

Presented By:

AES

ADVANCED ENCRYPTION
STANDARD

170050107507

Dharmik Gadhiya

170050107511

Harsh Golakiya

170050107513

Bhrugesh Jadav

170050107543

Dhruvil Pethani

What is AES?



- AES is an encryption standard chosen by the National Institute of Standards and Technology (NIST), USA to protect classified information. It has been accepted world wide as a desirable algorithm to encrypt sensitive data.

- It is a block cipher which operates on block size of 128 bits for both encrypting as well as decrypting.

- Each Round performs same operations.

WHY AES?

- Cracking of DES algorithm became possible very easily as DES only has a 56-bit key (compared to the maximum of 256-bit in AES).
- Around 56 hrs of bruteforcing can crack the message.
- So to make Encryption more powerful AES was developed with a fixed block-size of 128-bits and key sizes of 128, 192 and 256-bits.

The features of AES are

```
graph TD; A[The features of AES are] --- B[Symmetric key -block cipher]; A --- C[128-bit data, 128/192/256-bit keys]; A --- D[Stronger and faster than Triple-DES]
```

Symmetric
key -block
cipher

128-bit data,
128/192/256-
bit keys

Stronger and
faster than
Triple-DES

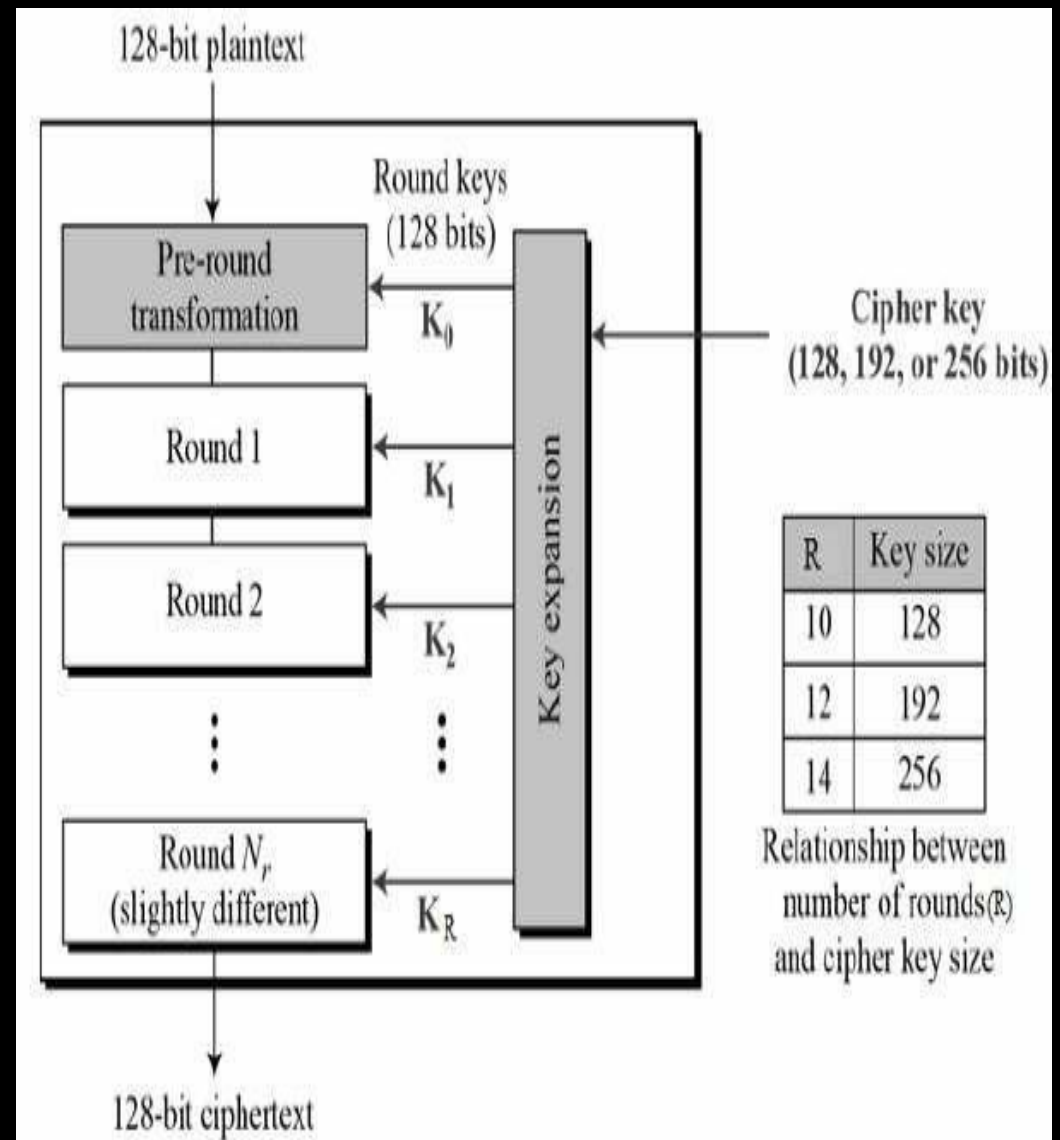
AES STRUCTURE

AES treats the 128 bits of a plaintext block as 16 bytes.

These 16 bytes are arranged in four columns and four rows for processing as a matrix.

A word consists of four bytes, that is 32 bits. Total there are 44 words.

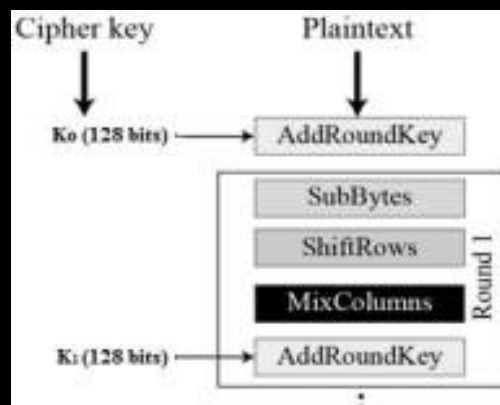
$$4 + 4 \times 10 = 44$$



AES Encryption Process

Each round
comprise of four
sub-processes.

- Initial Round
AddRoundKey
- Main Rounds
SubBytes
ShiftRows
MixColumns
AddRoundKey
- Final Round
SubBytes
ShiftRows
AddRoundKey



AES Example - Input (128 bit key and message)

Key in English: **Thats my Kung Fu** (16 ASCII characters, 1 byte each)

Translation into Hex:

T	h	a	t	s		m	y		K	u	n	g		F	u
54	68	61	74	73	20	6D	79	20	4B	75	6E	67	20	46	75

Key in Hex (128 bits): **54 68 61 74 73 20 6D 79 20 4B 75 6E 67 20 46 75**

Plaintext in English: **Two One Nine Two** (16 ASCII characters, 1 byte each)

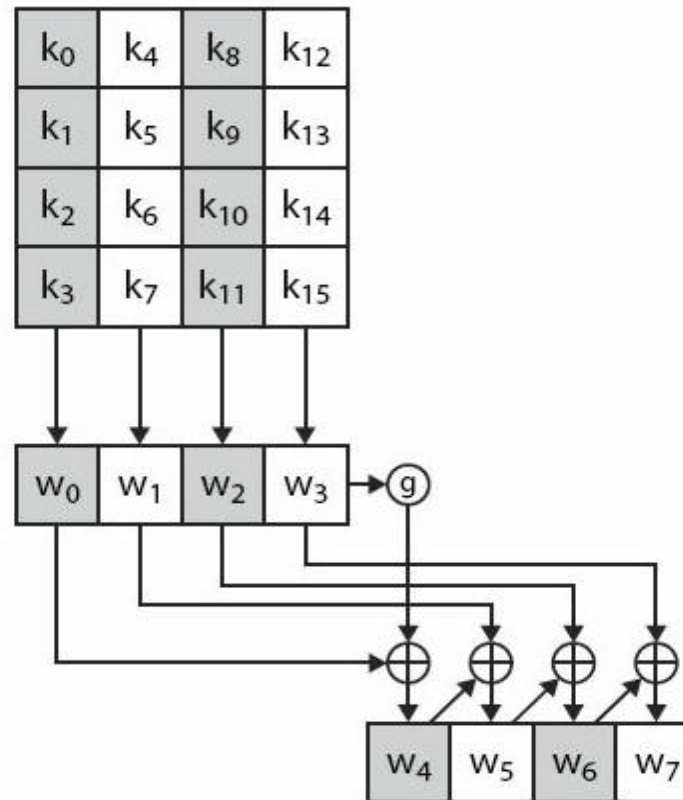
Translation into Hex:

T	w	o		O	n	e		N	i	n	e		T	w	o
54	77	6F	20	4F	6E	65	20	4E	69	6E	65	20	54	77	6F

Plaintext in Hex (128 bits): **54 77 6F 20 4F 6E 65 20 4E 69 6E 65 20 54 77 6F**

ASCII	Hex	ASCII	HEX	ASCII	Hex
0	30	L	4C	g	67
1	31	M	4D	h	68
2	32	N	4E	I	69
3	33	O	4F	j	6A
4	34	P	50	k	6B
5	35	Q	51	l	6C
6	36	R	52	m	6D
7	37	S	53	n	6E
8	38	T	54	o	6F
9	39	U	55	p	70
A	41	V	56	q	71
B	42	W	57	r	72
C	43	X	58	s	73
D	44	Y	59	t	74
E	45	Z	5A	u	75
F	46	a	61	v	76
G	47	b	62	w	77
H	48	c	63	x	78
I	49	d	64	y	79
J	4A	e	65	z	7A
K	4B	f	66		

KEY EXPANSION



AES Example - The first Roundkey

- Key in Hex (128 bits): 54 68 61 74 73 20 6D 79 20 4B 75 6E 67 20 46 75
- $w[0] = (54, 68, 61, 74)$, $w[1] = (73, 20, 6D, 79)$, $w[2] = (20, 4B, 75, 6E)$, $w[3] = (67, 20, 46, 75)$
- $g(w[3])$:
 - circular byte left shift of $w[3]$: (20, 46, 75, 67)
 - Byte Substitution (S-Box): (B7, 5A, 9D, 85)
 - Adding round constant (01, 00, 00, 00) gives: $g(w[3]) = (B6, 5A, 9D, 85)$
- $w[4] = w[0] \oplus g(w[3]) = (E2, 32, FC, F1)$:

0101 0100	0110 1000	0110 0001	0111 0100
1011 0110	0101 1010	1001 1101	1000 0101
1110 0010	0011 0010	1111 1100	1111 0001
E2	32	FC	F1

- $w[5] = w[4] \oplus w[1] = (91, 12, 91, 88)$, $w[6] = w[5] \oplus w[2] = (B1, 59, E4, E6)$,
 $w[7] = w[6] \oplus w[3] = (D6, 79, A2, 93)$
- first roundkey: E2 32 FC F1 91 12 91 88 B1 59 E4 E6 D6 79 A2 93

S - BOX

X	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

Key(128 bits): E2 32 FC F1 91 12 91 88 B1 59 E4 E6 D6 79 A2 93

$w[4]=E2\ 32\ FC\ F1$, $w[5]=91\ 12\ 91\ 88$

$w[6]=B1\ 59\ E4\ E6$, $w[7]=D6\ 79\ A2\ 93$

$g(w[7])$:

Circular byte left shift: 79 A2 93 D6

Byte Substitution (S-Box): B6 3A DC F6

Round Constant (02,00,00,00) gives: $g(w[7])=(B4,3A,DC,F6)$

$W[8]=w[4] \oplus g(w[7])$:

$w[4]$	E2	32	FC	F1
	11100010	00110010	11111100	11110001
$g(w[7])$	B4	3A	DC	F6
	10110100	00111010	11011100	11110110
$W[8]$	01010110 56	00001000 08	00100000 20	00000111 07

$w[9]=w[8] \oplus w[5]=(C7, 1A, B1, 8F)$ $w[10]=w[9] \oplus w[6]=(76,43,55,69)$

$w[11]=w[10] \oplus w[7] = (A0,3A,F7,FA)$

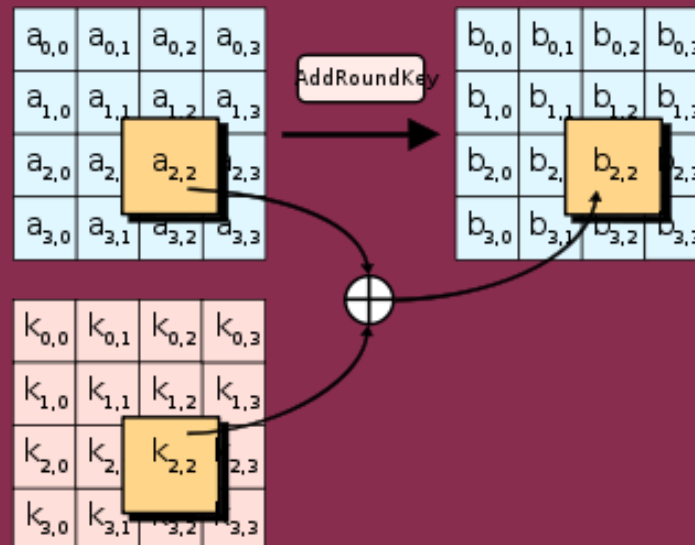
Second Round Key : 56 08 20 07 C7 1A B1 8F 76 43 55 69 A0 3A F7
FA

AES Example - All RoundKeys

- Round 0: 54 68 61 74 73 20 6D 79 20 4B 75 6E 67 20 46 75
- Round 1: E2 32 FC F1 91 12 91 88 B1 59 E4 E6 D6 79 A2 93
- Round 2: 56 08 20 07 C7 1A B1 8F 76 43 55 69 A0 3A F7 FA
- Round 3: D2 60 0D E7 15 7A BC 68 63 39 E9 01 C3 03 1E FB
- Round 4: A1 12 02 C9 B4 68 BE A1 D7 51 57 A0 14 52 49 5B
- Round 5: B1 29 3B 33 05 41 85 92 D2 10 D2 32 C6 42 9B 69
- Round 6: BD 3D C2 B7 B8 7C 47 15 6A 6C 95 27 AC 2E 0E 4E
- Round 7: CC 96 ED 16 74 EA AA 03 1E 86 3F 24 B2 A8 31 6A
- Round 8: 8E 51 EF 21 FA BB 45 22 E4 3D 7A 06 56 95 4B 6C
- Round 9: BF E2 BF 90 45 59 FA B2 A1 64 80 B4 F7 F1 CB D8
- Round 10: 28 FD DE F8 6D A4 24 4A CC C0 A4 FE 3B 31 6F 26

ADDRoundKey

The 16 bytes of the matrix are now considered as 128 bits and are XORed to the 128 bits of the round key.



AES Example - Add Roundkey, Round 0

- State Matrix and Roundkey No.0 Matrix:

PLAIN TEXT	$\left(\begin{array}{cccc} 54 & 4F & 4E & 20 \\ 77 & 6E & 69 & 54 \\ 6F & 65 & 6E & 77 \\ 20 & 20 & 65 & 6F \end{array} \right)$	$\left(\begin{array}{cccc} 54 & 73 & 20 & 67 \\ 68 & 20 & 4B & 20 \\ 61 & 6D & 75 & 46 \\ 74 & 79 & 6E & 75 \end{array} \right)$	KEY Y
---------------	---	---	----------

- XOR the corresponding entries, e.g., $69 \oplus 4B = 22$

$$\begin{array}{r} 0110 \ 1001 \\ 0100 \ 1011 \\ \hline 0010 \ 0010 \end{array}$$

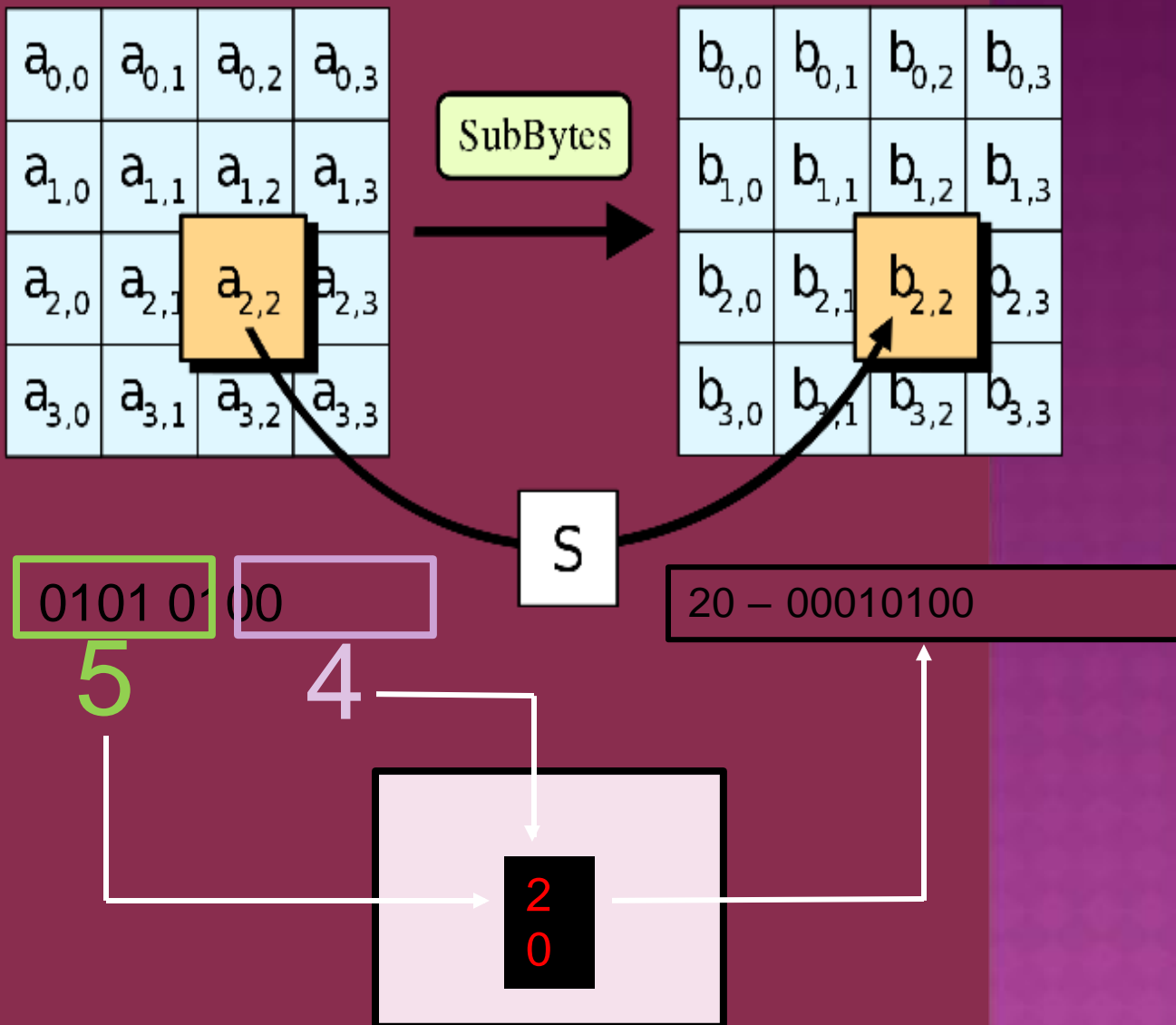
- the new State Matrix is

$$\left(\begin{array}{cccc} 00 & 3C & 6E & 47 \\ 1F & 4E & 22 & 74 \\ 0E & 08 & 1B & 31 \\ 54 & 59 & 0B & 1A \end{array} \right)$$

SUBBYTES

The 16 input bytes are substituted by looking up a fixed table (S-box).

The result is in a matrix of four rows and four columns.



AES Example - Round 1, Substitution Bytes

- current State Matrix is

$$\begin{pmatrix} 00 & 3C & 6E & 47 \\ 1F & 4E & 22 & 74 \\ 0E & 08 & 1B & 31 \\ 54 & 59 & 0B & 1A \end{pmatrix}$$

- substitute each entry (byte) of current state matrix by corresponding entry in AES S-Box
- for instance: byte 6E is substituted by entry of S-Box in row 6 and column E, i.e., by 9F
- this leads to new State Matrix

$$\begin{pmatrix} 63 & EB & 9F & A0 \\ C0 & 2F & 93 & 92 \\ AB & 30 & AF & C7 \\ 20 & CB & 2B & A2 \end{pmatrix}$$

- this non-linear layer is for resistance to differential and linear cryptanalysis attacks

SHIFTROWS

Each of the four rows of the matrix is shifted to the left.

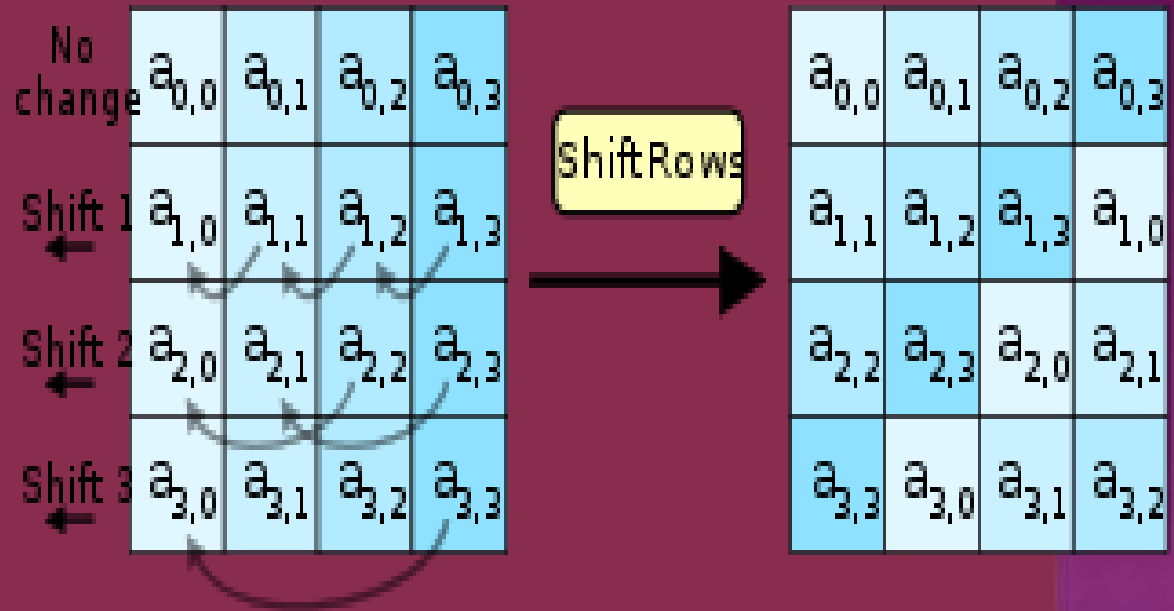
First row is not shifted.

Second row is shifted one (byte) position to the left.

Third row is shifted two positions to the left.

Fourth row is shifted three positions to the left.

The result is a new matrix consisting of the same 16 bytes but shifted with respect to each other.



AES Example - Round 1, Shift Row

- the current State Matrix is

$$\begin{pmatrix} 63 & EB & 9F & A0 \\ C0 & 2F & 93 & 92 \\ AB & 30 & AF & C7 \\ 20 & CB & 2B & A2 \end{pmatrix}$$

- four rows are shifted cyclically to the left by offsets of 0,1,2, and 3
- the new State Matrix is

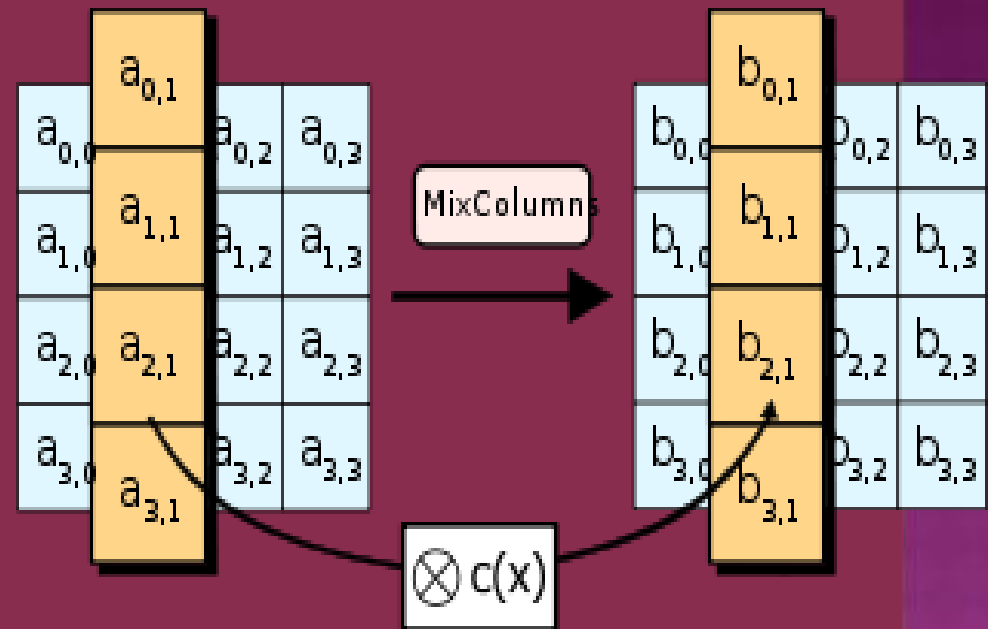
$$\begin{pmatrix} 63 & EB & 9F & A0 \\ 2F & 93 & 92 & C0 \\ AF & C7 & AB & 30 \\ A2 & 20 & CB & 2B \end{pmatrix}$$

- this linear mixing step causes diffusion of the bits over multiple rounds

MIXCOLUMN

Each column of four bytes is now transformed using a special mathematical function.

This function takes as input the four bytes of one column and outputs four completely new bytes, which replace the original column.



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

AES Example - Round 1, Mix Column

- Mix Column multiplies fixed matrix against current State Matrix:

$$\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} 63 & EB & 9F & A0 \\ 2F & 93 & 92 & C0 \\ AF & C7 & AB & 30 \\ A2 & 20 & CB & 2B \end{pmatrix} = \begin{pmatrix} BA & 84 & E8 & 1B \\ 75 & A4 & 8D & 40 \\ F4 & 8D & 06 & 7D \\ 7A & 32 & 0E & 5D \end{pmatrix}$$

- entry BA is result of $(02 \bullet 63) \oplus (03 \bullet 2F) \oplus (01 \bullet AF) \oplus (01 \bullet A2)$:
 - $02 \bullet 63 = 00000010 \bullet 01100011 = 11000110$
 - $03 \bullet 2F = (02 \bullet 2F) \oplus 2F = (00000010 \bullet 00101111) \oplus 00101111 = 01110001$
 - $01 \bullet AF = AF = 10101111$ and $01 \bullet A2 = A2 = 10100010$
 - hence

$$\begin{array}{r} 11000110 \\ 01110001 \\ 10101111 \\ 10100010 \\ \hline 10111010 \end{array}$$

AES Example - Add Roundkey, Round 1

- State Matrix and Roundkey No.1 Matrix:

$$\begin{pmatrix} BA & 84 & E8 & 1B \\ 75 & A4 & 8D & 40 \\ F4 & 8D & 06 & 7D \\ 7A & 32 & 0E & 5D \end{pmatrix} \quad \begin{pmatrix} E2 & 91 & B1 & D6 \\ 32 & 12 & 59 & 79 \\ FC & 91 & E4 & A2 \\ F1 & 88 & E6 & 93 \end{pmatrix}$$

- XOR yields new State Matrix

$$\begin{pmatrix} 58 & 15 & 59 & CD \\ 47 & B6 & D4 & 39 \\ 08 & 1C & E2 & DF \\ 8B & BA & E8 & CE \end{pmatrix}$$

- AES output after Round 1: 58 47 08 8B 15 B6 1C BA 59 D4 E2 E8 CD 39 DF CE

THANK

YOU