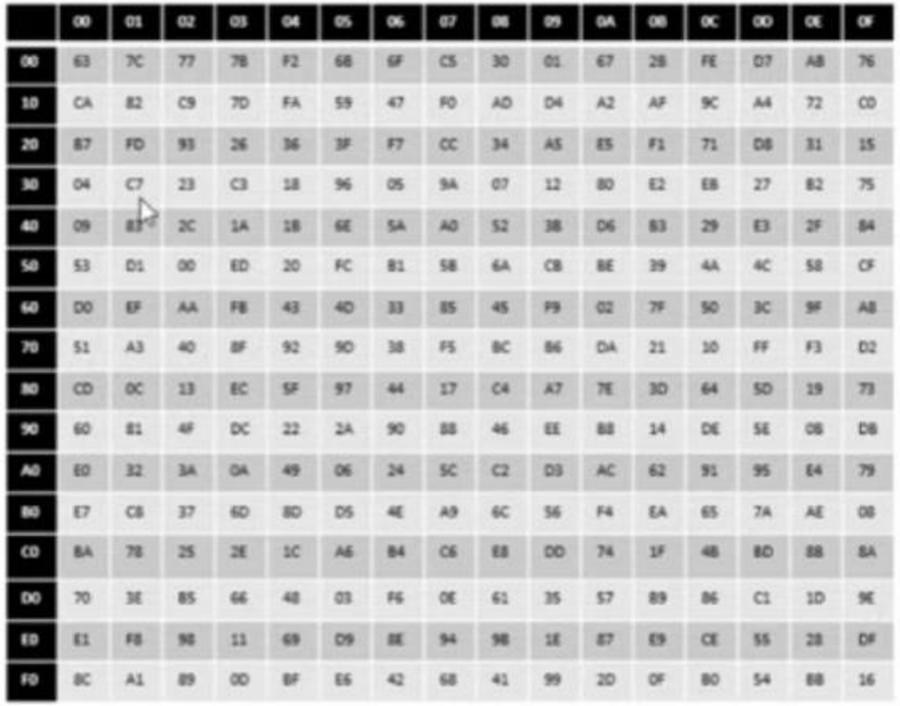
KEY STATE

54	53	50	31
45	43	49	32
41	4F	41	33
4D	52	4E	34

TAKING LAST COLUM OF
KEY AND DO ROTWORD



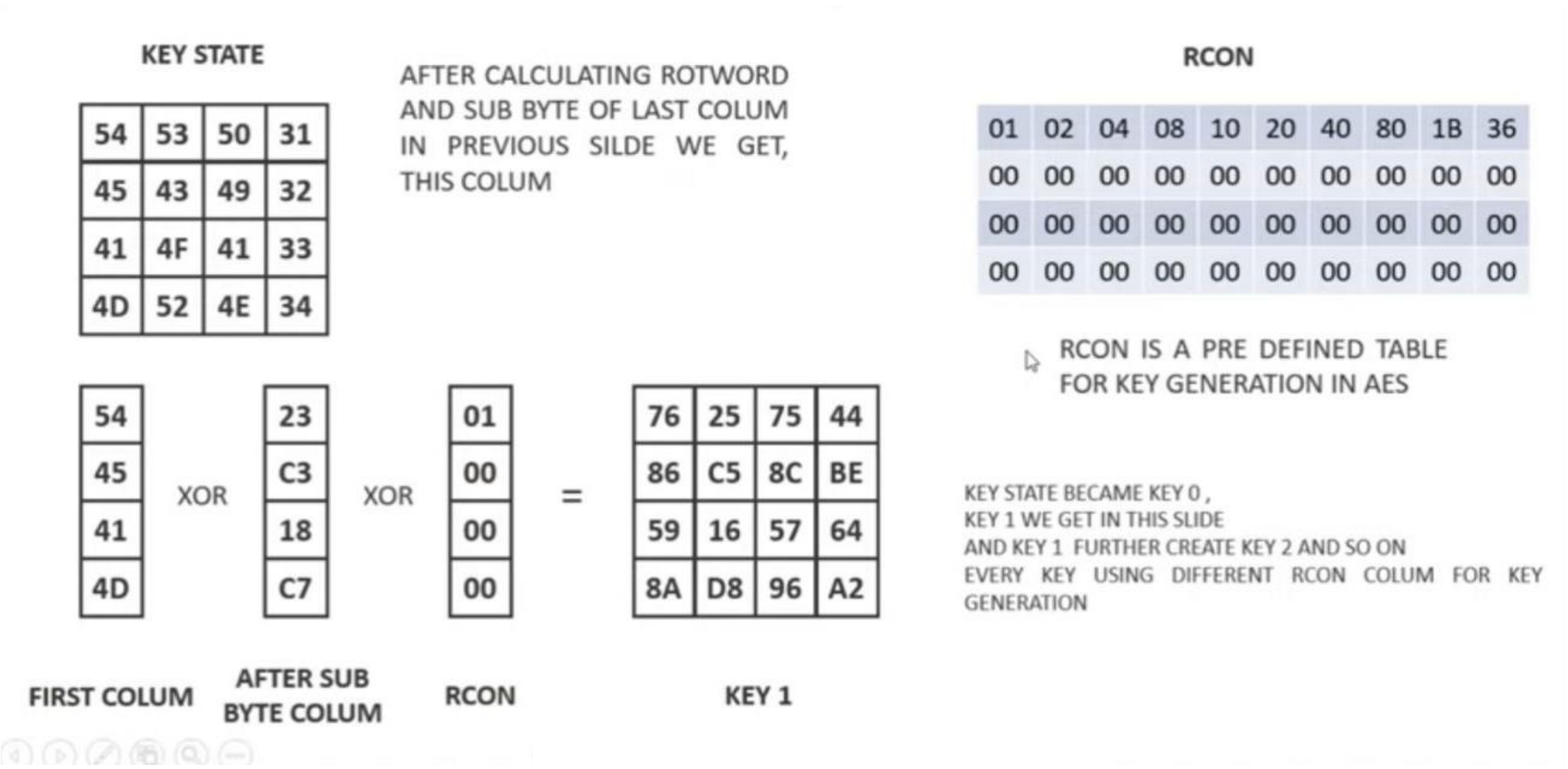
ROT WORD



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

IN SUB BYTE FIRST HEXA DECIMAL CHARACTER
BECOME ROW AND SECOND BECAME COLUM
AND ITERSECTION POINT BECAME NEW BYTE

SUB – KEY GENERATION



KEY STATE

54	53	50	31
45	43	49	32
41	4F	41	33
4D	52	4E	34

AFTER CALCULATING ROTWORD AND SUB BYTE OF LAST COLUM IN PREVIOUS SILDE WE GET, THIS COLUM

RCON

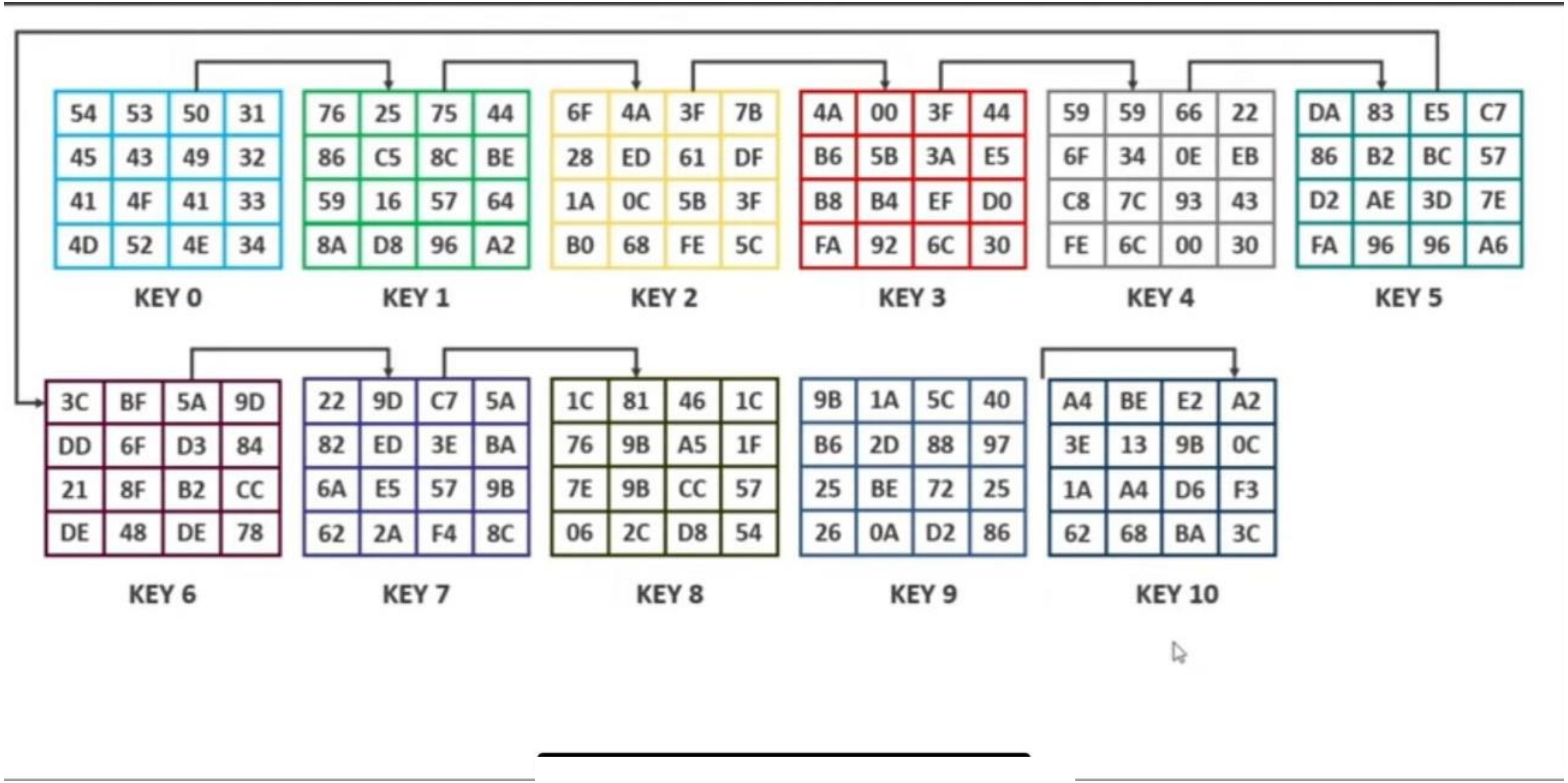
01	02	04	08	10	20	40	80	1B	36
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00

RCON IS A PRE DEFINED TABLE FOR KEY GENERATION IN AES

FIRST COLUM		AFTER SUB BYTE COLUM		RCON		KEY 1			
54		23		01		76	25	75	44
45	XOR	C3	XOR	00	=	86	C5	8C	BE
41		18		00		59	16	57	64
4D		C7		00		8A	D8	96	A2

KEY STATE BECAME KEY 0 ,
KEY 1 WE GET IN THIS SLIDE
AND KEY 1 FURTHER CREATE KEY 2 AND SO ON
EVERY KEY USING DIFFERENT RCON COLUM FOR KEY GENERATION

SUB – KEYS



KEY 0

54	53	50	31
45	43	49	32
41	4F	41	33
4D	52	4E	34

KEY 1

76	25	75	44
86	C5	8C	BE
59	16	57	64
8A	D8	96	A2

KEY 2

6F	4A	3F	7B
28	ED	61	DF
1A	0C	5B	3F
B0	68	FE	5C

KEY 3

4A	00	3F	44
B6	5B	3A	E5
B8	B4	EF	D0
FA	92	6C	30

KEY 4

59	59	66	22
6F	34	0E	EB
C8	7C	93	43
FE	6C	00	30

KEY 5

DA	83	E5	C7
86	B2	BC	57
D2	AE	3D	7E
FA	96	96	A6

KEY 6

3C	BF	5A	9D
DD	6F	D3	84
21	8F	B2	CC
DE	48	DE	78

KEY 7

22	9D	C7	5A
82	ED	3E	BA
6A	E5	57	9B
62	2A	F4	8C

KEY 8

1C	81	46	1C
76	9B	A5	1F
7E	9B	CC	57
06	2C	D8	54

KEY 9

9B	1A	5C	40
B6	2D	88	97
25	BE	72	25
26	0A	D2	86

KEY 10

A4	BE	E2	A2
3E	13	9B	0C
1A	A4	D6	F3
62	68	BA	3C

DECRYPTION PROCESS

The decryption is the process to obtain the original data that was encrypted. This process is based on the key that was received from the sender of the data. The decryption processes of an AES is similar to the encryption process in the reverse order and both sender and receiver have the same key to encrypt and decrypt data.

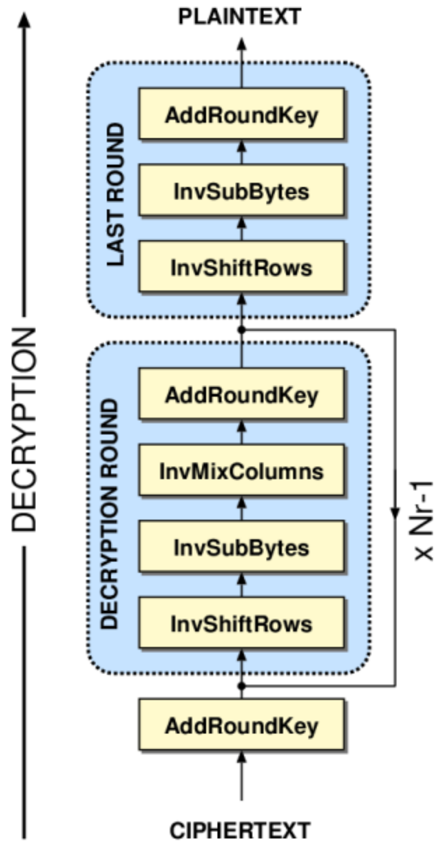


Fig. 15 Decryption Processes

THANK YOU