Information Security

NATIONAL UNIVERSITY OF COMPUTER & EMERGING SCIENCES

MOTIVATION

- Cryptography is an essential component of cyber security.
- The need to protect sensitive information and ensure the integrity of industrial control processes has placed a premium on cyber security skills in today's information technology market.
- Demand for cyber security jobs is expected to rise 6 million globally by 2019, with a projected shortfall of 1.5 million, according to Symantec, the world's largest security software vendor.
- According to Forbes, the cyber security market is expected to grow from $75 billion in 2015 to $170 billion by 2020.

TODAY'S LECTURE

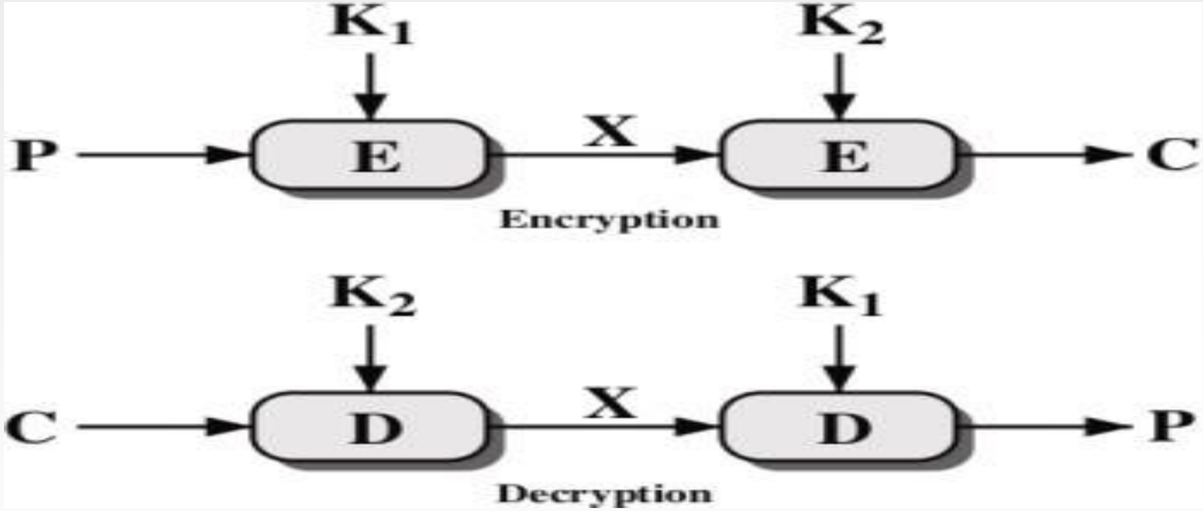
- Block Ciphers
  - Data Encryption Standard (DES)
    - DES Encryption / Decryption
    - Strength of DES
    - Weakness of DES
  - Multiple DES Encryption
  - Double DES
  - Meet-in-the Middle Attack
  - Triple DES
  - Advance Encryption Standard (AES)

DES WEAKNESS

- DES is vulnerable to brute force attack due to small key size
- $2^{56} = 72{,}057{,}594{,}037{,}927{,}936$ The number of different possible keys in the obsolete 56 bit DES symmetric cipher.
- Alternative block cipher that makes use of DES software/equipment/knowledge: encrypt multiple times with different keys options:
  - Double DES
  - Triple DES

DOUBLE DES

- For DES, 2 × 56-bit keys, meaning 112-bit key length
- Meet-in-the-middle attack makes it easier



MEET-IN-THE-MIDDLE ATTACK

- Double DES Encryption: $C = E(K2; E(K1; P))$
- Say $E(K1; P) = X = D(K2; C)$
  - Attacker knows two plaintext, ciphertext pairs $(Pa; Ca)$ and $(Pb; Cb)$ Encrypt Pa using all 2^{56} values of $K1$ to get multiple values of X
  - Store results in table and sort by X
  - Decrypt Ca using all 2^{56} values of $K2$
  - As each decryption result produced, check against table
  - If match, check current $K1; K2$ on Cb. If Pb obtained, then accept the keys
- With two known plaintext, ciphertext pairs, probability of successful attack is almost 1
- Encrypt/decrypt operations required: 2^{56} (twice as many as single DES)

EXAMPLE: MEET-IN-THE-MIDDLE ATTACK

Example 5 Bit Block Cipher

P	Ciphertext for key, K:							
	000	*001*	*010*	*011*	*100*	*101*	*110*	*111*
00000	00001	10010	01101	01111	11011	10011	10000	11101
00001	10001	01001	11010	10000	01010	11100	10100	01010
00010	01011	10100	11011	01100	00100	10100	00111	00100
00011	01110	10110	01011	00111	10110	11101	11000	00101
00100	00011	00011	00001	11101	11001	10010	11011	01100
00101	10100	10111	01110	00010	01101	00011	01101	00110
00110	10101	11111	00110	10011	00010	10001	10111	10110
00111	01101	10001	10111	00110	11111	01100	11100	10011
01000	01000	11011	10011	01010	01001	10110	10011	11111
01001	10010	11110	10001	10101	01111	00100	00000	01110
01010	01111	00010	10000	10110	11000	01010	00001	00010
01011	11110	01110	00111	01011	11101	11011	01111	10010
01100	11011	10000	01010	00101	01100	00101	01100	00111
01101	11101	00111	10110	01000	01000	10111	10010	11100
01110	11000	01000	10100	00000	11010	01111	11111	01000
01111	01001	11101	01100	00001	00011	01000	01010	01101
10000	00110	11100	01111	01001	01011	11111	00010	11011
10001	11111	01100	10010	10010	00000	11010	11110	00000
10010	10110	10011	11110	01101	10111	01101	10001	10000
10011	00010	00001	11000	11100	10100	00111	00011	10111
10100	10111	01101	11001	11111	10011	00000	00100	00011
10101	01010	01111	00101	00011	00001	01001	10101	01011
10110	00000	00110	10101	11010	00110	01011	01000	11001
10111	00111	11000	01001	11110	10000	00010	01110	10100
11000	00101	01011	00010	10001	11100	10000	11010	10001
11001	11100	00000	11101	10111	10001	01110	00101	11000
11010	11010	11001	01000	01110	01110	11110	01011	01001
11011	01100	11010	11111	11001	10101	00001	10110	00001

TRIPLE DES (3DES)

- We saw that Double-DES has a key length of 112 bits, but meet-in-the-middle attack against Double-DES reduces its work factor to about the same as DES. Thus, it is no more secure than DES. So let’s move on to 3DES.

3DES PERFORMANCE

- 3DES uses 48 rounds in its computation, which makes it highly resistant to differential cryptanalysis. However, because of the extra work 3DES performs, there is a heavy performance hit. It can take up to three times longer than DES to perform encryption and decryption.

3DES MODES

- **DES-EEE3** Uses three different keys for encryption, and the data are encrypted, encrypted, encrypted
- **DES-EDE3** Uses three different keys for encryption, and the data are encrypted, decrypted, and encrypted
- **DES-EEE2** The same as DES-EEE3 but uses only two keys, and the first and third encryption processes use the same key
- **DES-EDE2** The same as DES-EDE3 but uses only two keys, and the first and third encryption processes use the same key

ADVANCED ENCRYPTION STANDARD (AES)

- After DES was used as an encryption standard for over 20 years and it was cracked in a relatively short time once the necessary technology was available, NIST decided a new standard, the Advanced Encryption Standard (AES), needed to be put into place.

AES Selection Process

- September 12, 1997: the NIST publicly calls for nominees for the new AES
- 1st AES conference, August 20-23, 1998
  - (15 algorithms are candidates for becoming AES)
- Public Review of the algorithms
- 2nd AES conference, March 22-23, 1999
  - (presentation, analysis and testing)
- August 9, 1999: the 5 finalists are announced
  - (MARS, RC6, RINJDAEL, SERPENT, TWOFISH)
- Public Review
- 3rd AES conferece, April 13-14, 2000
  - (presentation, analysis and testing)

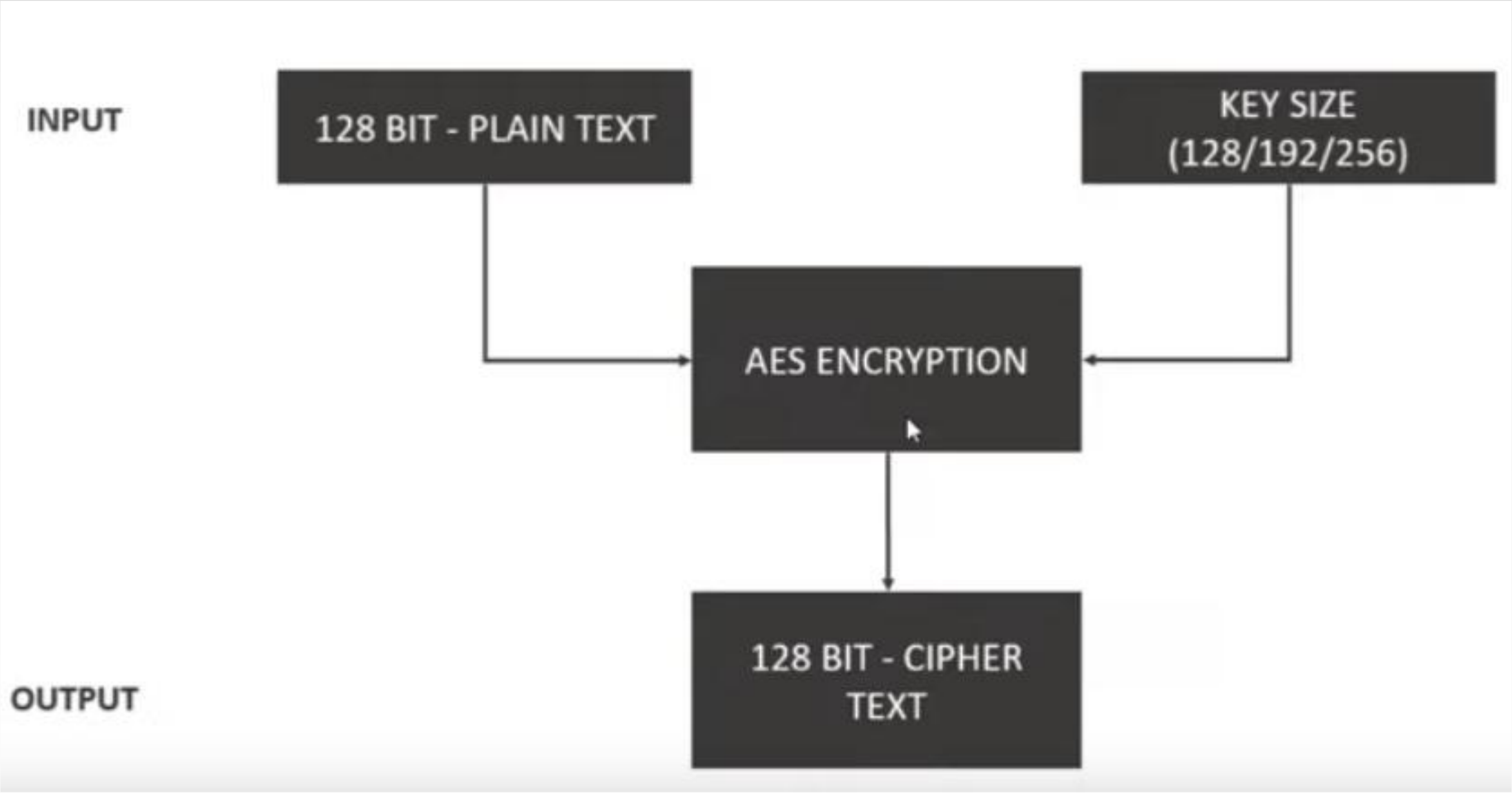
AES

- Rijndael chosen, standard called AES created in 2001
- AES:
  - Symmetric key symmetric block cipher
  - Block size: 128 bits (others possible)
  - Key size: 128, 192, 256 bits
  - Rounds: 10, 12, 14 (depending on key)
  - Operations: XOR with round key, substitutions using S-Boxes, mixing using Galois Field arithmetic
  - Widely used in file encryption, network communications
  - Generally considered secure

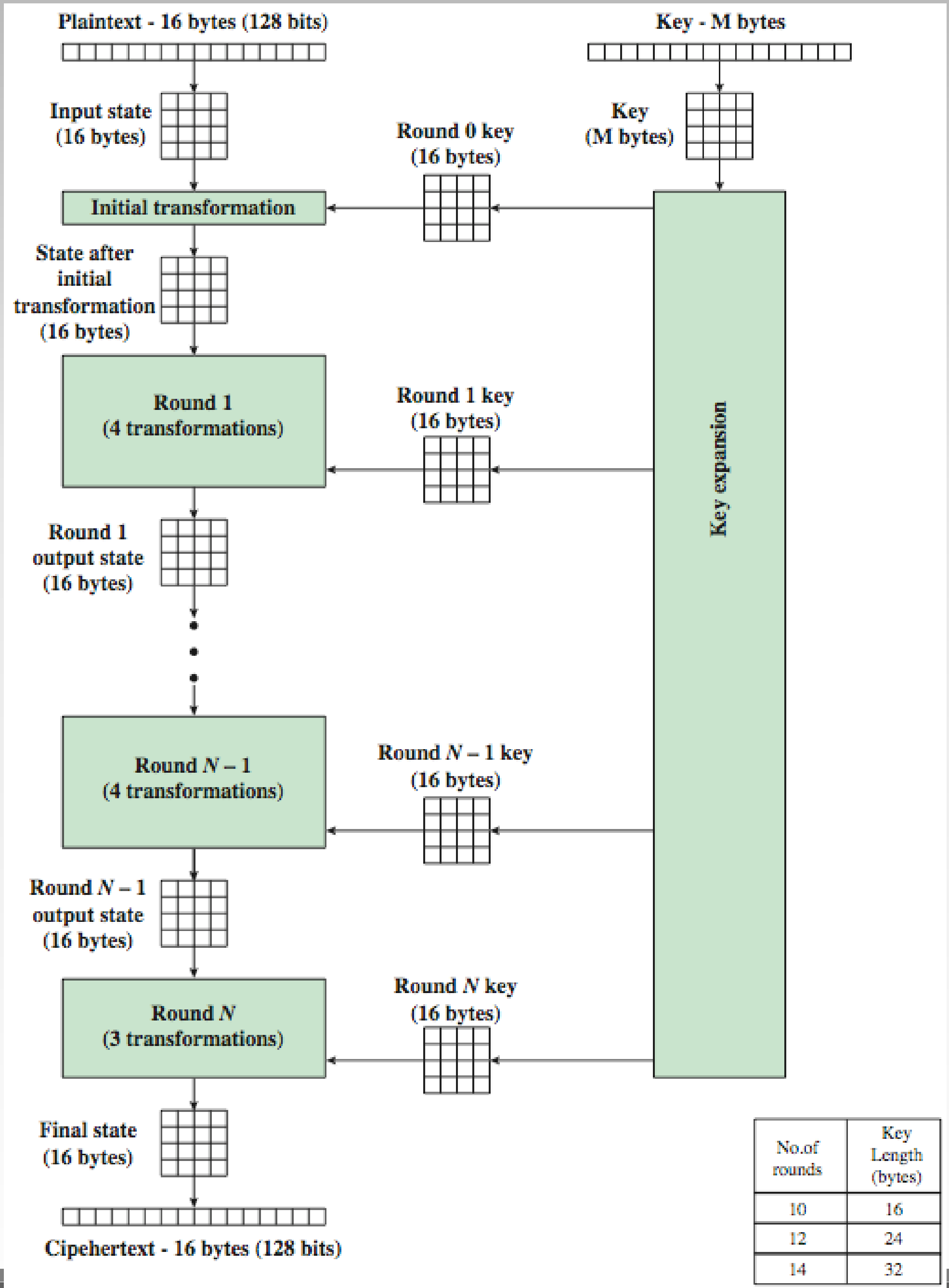
AES

- AES:
  - Stronger and faster than Triple-DES and six time faster.
  - Widely adopted symmetric encryption algorithm
  - AES based Rijndael cipher developed by two Belgian cryptographers; Vincent Rijmen and Joan Daemen.

AES Working Mechanism

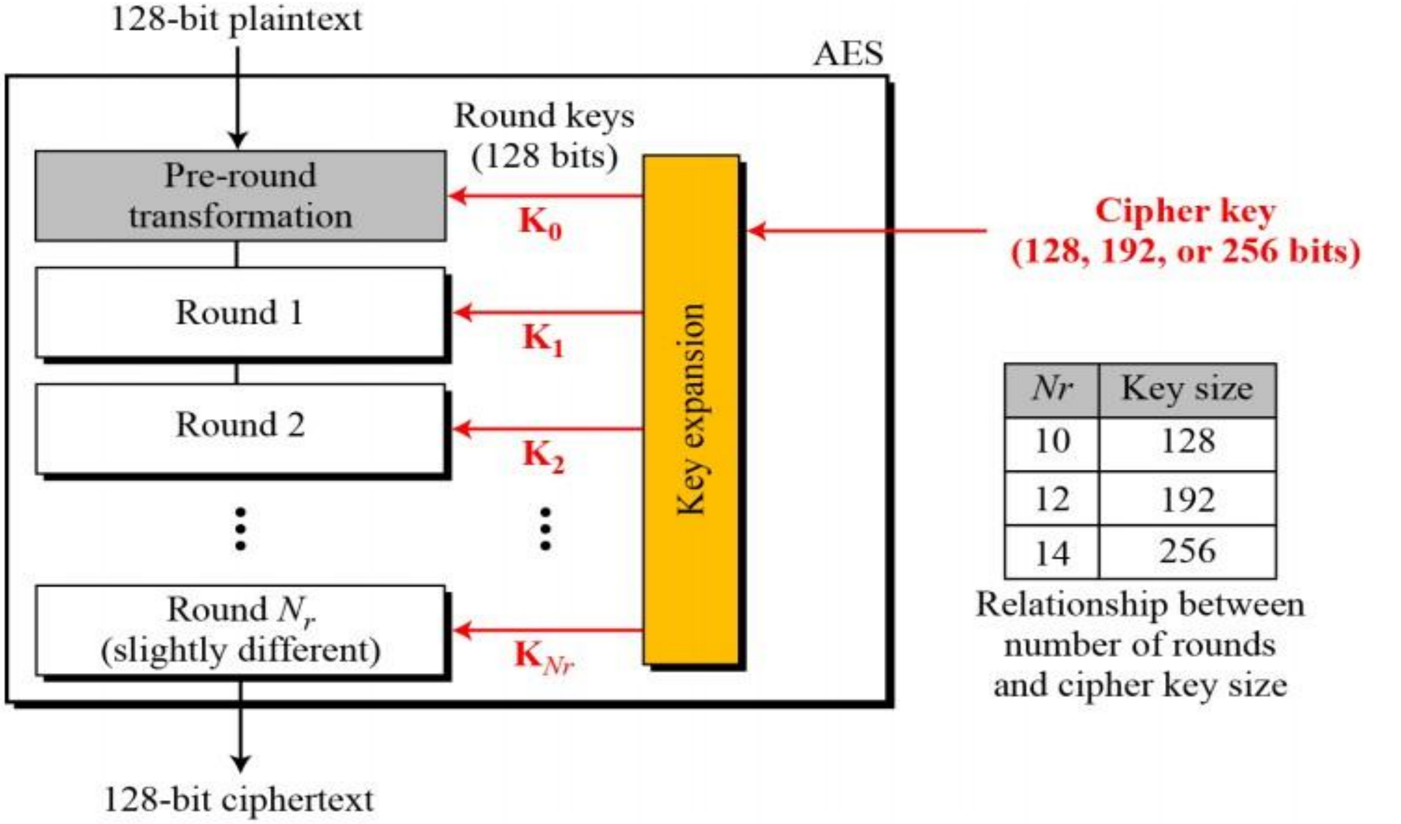


AES Encryption Process



No.of rounds	Key Length (bytes)
10	16
12	24
14	32

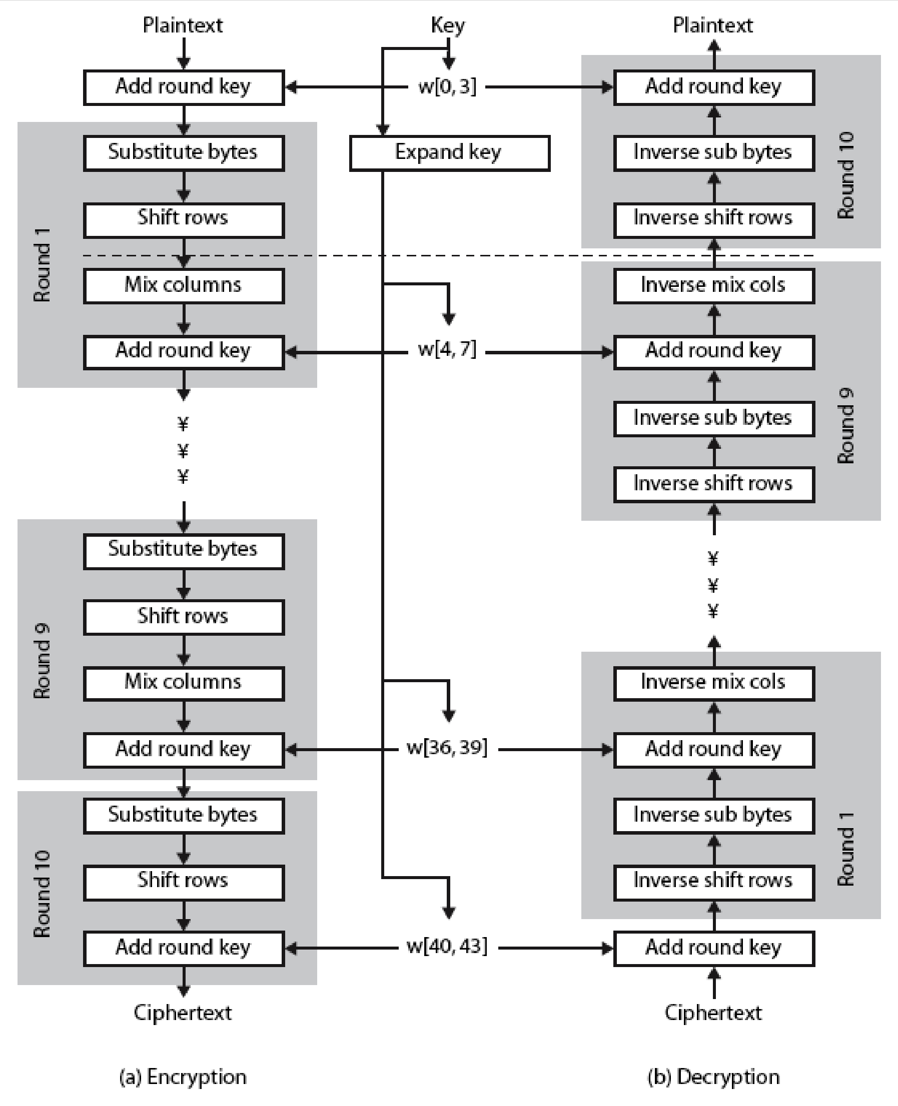
AES Encryption Process



Nr	Key size
10	128
12	192
14	256

Relationship between number of rounds and cipher key size

AES Structure



The AES Cipher

- Assume 128 bit block as input
- Input blocks represented as states at intermediates stages.

Input

in_0	in_4	in_8	in_{12}
in_1	in_5	in9	in13
in2	in6	in10	in14
in3	in7	in11	in15

State array

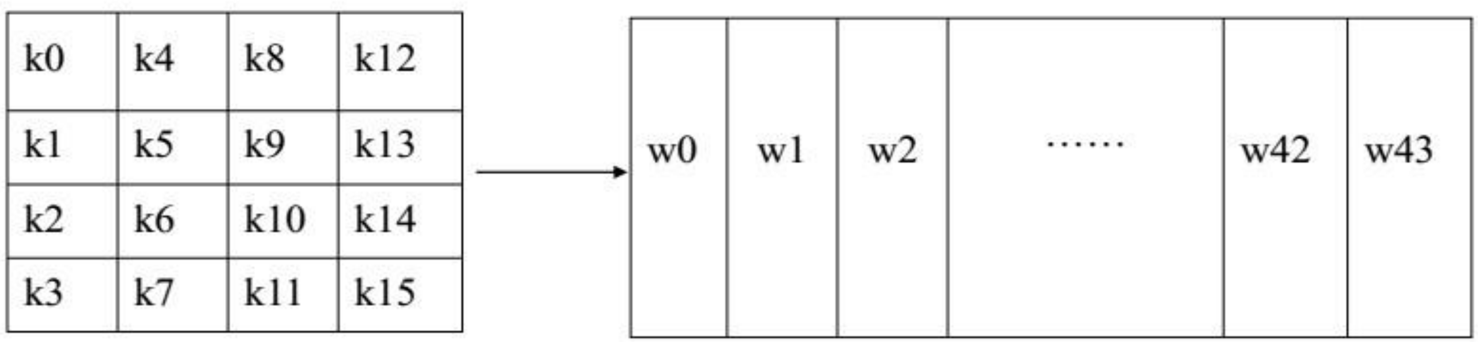
$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,3}$
$S_{1,0}$	$S_{1,1}$	$S_{1,2}$	$S_{1,3}$
$S_{2,0}$	$S_{2,1}$	$S_{2,2}$	$S_{2,3}$
$S_{3,0}$	$S_{3,1}$	$S_{3,2}$	$S_{3,3}$

Output

out0	out 4	out8	out12
out1	out5	out9	out13
out2	out6	out10	out14
out3	out7	out11	out15

The AES Cipher

- Key received as input array of 4 rows and N_k columns.
- N_k = 4,6, or 8, parameter which depends key size 128,192 or 256.
- Input key is expanded into an array of 44/52/60 words of 32 bits each depending upon key size.
- 4 different words serve as a key for each round.



Process In AES

There are two steps in AES: Key Generation & Rounds

- Key Generation:
  - ROT word of last Column
  - Sub Byte of ROT word
  - XOR with RCON and First Column of key and Sub-byte
  - Result become first column of round key one
- Round:

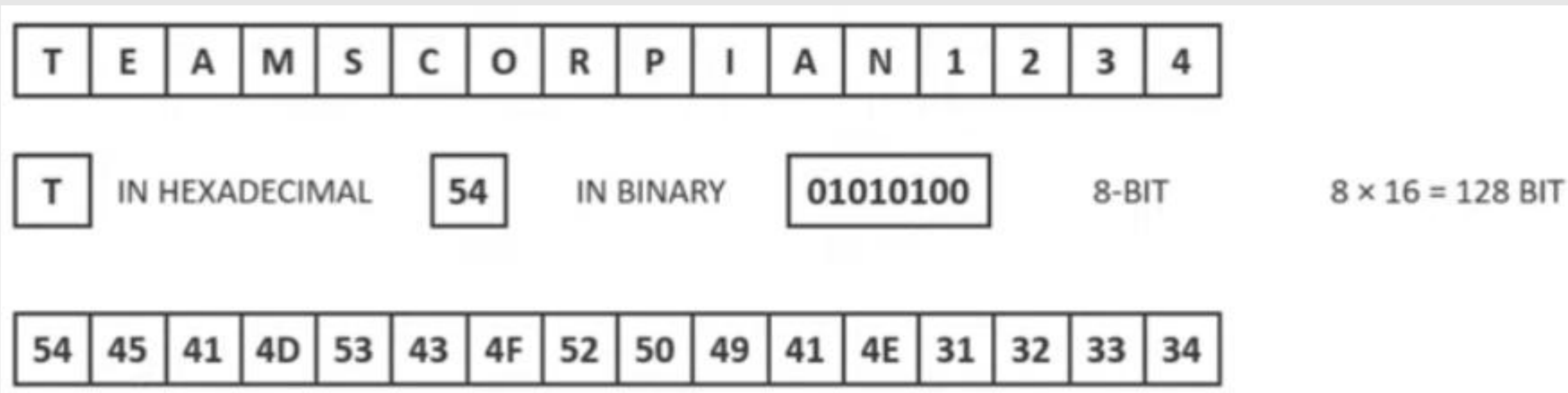
Initial Round	Main Round	Final Round
• XOR with round key 0	• Sub byte • Shift rows • Mix Columns • Add round key	• Sub byte • Shift rows • Add round key

AES Key Expansion

- Takes 128-bit (16-byte) key and expands into array of 44/52/60 32-bit words
- Start by copying key into first 4 words
- 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

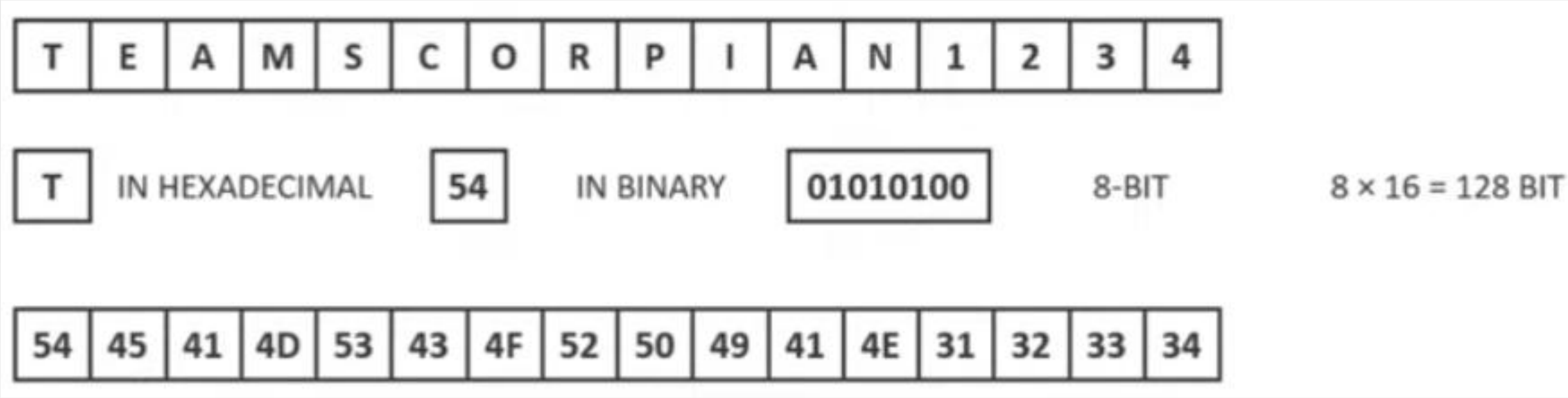
Key Generation

128-bit Key: **TEAMSCORPIAN1234**



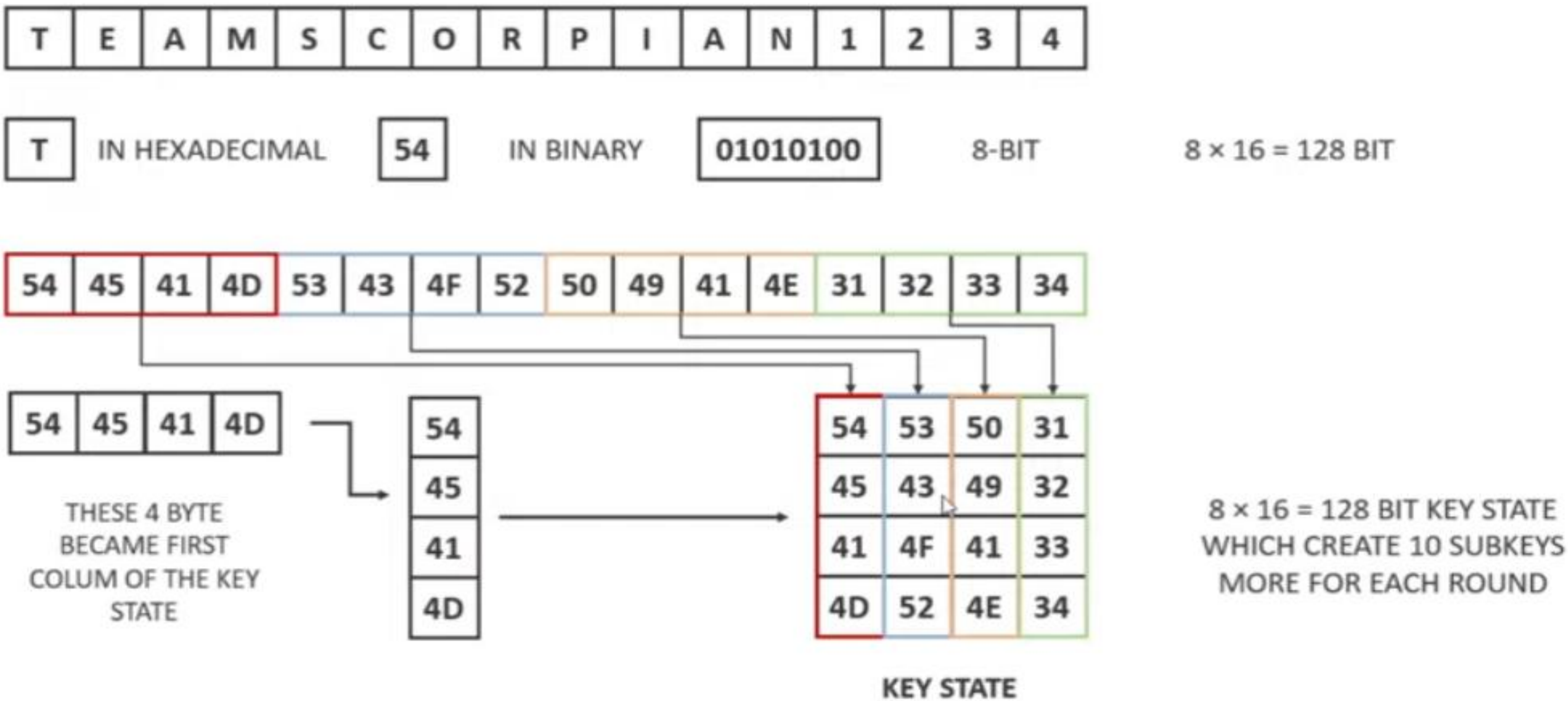
Key Generation

- 128-bit Key: **TEAMSCORPIAN1234**



- Every single column is a byte as well: 8bits = 1 Byte

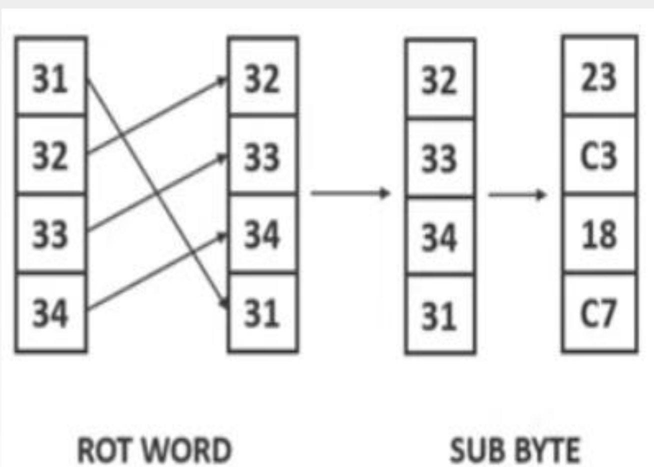
Key Generation



Sub-Key Generation from Key State

KEY STATE

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



SubBytes transformation 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	CB	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

Sub-Key Generation from Key State

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

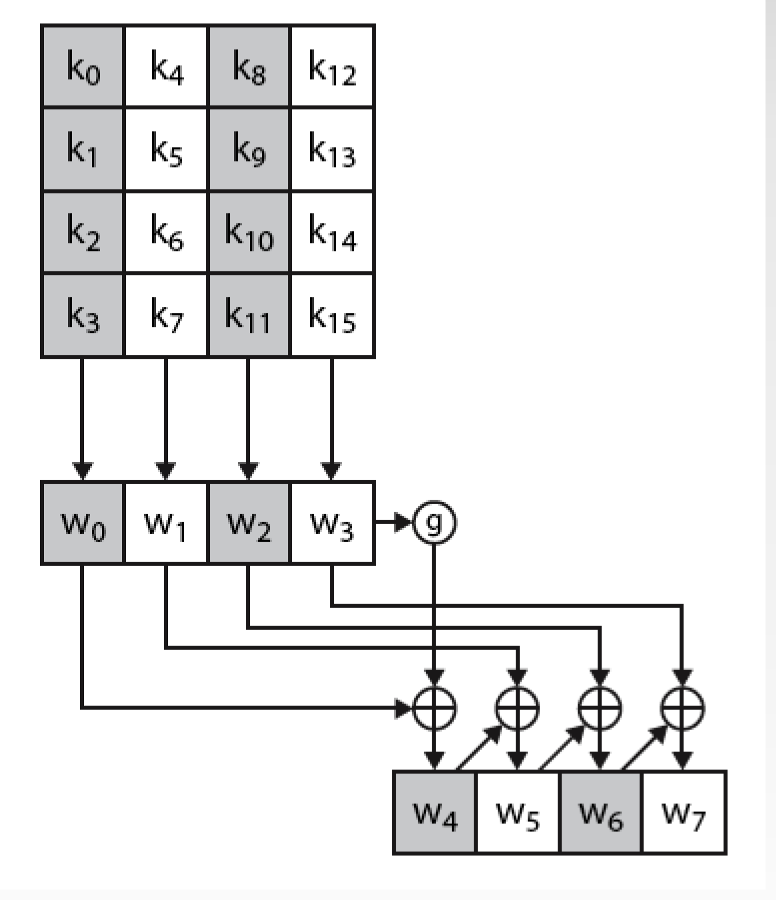
01	02	04	08	10	20	40	80	1B	36
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00

RCON IS A PRE DEFINED TABLE FOR KEY GENERATION IN AES

54		23		01		76
45	XOR	C3	XOR	00	=	86
41		18		00		59
4D		C7		00		8A

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

AES Key Expansion

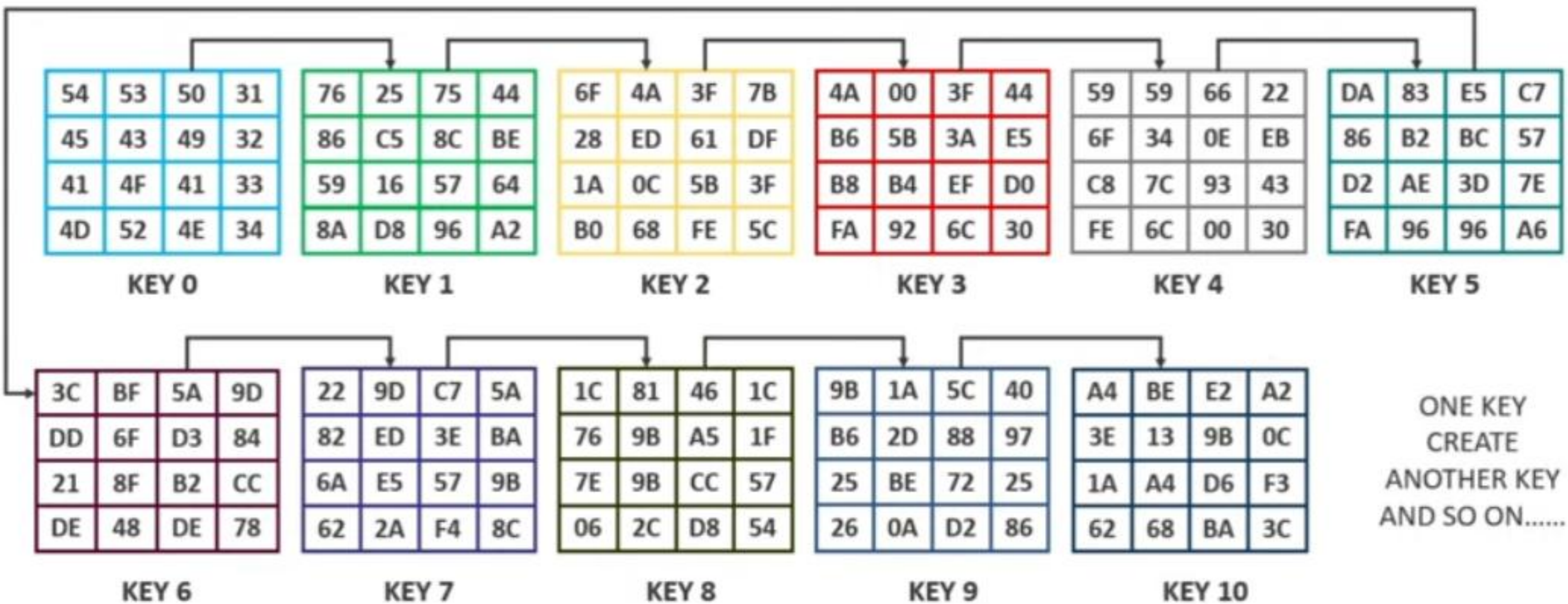


Class Participation:

“Participation012”: generate the first 2 keys

Hex	Value	Hex	Value	Hex	Value	Hex	Value	Hex	Value	Hex	Value	Hex	Value	Hex	Value
00	NUL	10	DLE	20	SP	30	0	40	@	50	P	60	`	70	p
01	SOH	11	DC1	21	!	31	1	41	A	51	Q	61	a	71	q
02	STX	12	DC2	22	"	32	2	42	B	52	R	62	b	72	r
03	ETX	13	DC3	23	#	33	3	43	C	53	S	63	c	73	s
04	EOT	14	DC4	24	$	34	4	44	D	54	T	64	d	74	t
05	ENQ	15	NAK	25	%	35	5	45	E	55	U	65	e	75	u
06	ACK	16	SYN	26	&	36	6	46	F	56	V	66	f	76	v
07	BEL	17	ETB	27	'	37	7	47	G	57	W	67	g	77	w
08	BS	18	CAN	28	(	38	8	48	H	58	X	68	h	78	x
09	HT	19	EM	29	)	39	9	49	I	59	Y	69	i	79	y
0A	LF	1A	SUB	2A	*	3A	:	4A	J	5A	Z	6A	j	7A	z
0B	VT	1B	ESC	2B	+	3B	;	4B	K	5B	[	6B	k	7B	{
0C	FF	1C	FS	2C	,	3C	<	4C	L	5C	\	6C	l	7C	|
0D	CR	1D	GS	2D	-	3D	=	4D	M	5D	]	6D	m	7D	}
0E	SO	1E	RS	2E	.	3E	>	4E	N	5E	^	6E	n	7E	~
0F	SI	1F	US	2F	/	3F	?	4F	O	5F	_	6F	o	7F	DEL

Sub-Keys

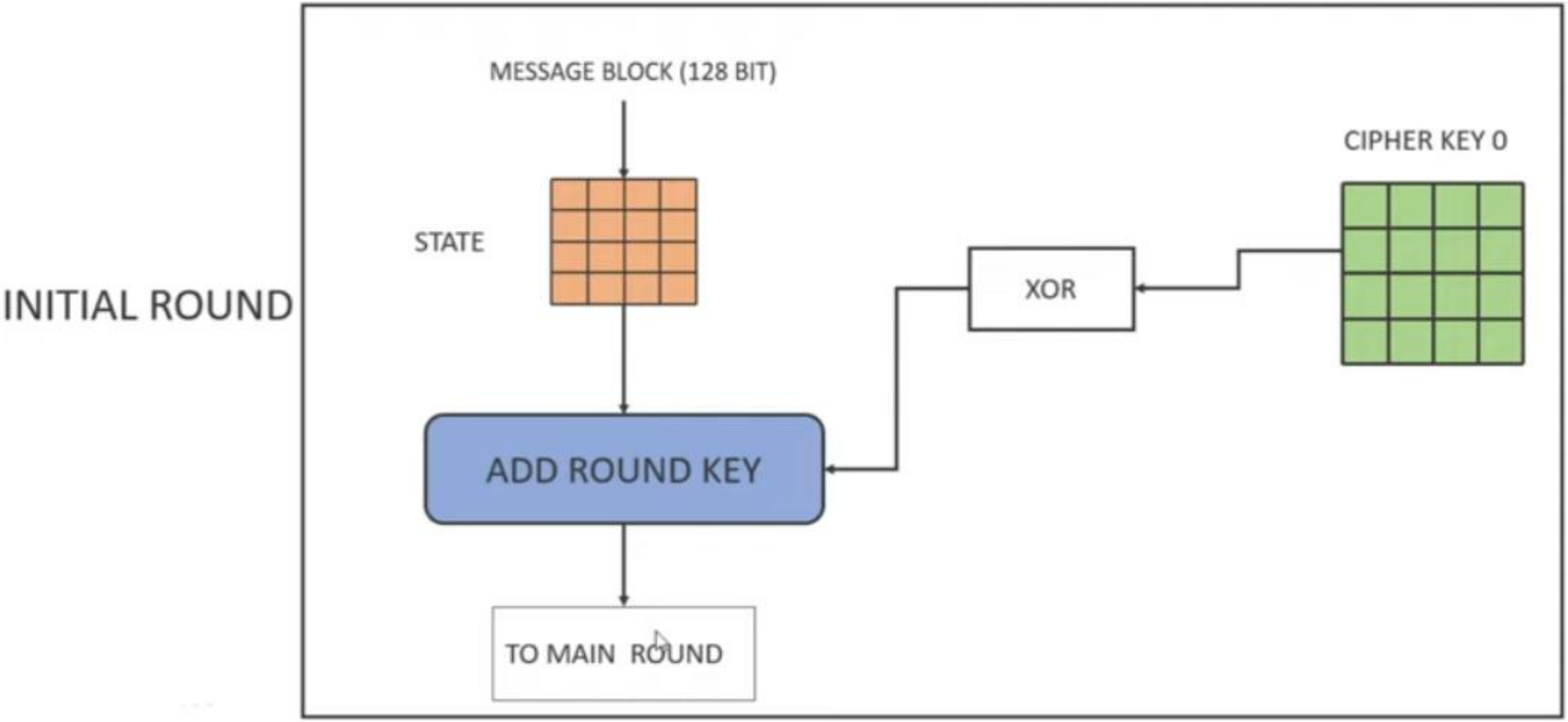


54 53 50 31
45 43 49 32
41 4F 41 33
4D 52 4E 34
KEY 0
76 25 75 44
86 C5 8C BE
59 16 57 64
8A D8 96 A2
KEY 1
6F 4A 3F 7B
28 ED 61 DF
1A 0C 5B 3F
B0 68 FE 5C
KEY 2
4A 00 3F 44
B6 5B 3A E5
B8 B4 EF D0
FA 92 6C 30
KEY 3
59 59 66 22
6F 34 0E EB
C8 7C 93 43
FE 6C 00 30
KEY 4
DA 83 E5 C7
86 B2 BC 57
D2 AE 3D 7E
FA 96 96 A6
KEY 5
3C BF 5A 9D
DD 6F D3 84
21 8F B2 CC
DE 48 DE 78
KEY 6
22 9D C7 5A
82 ED 3E BA
6A E5 57 9B
62 2A F4 8C
KEY 7
1C 81 46 1C
76 9B A5 1F
7E 9B CC 57
06 2C D8 54
KEY 8
9B 1A 5C 40
B6 2D 88 97
25 BE 72 25
26 0A D2 86
KEY 9
A4 BE E2 A2
3E 13 9B 0C
1A A4 D6 F3
62 68 BA 3C
KEY 10
ONE KEY CREATE ANOTHER KEY AND SO ON……

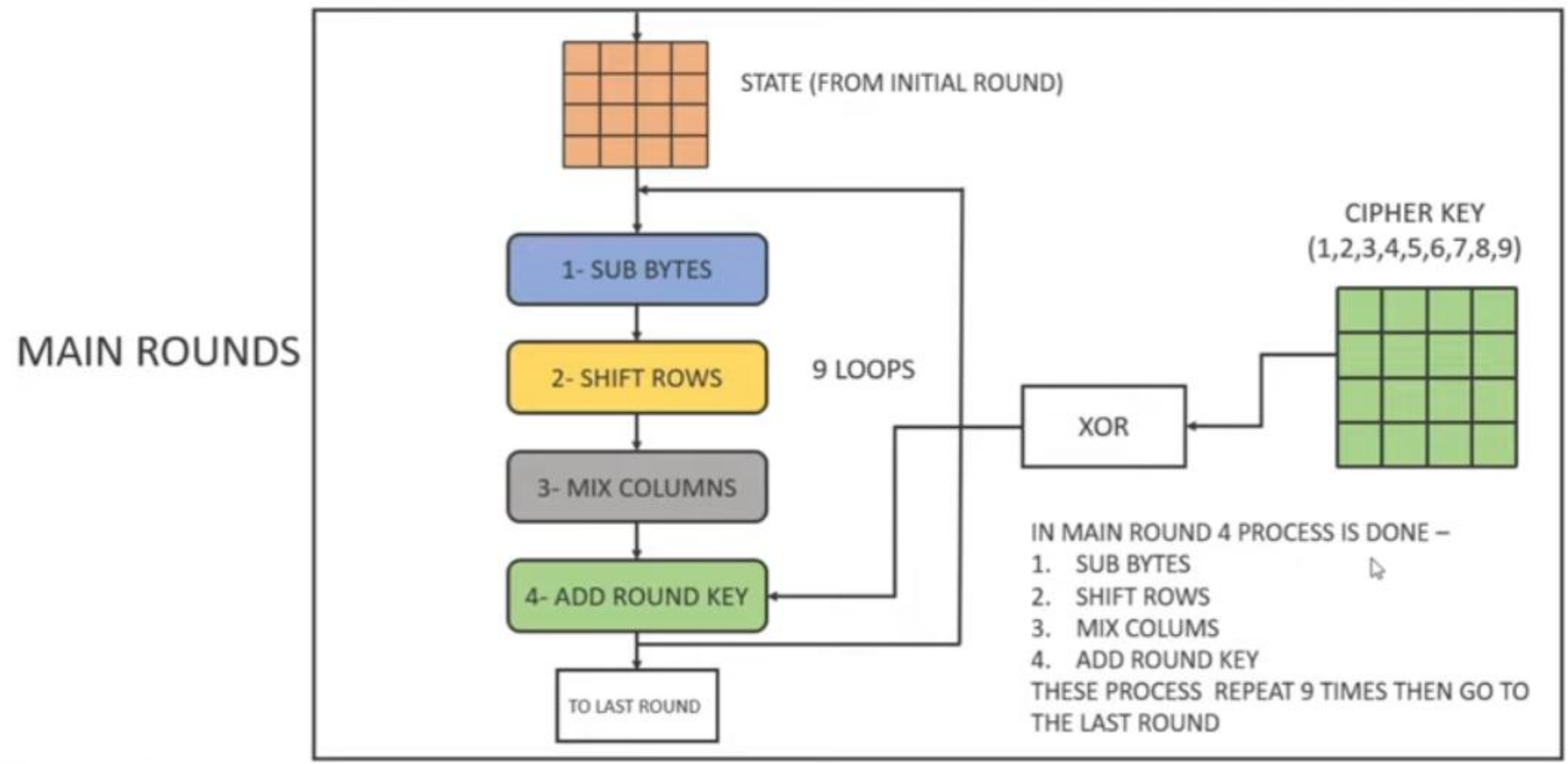
Encryption Process

- Three types of rounds:
  - Initial Round
  - Main Round
  - Final Round

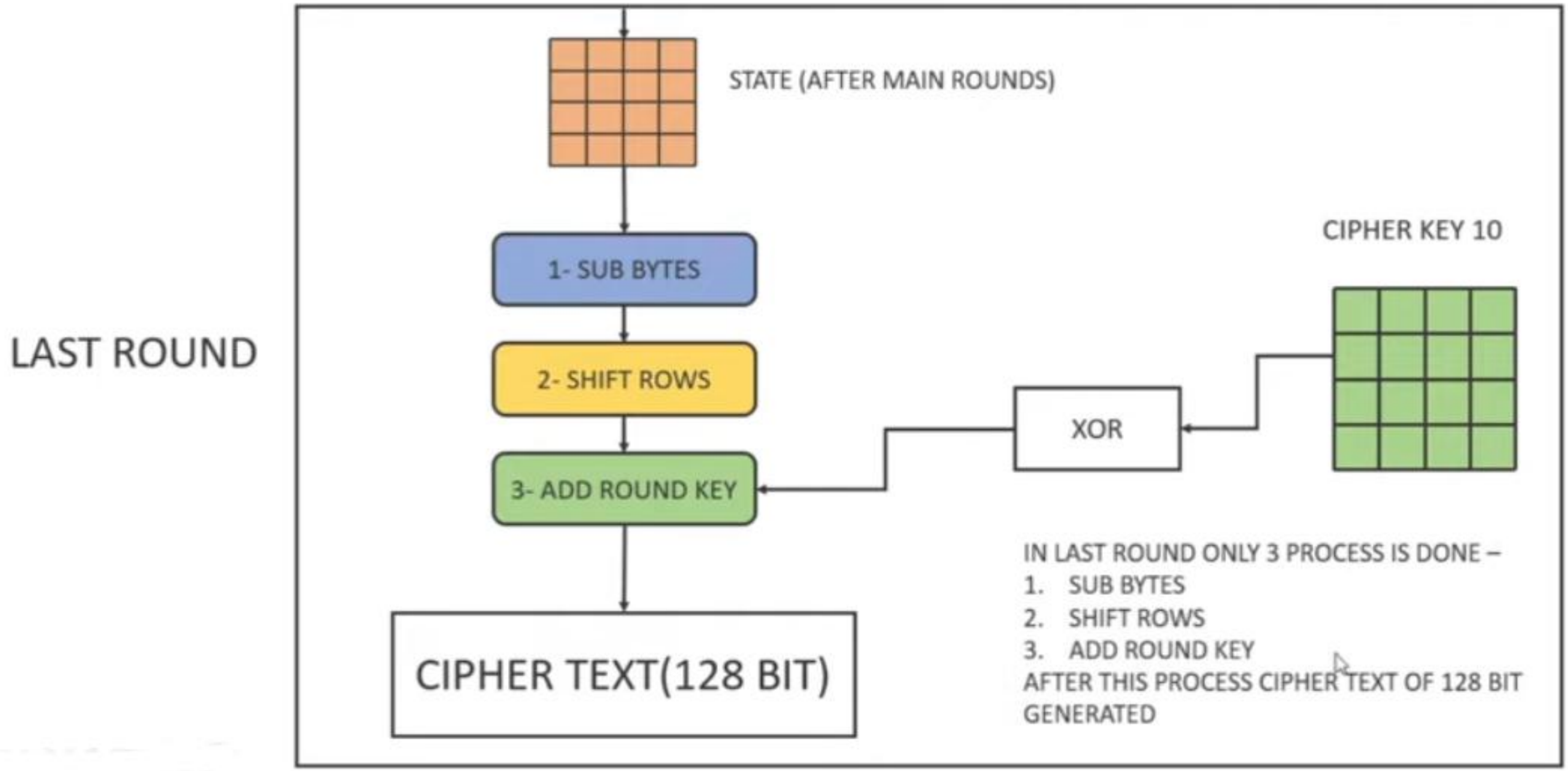
Encryption Process



Encryption Process

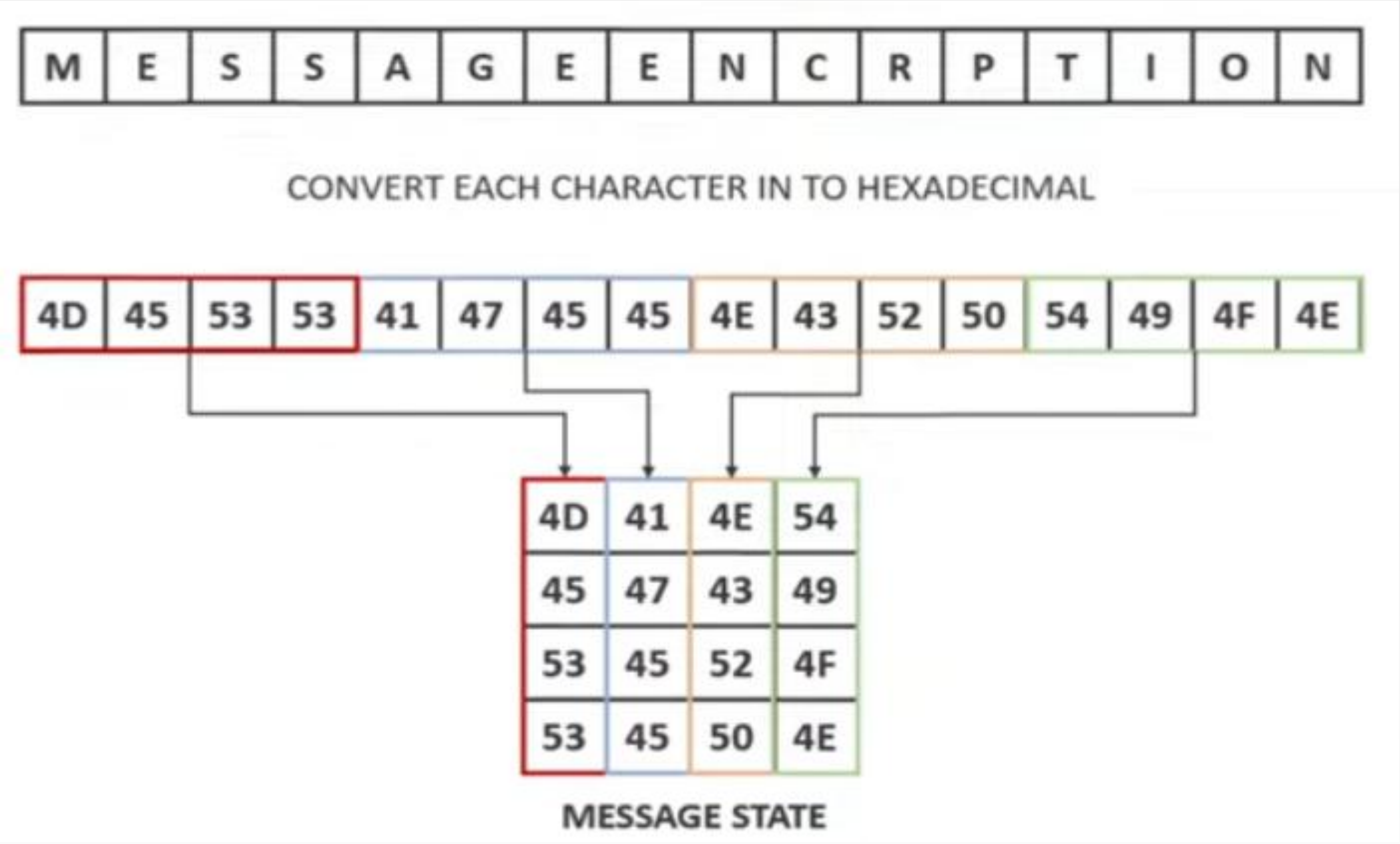


Encryption Process



Message Conversion into State

128-bit (16 Byte) Message :- **MESSAGEENCRPTION**

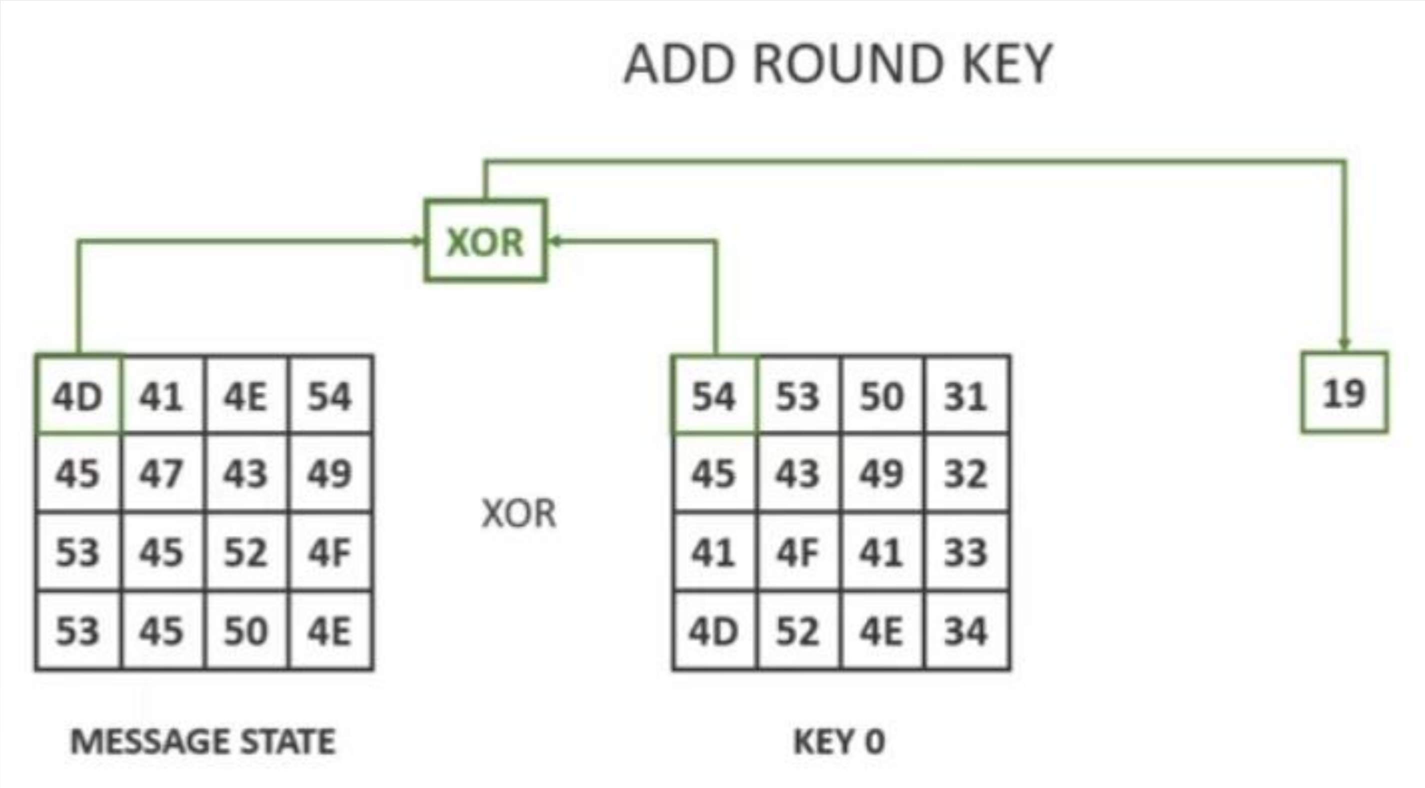


Round Steps

There are four steps in each round-

- Add round key
- Sub Bytes
- Shift Rows
- Mix Columns

Round Steps



ADD ROUND KEY
XOR
4D 41 4E 54
45 47 43 49
53 45 52 4F
53 45 50 4E
XOR
54 53 50 31
45 43 49 32
41 4F 41 33
4D 52 4E 34
19
MESSAGE STATE
KEY 0

Round Steps: Add round key

4D	41	4E	54
45	47	43	49
53	45	52	4F
53	45	50	4E

MESSAGE STATE

XOR

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

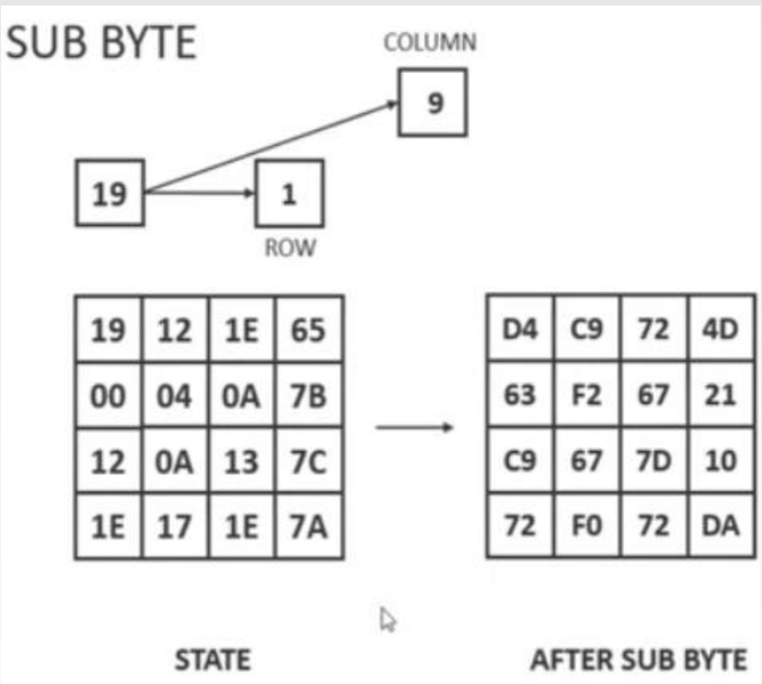
KEY 0

=

19	12	1E	65
00	04	0A	7B
12	0A	13	7C
1E	17	1E	7A

RESULT STATE

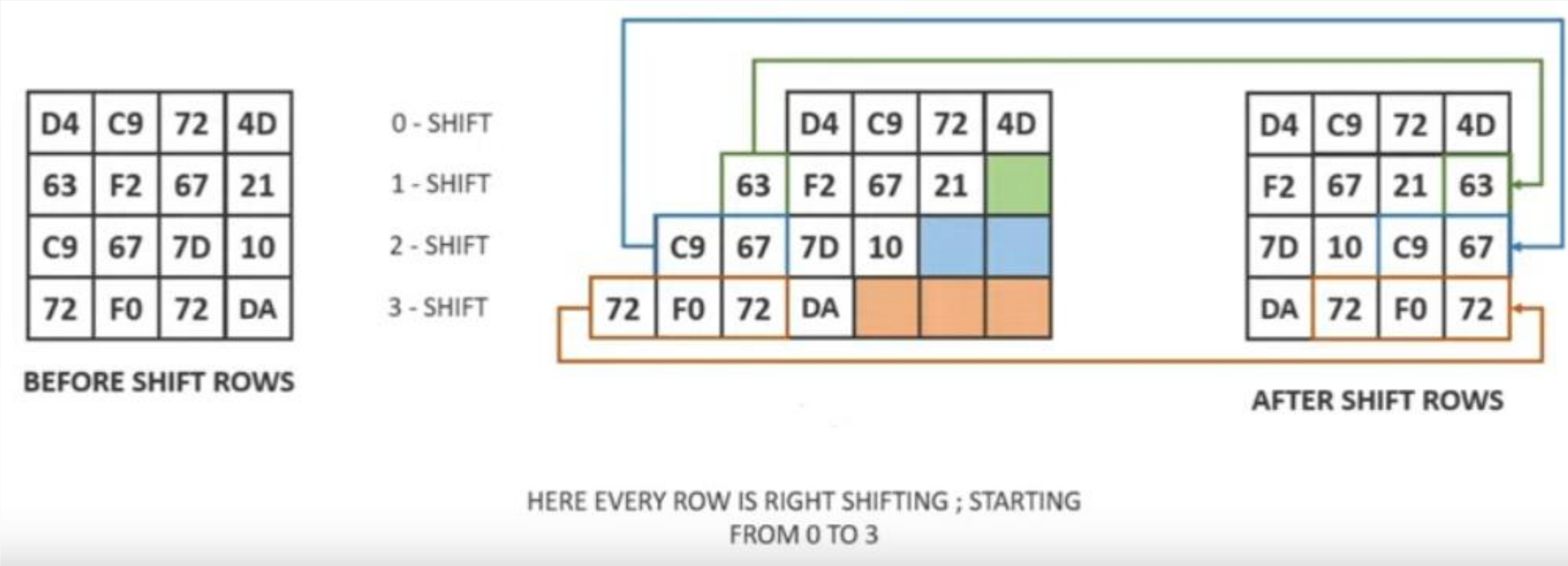
Round Steps: Sub Byte



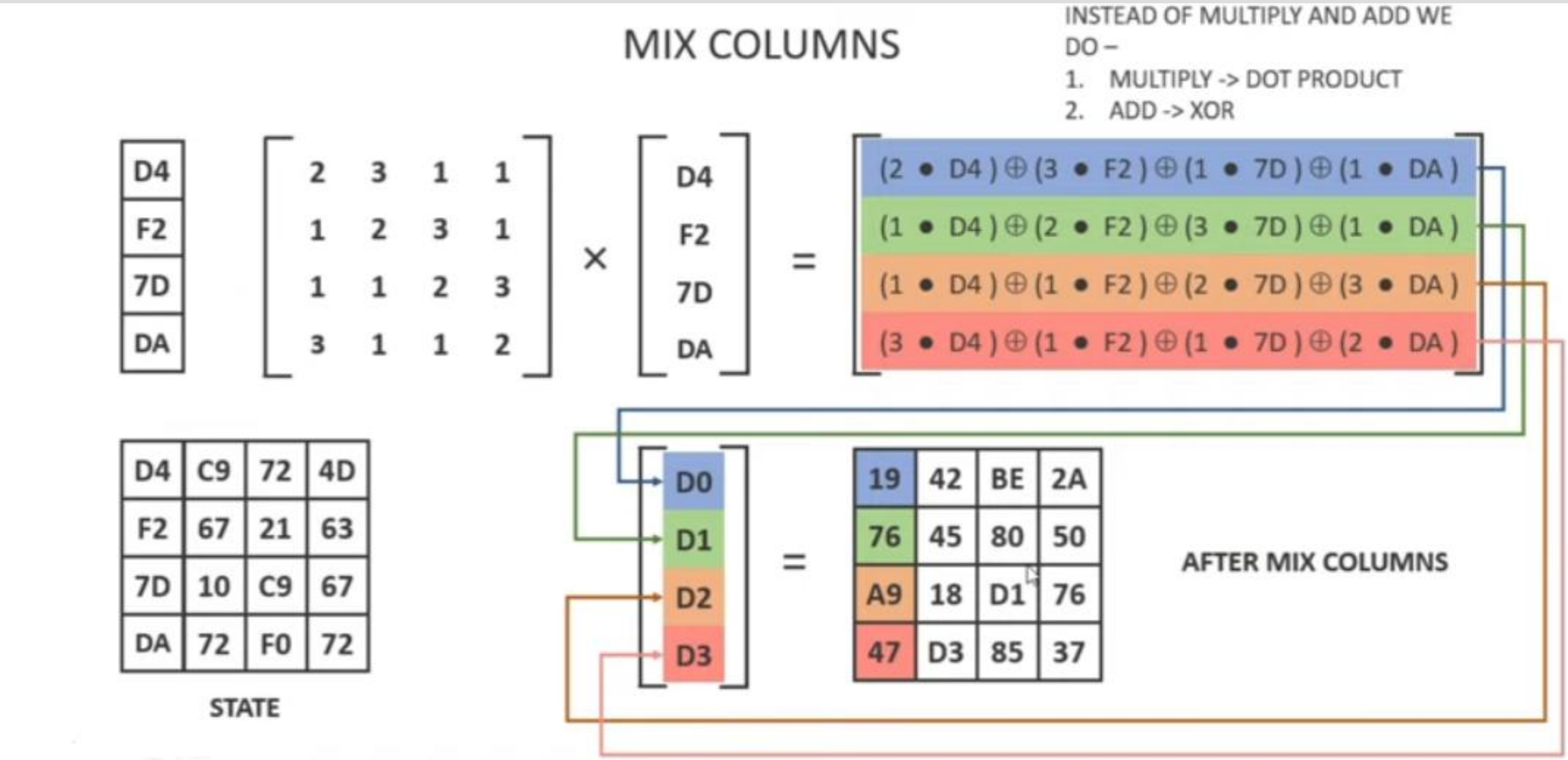
SubBytes transformation table

	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	CB	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

Round Steps: Shift Rows



Round Steps: Mix Column



Round Steps: Mix Column

- In general, dot product (instead of multiplying) of vectors of Galoi's fields. This means multiplying corresponding Galoi's field from the vectors and summing these products.
- If product is bigger than a byte than we have to reduce with reduce polynomial.

Round Steps: Mix Column (Reducing Polynomial)

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \times \begin{bmatrix} D4 \\ F2 \\ 7D \\ DA \end{bmatrix} \longrightarrow \begin{matrix} 2 & \bullet & D4 \\ 3 & \bullet & F2 \\ 1 & \bullet & 7D \\ 1 & \bullet & DA \end{matrix}$$

$$2 \bullet D4$$

$$10 \times 11010100$$

$$(X^1) \times (X^7 + X^6 + X^4 + X^2)$$

$$= (X^8 + X^7 + X^5 + X^3) \rightarrow 110101000$$

IF YOU GET –

- $2X^6$ = 0(EVEN CONSIDER AS 0)
- X^6 = 1(ONLY ODD CONSIDER AS 1)
- IF NUMBER IS NOT PRESENT THAT CONSIDER IS ALSO ZERO
- IF YOU GET X^8 WHICH IS MORE THAN A BYTE THAN USING REDUCING POLYNOMIAL(($X^8 + X^4 + X^3 + X^1 + X^0$) CONVERT THIS POLYNOMIAL INTO BINARY NUMBERS AND DIVIDE IT (TAKING REMAINDER AS RESULT) INSTEAD OF MINUS USING XOR

NOW WE NEED TO REDUCE IT INTO BYTE WITH

REDUCE POLYNOMIAL – ($X^8 + X^4 + X^3 + X^1 + X^0$) -> 100011011

$$\begin{array}{r} 110101000 \\ \oplus\ 100011011 \\ \hline 010110011 \end{array}$$

REPEAT THIS PROCESS UNTIL THE REMAINDER IS UNDER 8 BIT , THIS PROCESS IS ONLY DONE WHEN THE POLYNOMIAL OR RESULT IS OVER 8 BIT

Round Steps: Mix Column (Reducing Polynomial)

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \times \begin{bmatrix} D4 \\ F2 \\ 7D \\ DA \end{bmatrix} \longrightarrow$$

$2 \bullet D4 \rightarrow$

$3 \bullet F2 \rightarrow$

$1 \bullet 7D \rightarrow$

$1 \bullet DA \rightarrow$

$$\begin{bmatrix} 19 \\ 76 \\ A9 \\ 47 \end{bmatrix}$$

THEN 76 USING NEXT ROW OF MATRIX AND SO ON ; THIS PROCESS CREATE SINGLE COLUMN AFTER MIX COLUMN

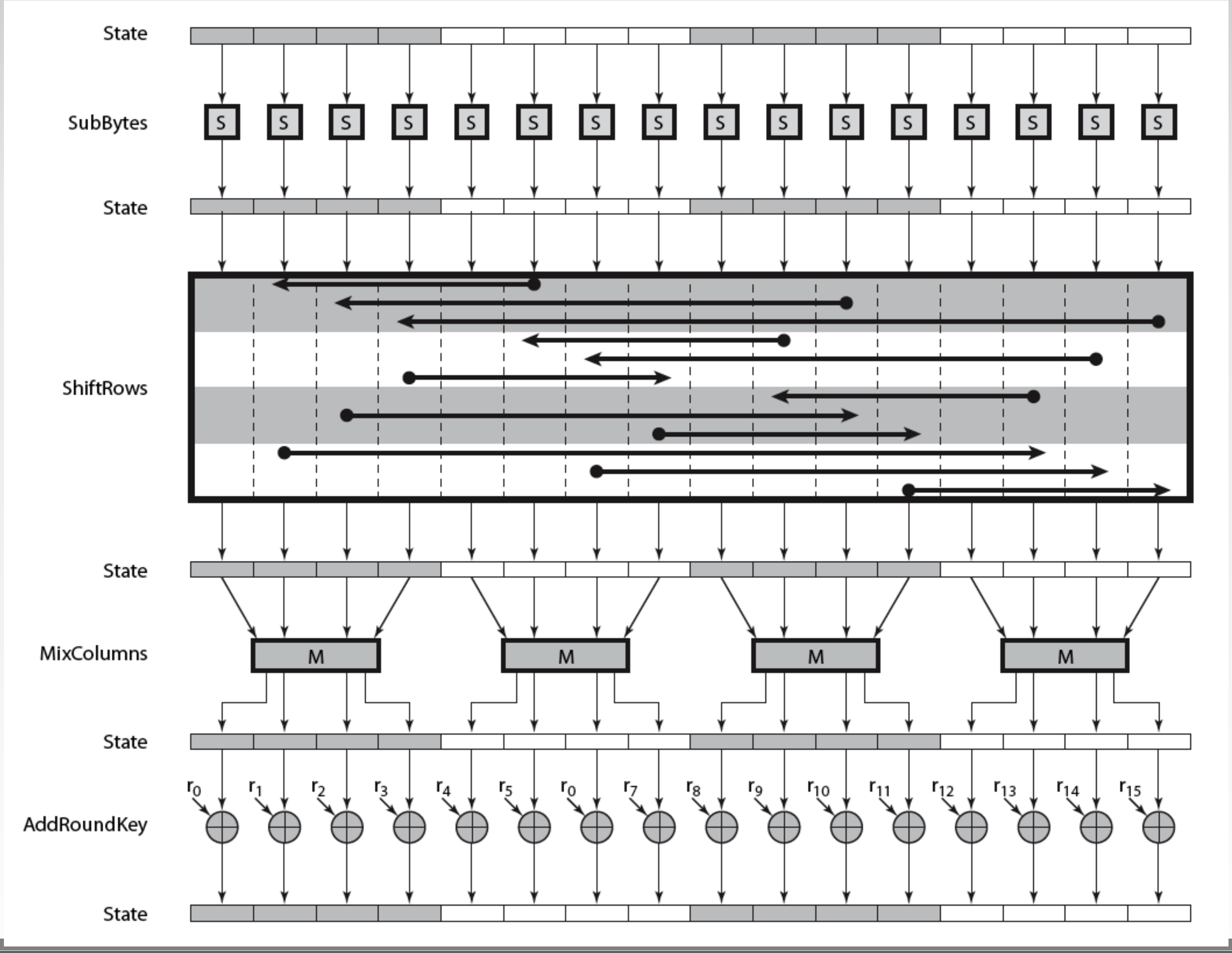
$2 \bullet D4$

10×11010100

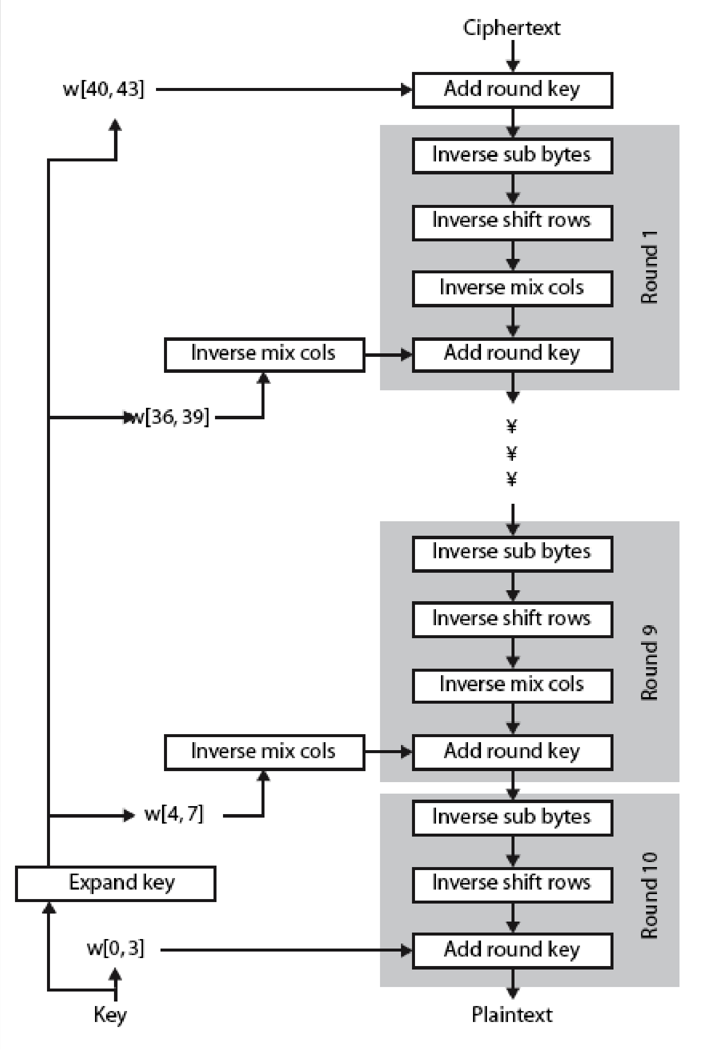
$(X^1) \times (X^7 + X^6 + X^4 + X^2)$

$= (X^8 + X^7 + X^5 + X^3) \rightarrow 110101000$

AES Round


State
SubBytes
S
State
ShiftRows
State
MixColumns
M
State
AddRoundKey
r_0 r_1 r_2 r_3 r_4 r_5 r_0 r_7 r_8 r_9 r_{10} r_{11} r_{12} r_{13} r_{14} r_{15}
State

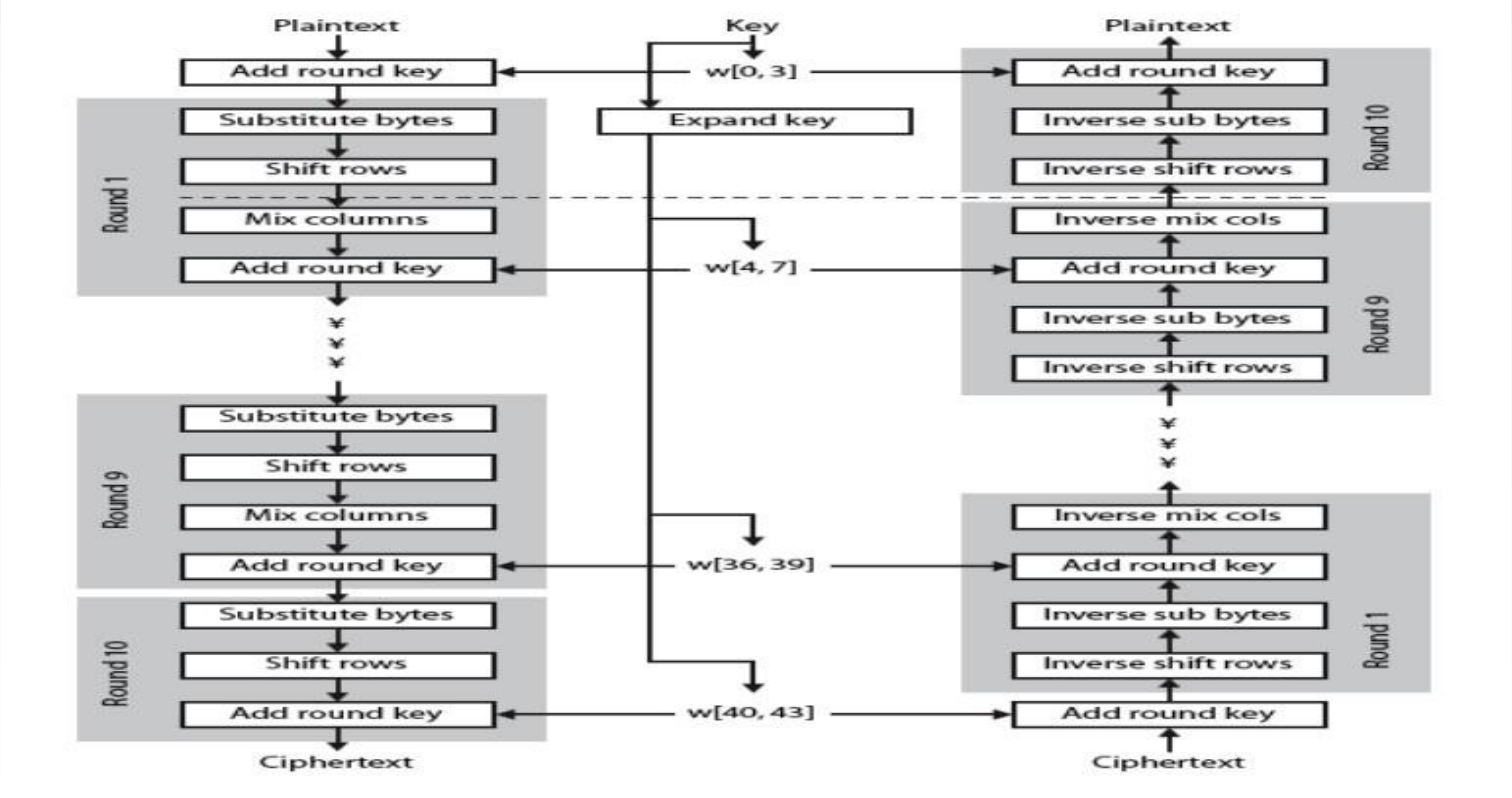
AES Decryption



AES Decryption

- AES decryption is not identical to encryption since steps done in reverse.
- But can define an equivalent inverse cipher with steps as for encryption.
  - but using inverses of each step
  - with a different key schedule
- Works since result is unchanged when
  - swap byte substitution & shift rows
  - swap mix columns & add (tweaked) round key

AES ENCRYPTION VS. DECRYPTION



Equivalent Inverse Cipher

- The original sequence is :

Encryption:

SubBytes ShiftRows MixColumns AddRoundKey

Decryption:

InvShiftRows InvSubBytes AddRoundKey InvMixColumns

- Thus **InvShiftRows** needs to be interchanged with **InvSubBytes** and **AddRoundKey** with **InvMixColumns**

AES Example Key Expansion

Key Words	Auxiliary Function
w0 = 0f 15 71 c9 w1 = 47 d9 e8 59 w2 = 0c b7 ad w3 = af 7f 67 98	RotWord(w3)= 7f 67 98 af = x1 SubWord(x1)= d2 85 46 79 = y1 Rcon(1)= 01 00 00 00 y1 ⊕ Rcon(1)= d3 85 46 79 = z1
w4 = w0 ⊕ z1 = dc 90 37 b0 w5 = w4 ⊕ w1 = 9b 49 df e9 w6 = w5 ⊕ w2 = 97 fe 72 3f w7 = w6 ⊕ w3 = 38 81 15 a7	RotWord(w7)= 81 15 a7 38 = x2 SubWord(x4)= 0c 59 5c 07 = y2 Rcon(2)= 02 00 00 00 y2 ⊕ Rcon(2)= 0e 59 5c 07 = z2
w8 = w4 ⊕ z2 = d2 c9 6b b7 w9 = w8 ⊕ w5 = 49 80 b4 5e w10 = w9 ⊕ w6 = de 7e c6 61 w11 = w10 ⊕ w7 = e6 ff d3 c6	RotWord(w11)= ff d3 c6 e6 = x3 SubWord(x2)= 16 66 b4 8e = y3 Rcon(3)= 04 00 00 00 y3 ⊕ Rcon(3)= 12 66 b4 8e = z3
w12 = w8 ⊕ z3 = c0 af df 39 w13 = w12 ⊕ w9 = 89 2f 6b 67 w14 = w13 ⊕ w10 = 57 51 ad 06 w15 = w14 ⊕ w11 = b1 ae 7e c0	RotWord(w15)= ae 7e c0 b1 = x4 SubWord(x3)= e4 f3 ba c8 = y4 Rcon(4)= 08 00 00 00 y4 ⊕ Rcon(4)= ec f3 ba c8 = 4
w16 = w12 ⊕ z4 = 2c 5c 65 f1 w17 = w16 ⊕ w13 = a5 73 0e 96 w18 = w17 ⊕ w14 = f2 22 a3 90 w19 = w18 ⊕ w15 = 43 8c dd 50	RotWord(w19)= 8c dd 50 43 = x5 SubWord(x4)= 64 c1 53 1a = y5 Rcon(5)= 10 00 00 00 y5 ⊕ Rcon(5)= 74 c1 53 1a = z5
w20 = w16 ⊕ z5 = 58 9d 36 eb w21 = w20 ⊕ w17 = fd ee 38 7d w22 = w21 ⊕ w18 = 0f cc 9b ed w23 = w22 ⊕ w19 = 4c 40 46 bd	RotWord(w23)= 40 46 bd 4c = x6 SubWord(x5)= 09 5a 7a 29 = y6 Rcon(6)= 20 00 00 00 y6 ⊕ Rcon(6)= 29 5a 7a 29 = z6
w24 = w20 ⊕ z6 = 71 c7 4c c2 w25 = w24 ⊕ w21 = 8c 29 74 bf w26 = w25 ⊕ w22 = 83 e5 ef 52 w27 = w26 ⊕ w23 = cf a5 a9 ef	RotWord(w27)= a5 a9 ef cf = x7 SubWord(x6)= 06 d3 df 8a = y7 Rcon(7)= 40 00 00 00 y7 ⊕ Rcon(7)= 46 d3 df 8a = z7
w28 = w24 ⊕ z7 = 37 14 93 48 w29 = w28 ⊕ w25 = bb 3d e7 f7 w30 = w29 ⊕ w26 = 38 d8 08 a5 w31 = w30 ⊕ w27 = f7 7d a1 4a	RotWord(w31)= 7d a1 4a f7 = x8 SubWord(x7)= ff 32 d6 68 = y8 Rcon(8)= 80 00 00 00 y8 ⊕ Rcon(8)= 7f 32 d6 68 = z8
w32 = w28 ⊕ z8 = 48 26 45 20 w33 = w32 ⊕ w29 = f3 1b a2 d7 w34 = w33 ⊕ w30 = cb c3 aa 72 w35 = w34 ⊕ w32 = 3c be 0b 38	RotWord(w35)= be 0b 38 3c = x9 SubWord(x8)= ae 2b 07 eb = y9 Rcon(9)= 1B 00 00 00 y9 ⊕ Rcon(9)= b5 2b 07 eb = z9
w36 = w32 ⊕ z9 = fd 0d 42 cb w37 = w36 ⊕ w33 = 0e 16 e0 1c w38 = w37 ⊕ w34 = c5 d5 4a 6e w39 = w38 ⊕ w35 = f9 6b 41 56	RotWord(w39)= 6b 41 56 f9 = x10 SubWord(x9)= 7f 83 b1 99 = y10 Rcon(10)= 36 00 00 00 y10 ⊕ Rcon(10)= 49 83 b1 99 = z10
w40 = w36 ⊕ z10 = b4 8e f3 52 w41 = w40 ⊕ w37 = ba 98 13 4e w42 = w41 ⊕ w38 = 7f 4d 59 20 w43 = w42 ⊕ w39 = 86 26 18 76	

AES Example Encryption

Start of round	After SubBytes	After ShiftRows	After MixColumns	Round Key
01 89 fe 76 23 ab dc 54 45 cd ba 32 67 ef 98 10				0f 47 0c af 15 d9 b7 7f 71 e8 ad 67 c9 59 d6 98
0e ce f2 d9 36 72 6b 2b 34 25 17 55 ae b6 4e 88	ab 8b 89 35 05 40 7f f1 18 3f f0 fc e4 4e 2f c4	ab 8b 89 35 40 7f f1 05 f0 fc 18 3f c4 e4 4e 2f	b9 94 57 75 e4 8e 16 51 47 20 9a 3f c5 d6 f5 3b	dc 9b 97 38 90 49 fe 81 37 df 72 15 b0 e9 3f a7
65 0f c0 4d 74 c7 e8 d0 70 ff e8 2a 75 3f ca 9c	4d 76 ba e3 92 c6 9b 70 51 16 9b e5 9d 75 74 de	4d 76 ba e3 c6 9b 70 92 9b e5 51 16 de 9d 75 74	8e 22 db 12 b2 f2 dc 92 df 80 f7 c1 2d c5 1e 52	d2 49 de e6 c9 80 7e ff 6b b4 c6 d3 b7 5e 61 c6
5c 6b 05 f4 7b 72 a2 6d b4 34 31 12 9a 9b 7f 94	4a 7f 6b bf 21 40 3a 3c 8d 18 c7 c9 b8 14 d2 22	4a 7f 6b bf 40 3a 3c 21 c7 c9 8d 18 22 b8 14 d2	b1 c1 0b cc ba f3 8b 07 f9 1f 6a c3 1d 19 24 5c	c0 89 57 b1 af 2f 51 ae df 6b ad 7e 39 67 06 c0
71 48 5c 7d 15 dc da a9 26 74 c7 bd 24 7e 22 9c	a3 52 4a ff 59 86 57 d3 f7 92 c6 7a 36 f3 93 de	a3 52 4a ff 86 57 d3 59 c6 7a f7 92 de 36 f3 93	d4 11 fe 0f 3b 44 06 73 cb ab 62 37 19 b7 07 ec	2c a5 f2 43 5c 73 22 8c 65 0e a3 dd f1 96 90 50
f8 b4 0c 4c 67 37 24 ff ae a5 c1 ea e8 21 97 bc	41 8d fe 29 85 9a 36 16 e4 06 78 87 9b fd 88 65	41 8d fe 29 9a 36 16 85 78 87 e4 06 65 9b fd 88	2a 47 c4 48 83 e8 18 ba 84 18 27 23 eb 10 0a f3	58 fd 0f 4c 9d ee cc 40 36 38 9b 46 eb 7d ed bd
72 ba cb 04 1e 06 d4 fa b2 20 bc 65 00 6d e7 4e	40 f4 1f f2 72 6f 48 2d 37 b7 65 4d 63 3c 94 2f	40 f4 1f f2 6f 48 2d 72 65 4d 37 b7 2f 63 3c 94	7b 05 42 4a 1e d0 20 40 94 83 18 52 94 c4 43 fb	71 8c 83 cf c7 29 e5 a5 4c 74 ef a9 c2 bf 52 ef
0a 89 c1 85 d9 f9 c5 e5 d8 f7 f7 fb 56 7b 11 14	67 a7 78 97 35 99 a6 d9 61 68 68 0f b1 21 82 fa	67 a7 78 97 99 a6 d9 35 68 0f 61 68 fa b1 21 82	ec 1a c0 80 0c 50 53 c7 3b d7 00 ef b7 22 72 e0	37 bb 38 f7 14 3d d8 7d 93 e7 08 a1 48 f7 a5 4a
db a1 f8 77 18 6d 8b ba a8 30 08 4e ff d5 d7 aa	b9 32 41 f5 ad 3c 3d f4 c2 04 30 2f 16 03 0e ac	b9 32 41 f5 3c 3d f4 ad 30 2f c2 04 ac 16 03 0e	b1 1a 44 17 3d 2f ec b6 0a 6b 2f 42 9f 68 f3 b1	48 f3 cb 3c 26 1b c3 be 45 a2 aa 0b 20 d7 72 38
f9 e9 8f 2b 1b 34 2f 08 4f c9 85 49 bf bf 81 89	99 1e 73 f1 af 18 15 30 84 dd 97 3b 08 08 0c a7	99 1e 73 f1 18 15 30 af 97 3b 84 dd a7 08 08 0c	31 30 3a c2 ac 71 8c c4 46 65 48 eb 6a 1c 31 62	fd 0e c5 f9 0d 16 d5 6b 42 e0 4a 41 cb 1c 6e 56
cc 3e ff 3b a1 67 59 af 04 85 02 aa a1 00 5f 34	4b b2 16 e2 32 85 cb 79 f2 97 77 ac 32 63 cf 18	4b b2 16 e2 85 cb 79 32 77 ac f2 97 18 32 63 cf	4b 86 8a 36 b1 cb 27 5a fb f2 f2 af cc 5a 5b cf	b4 8e f3 52 ba 98 13 4e 7f 4d 59 20 86 26 18 76
ff 08 69 64 0b 53 34 14 84 bf ab 8f 4a 7c 43 b9				

AES Example Avalanche

Round		Number of bits that differ
	0123456789abcdeffedcba9876543210 0023456789abcdeffedcba9876543210	1
0	0e3634aece7225b6f26b174ed92b5588 0f3634aece7225b6f26b174ed92b5588	1
1	657470750fc7ff3fc0e8e8ca4dd02a9c c4a9ad090fc7ff3fc0e8e8ca4dd02a9c	20
2	5c7bb49a6b72349b05a2317ff46d1294 fe2ae569f7ee8bb8c1f5a2bb37ef53d5	58
3	7115262448dc747e5cdac7227da9bd9c ec093dfb7c45343d689017507d485e62	59
4	f867aee8b437a5210c24c1974cffeabc 43efdb697244df808e8d9364ee0ae6f5	61
5	721eb200ba06206dcbd4bce704fa654e 7b28a5d5ed643287e006c099bb375302	68
6	0ad9d85689f9f77bc1c5f71185e5fb14 3bc2d8b6798d8ac4fe36a1d891ac181a	64
7	db18a8ffa16d30d5f88b08d777ba4eaa 9fb8b5452023c70280e5c4bb9e555a4b	67
8	f91b4fbfe934c9bf8f2f85812b084989 20264e1126b219aef7feb3f9b2d6de40	65
9	cca104a13e678500ff59025f3bafaa34 b56a0341b2290ba7dfdfbddcd8578205	61
10	ff0b844a0853bf7c6934ab4364148fb9 612b89398d0600cde116227ce72433f0	58

SOME KEY APPLICATIONS

- **RAR**
- **Winzip**
- **VPNs**
- **IEEE 802.11e**
- **Signal Protocol**
  - **Facebook Messenger**
  - **WhatsApp**
- Hopefully, you are now beginning to realize just how integral AES in running the entire framework of modern society.

STRENGTHS OF AES

- As it is implemented in both hardware and software, it is most robust security protocol.
- It uses higher length key sizes such as 128, 192 and 256 bits for encryption. Hence it makes AES algorithm more robust against hacking.
- It is most common security protocol used for wide various of applications such as wireless communication, financial transactions, e-business, encrypted data storage etc.
- It is one of the most spread commercial and open source solutions used all over the world.
- For 128 bit, about 2^{128} attempts are needed to break. This makes it very difficult to hack it as a result it is very safe protocol.