Cryptography and System Security

Advanced Encryption Standard (AES)

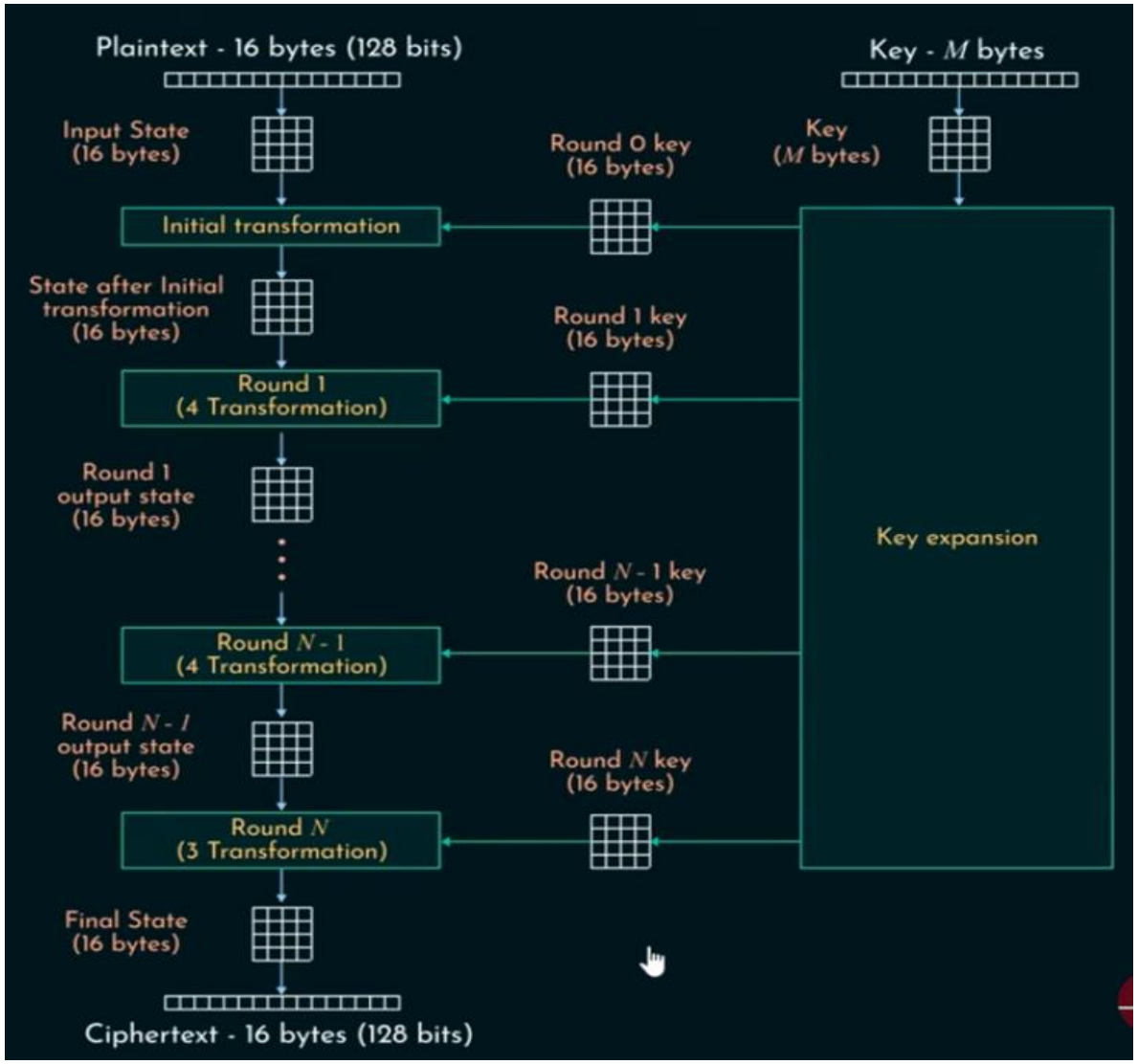
Symmetric and Asymmetric key Cryptography and Key management

Sejal Chopra
Assistant Professor - Dept. of Computer Engineering
Don Bosco Institute of Technology, Mumbai

Contents to be discussed

- **AES Structure**
- **AES Parameters**
- **AES encryption and decryption**
- **AES Transformation functions**
- **AES Key Scheduling**
- **Comparison of AES and DES**

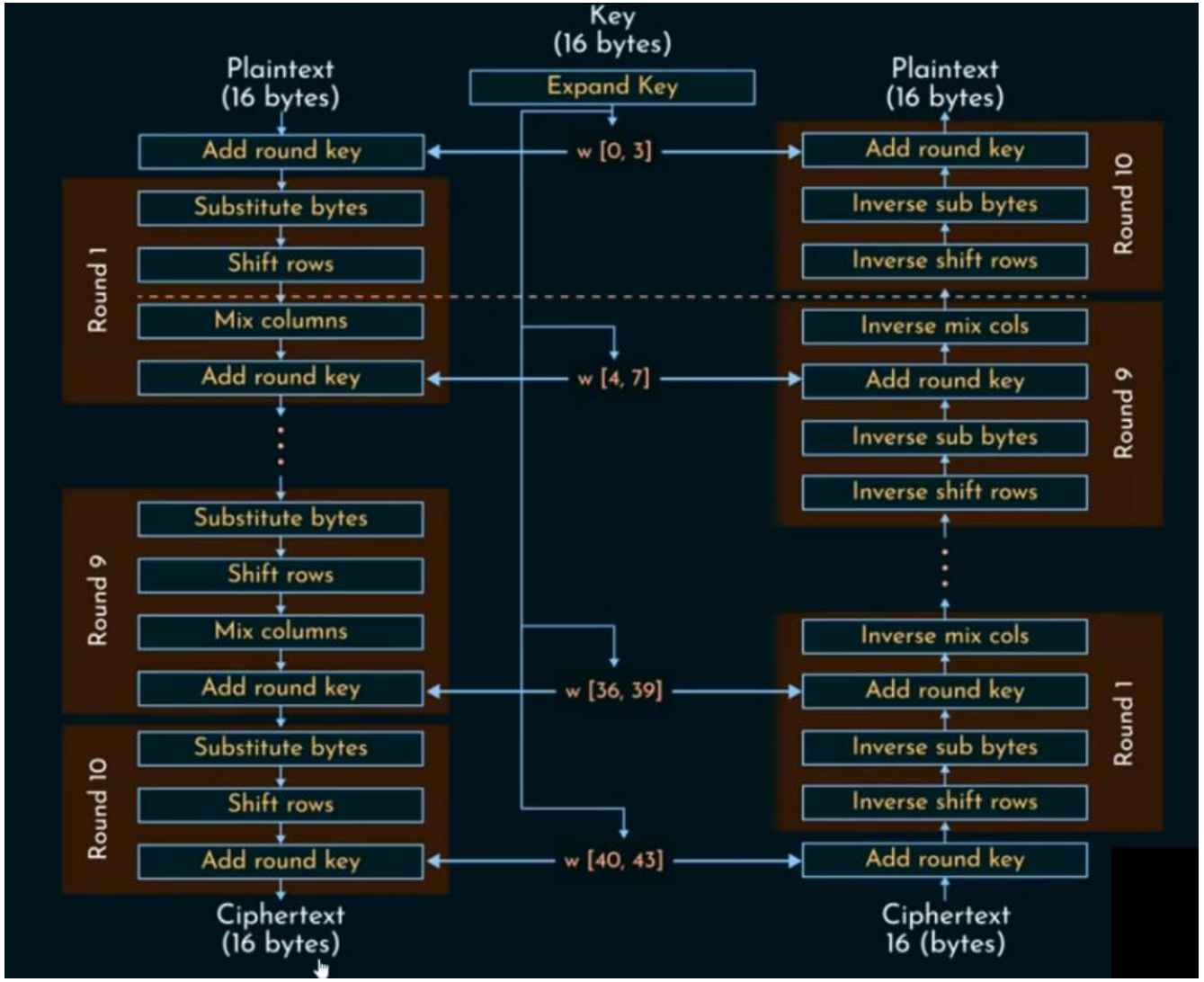
AES Structure



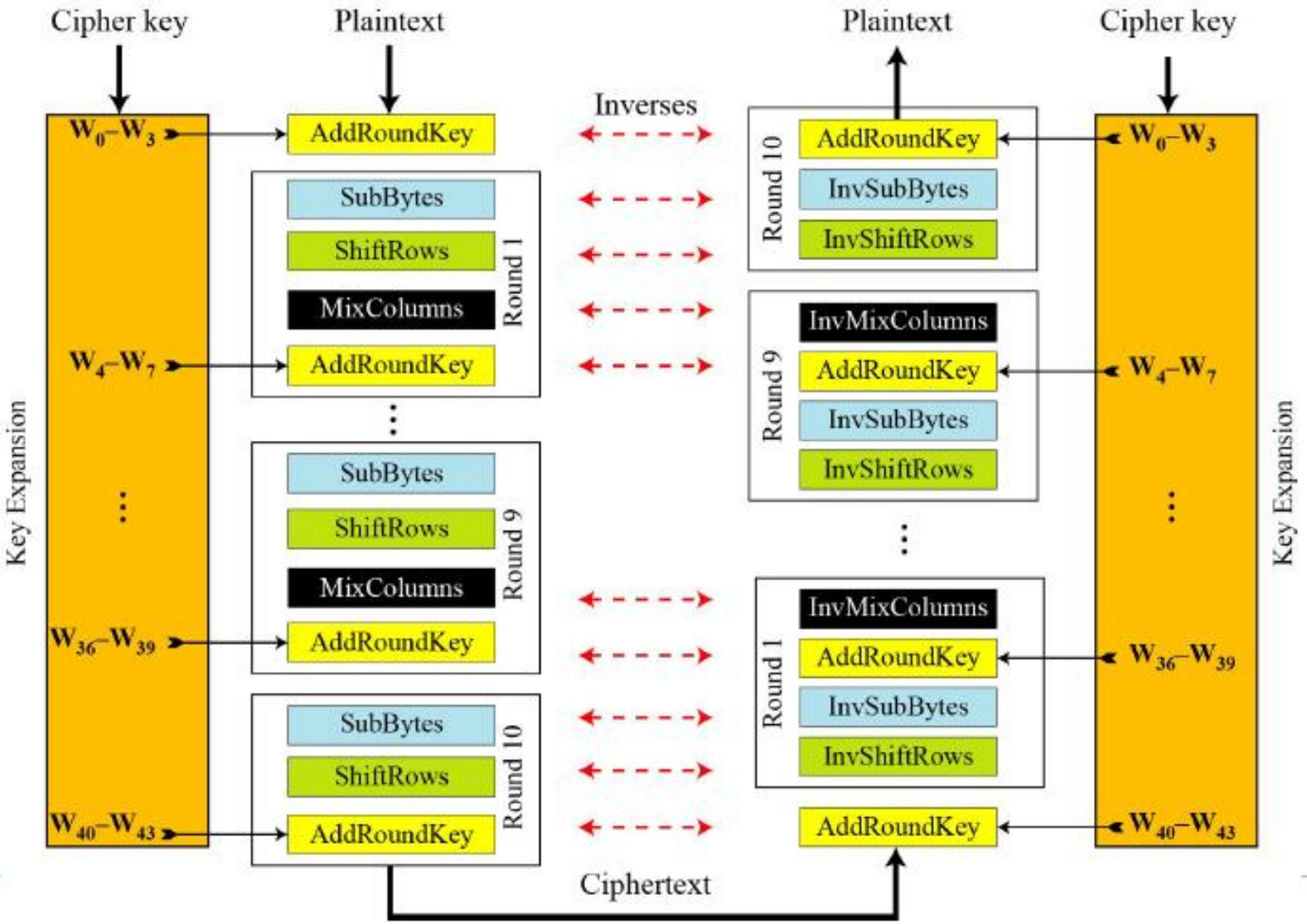
No. of rounds	Key size (in bits)
10	128
12	192
14	256

AES Parameters

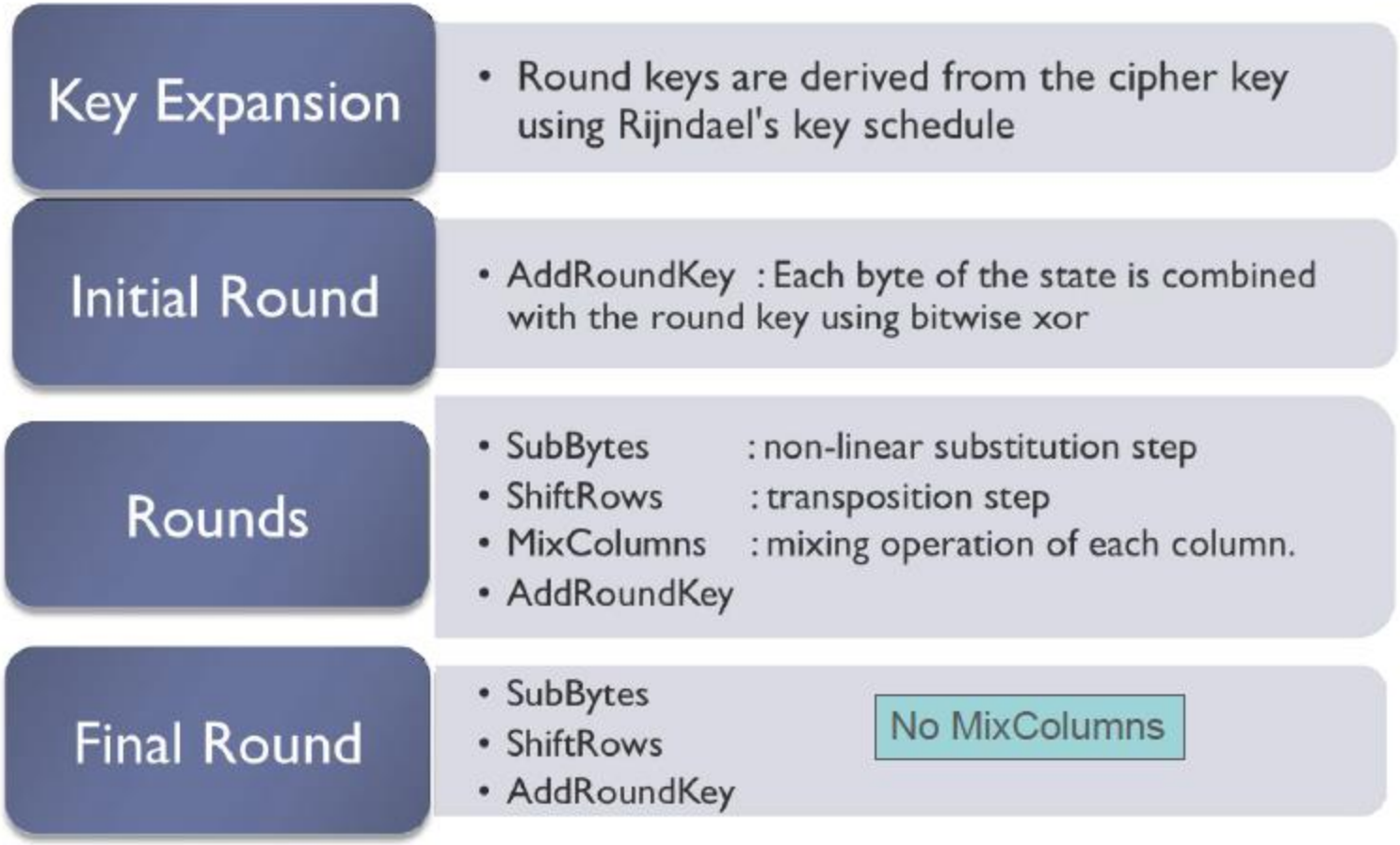
AES Encryption and decryption



AES Encryption and decryption

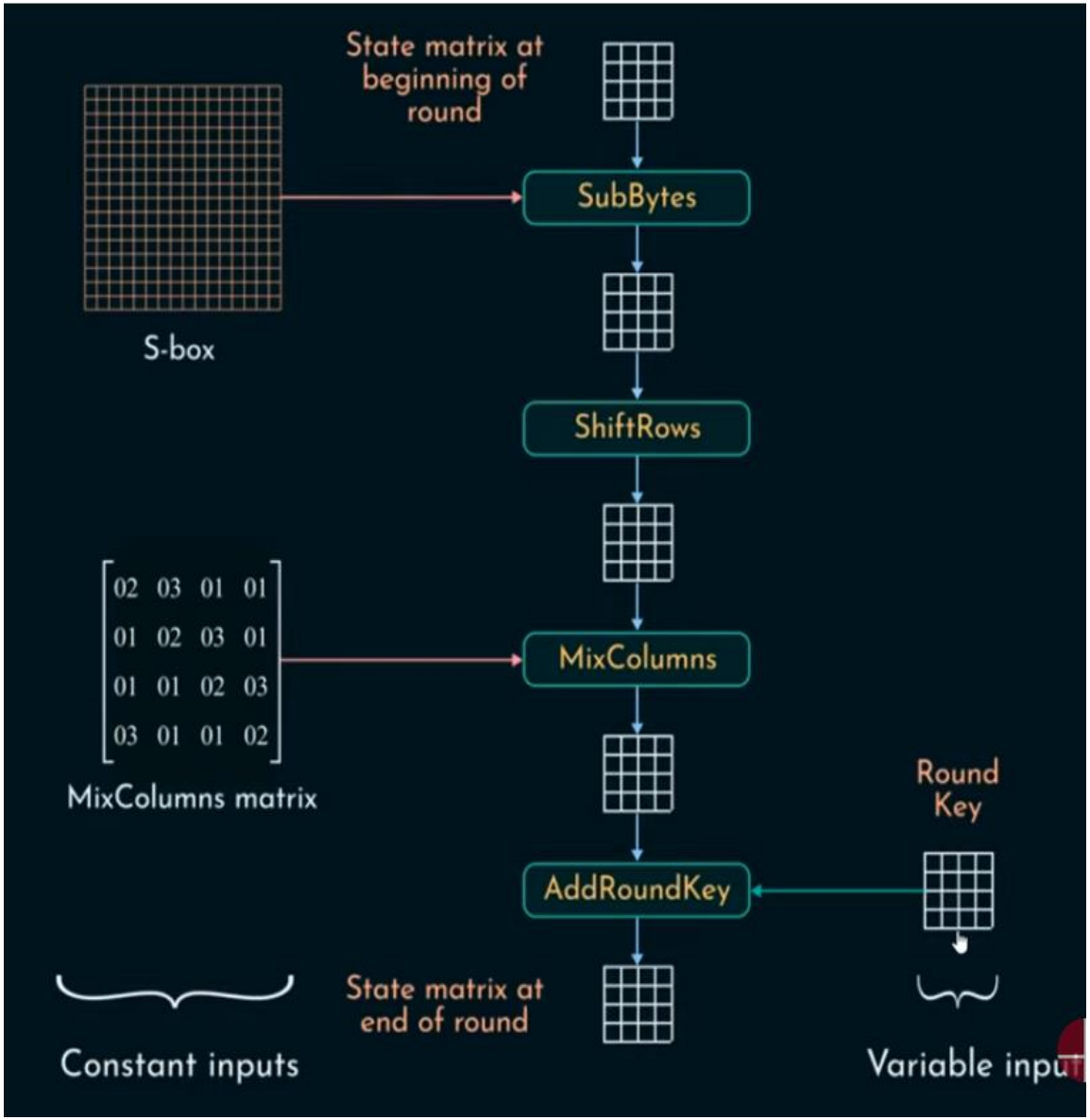


AES Encryption and decryption

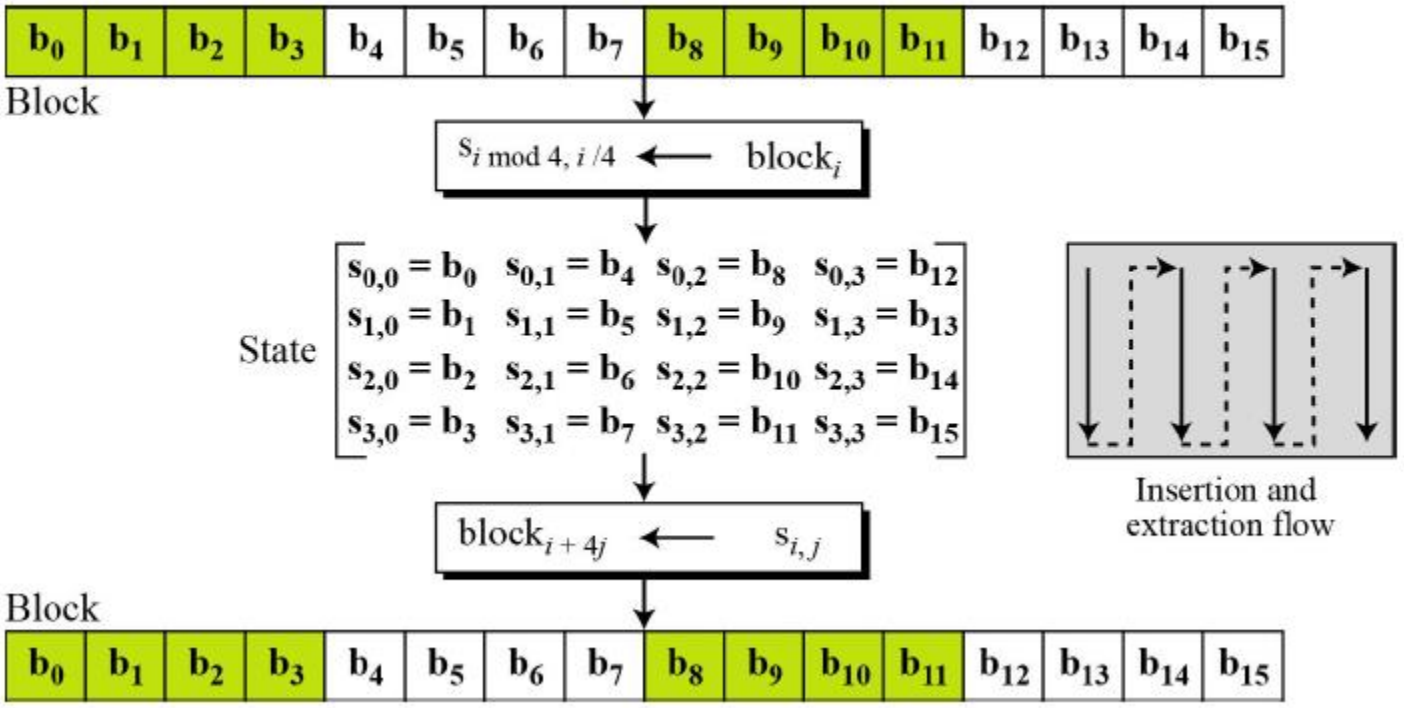


AES Transformation functions

- ★ Substitute Bytes
- ★ Shift Rows
- ★ Mix Columns
- ★ Add Round Key



Substitute byte Formation



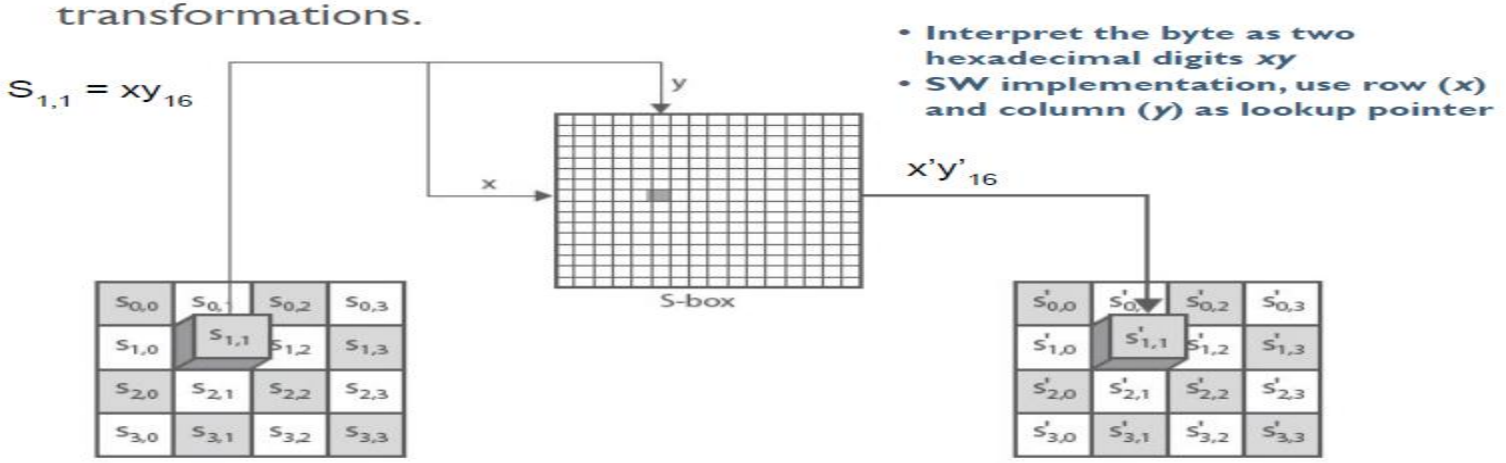
Changing Plain text to State

Text	A	E	S	U	S	E	S	A	M	A	T	R	I	X	Z	Z
Hexadecimal	00	04	12	14	12	04	12	00	0C	00	13	11	08	23	19	19

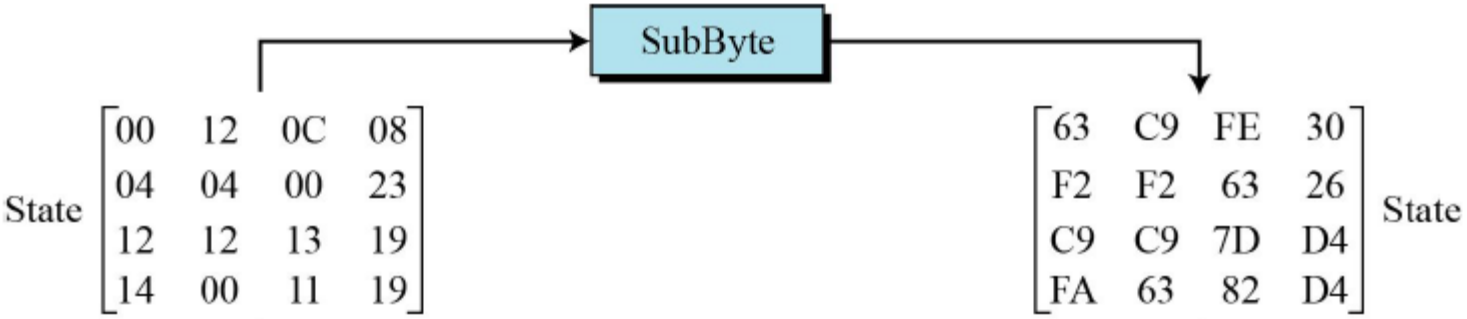
$$\begin{bmatrix} 00 & 12 & 0C & 08 \\ 04 & 04 & 00 & 23 \\ 12 & 12 & 13 & 19 \\ 14 & 00 & 11 & 19 \end{bmatrix}$$ State

Substitute byte Formation

- A simple substitution of each byte
  - provide a confusion
- Uses one S-box of 16x16 bytes containing a permutation of all 256 8-bit values
- Each byte of state is replaced by byte indexed by row (left 4-bits) & column (right 4-bits)
  - eg. byte {95} is replaced by byte in row 9 column 5
  - which has value {2A}
- The SubBytes operation involves 16 independent byte-to-byte transformations.



Substitute byte Formation



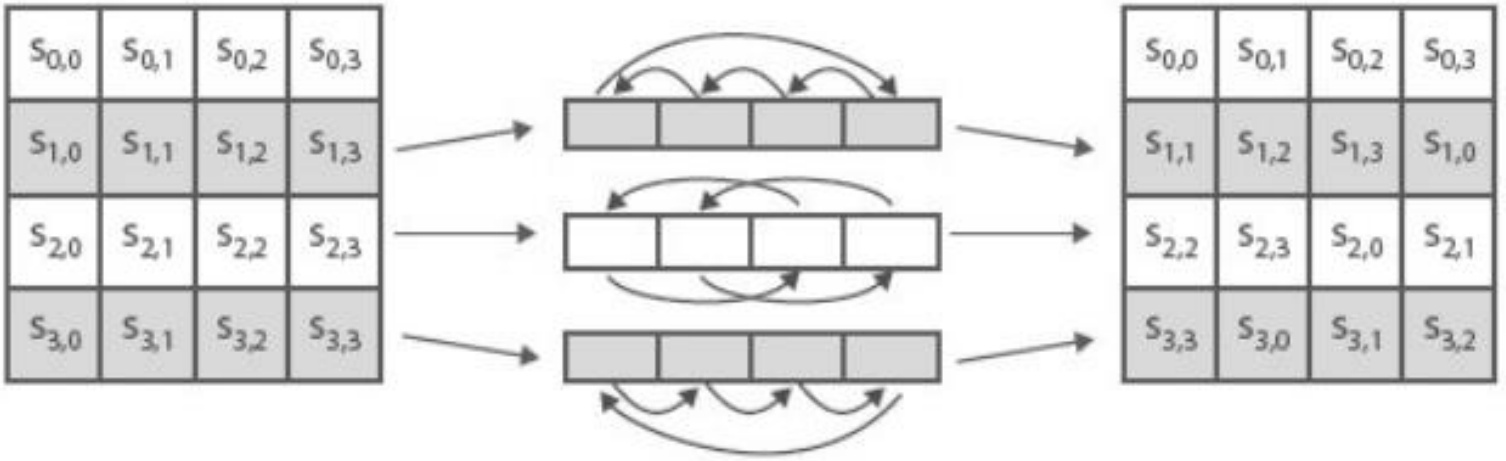
x \ y	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	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

Shift Rows and Mix Columns

ShiftRows and MixColumns provide diffusion to the cipher

Each column is processed separately

Each byte is replaced by a value dependent on all 4 bytes in the column

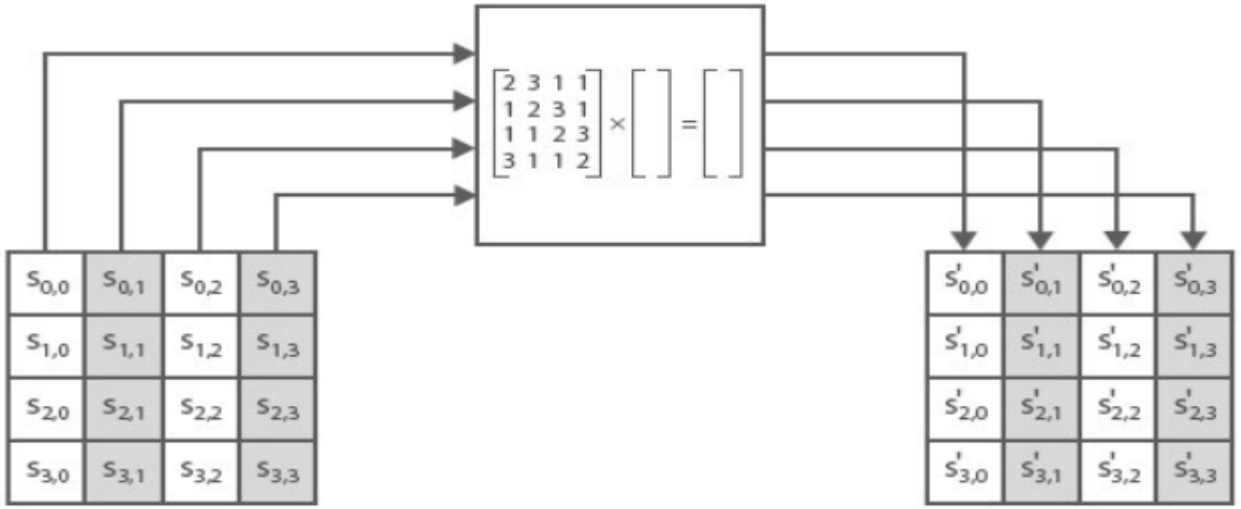


- 1st row is unchanged
- 2nd row does 1 byte circular shift to left
- 3rd row does 2 byte circular shift to left
- 4th row does 3 byte circular shift to left

Shift Rows and Mix Columns

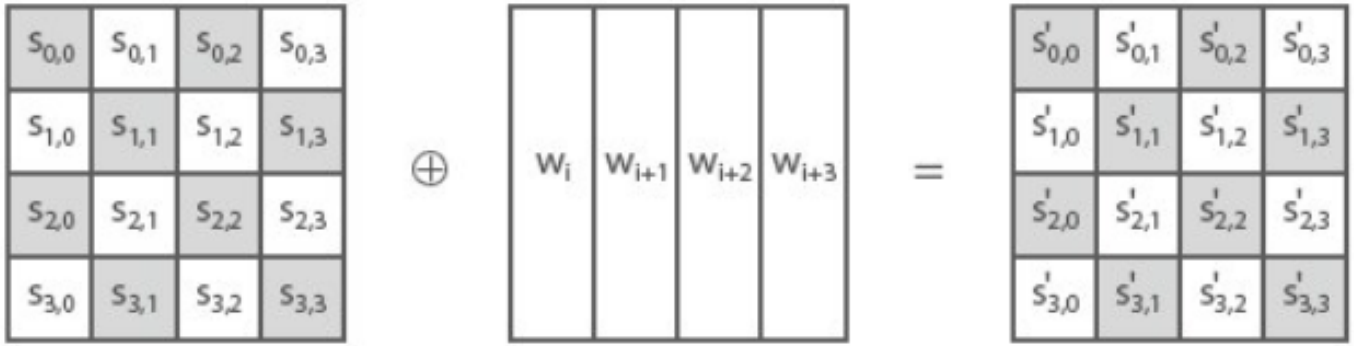
$$\begin{matrix} ax + by + cz + dt \\ ex + fy + gz + ht \\ ix + jy + kz + lt \\ mx + ny + oz + pt \end{matrix} = \begin{bmatrix} a & b & c & d \\ e & f & g & h \\ i & j & k & l \\ m & n & o & p \end{bmatrix} \times \begin{bmatrix} x \\ y \\ z \\ t \end{bmatrix}$$

New matrix | **Constant matrix** | Old matrix



The MixColumns transformation operates at the column level; it transforms each column of the state to a new column.

Add Round Key operation

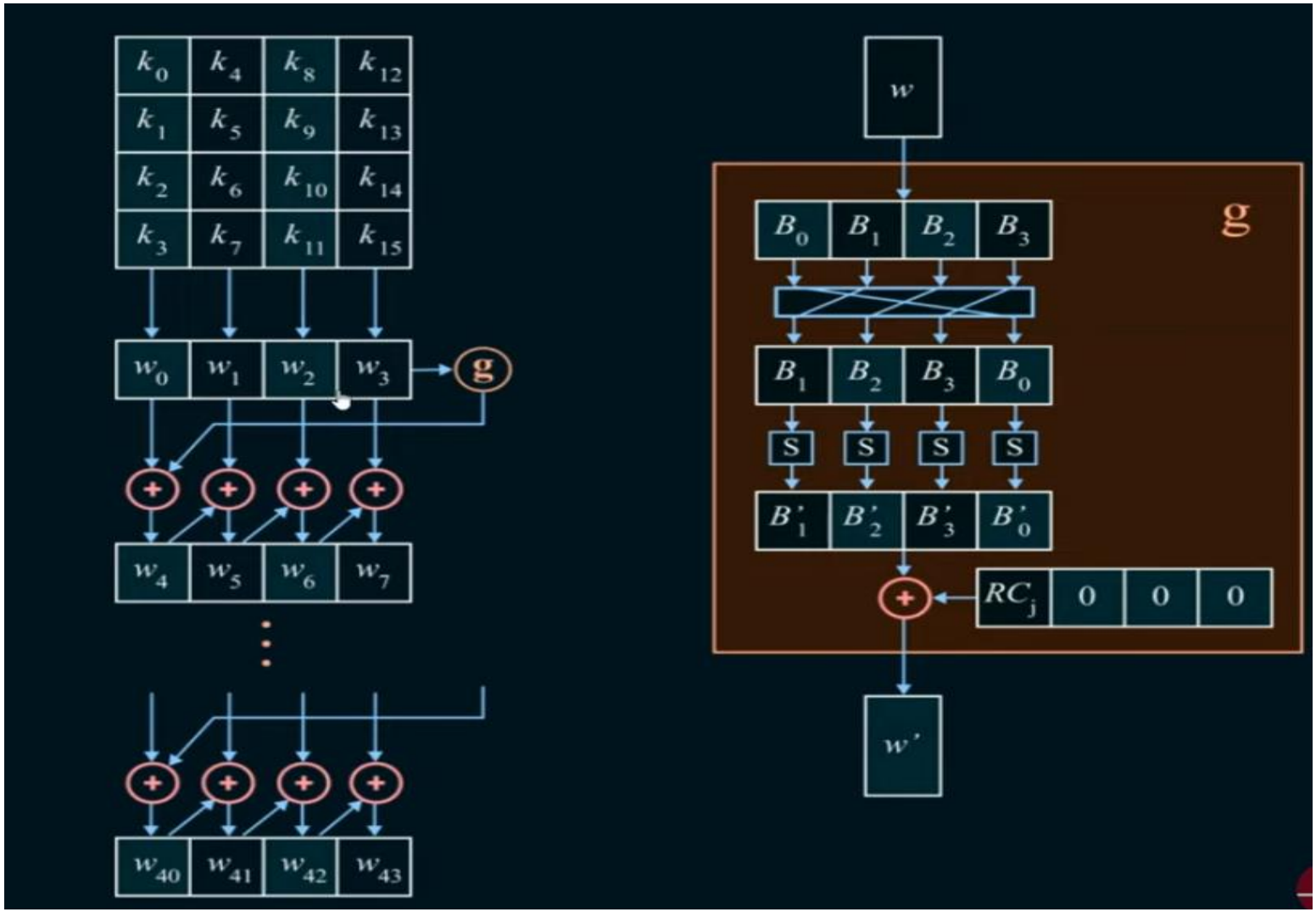


AES Key Scheduling

- takes 128-bits (16-bytes) key and expands into array of 44 32-bit words

Round	*Words*			
Pre-round	$\mathbf{w}_0$	$\mathbf{w}_1$	$\mathbf{w}_2$	$\mathbf{w}_3$
1	$\mathbf{w}_4$	$\mathbf{w}_5$	$\mathbf{w}_6$	$\mathbf{w}_7$
2	$\mathbf{w}_8$	$\mathbf{w}_9$	$\mathbf{w}_{10}$	$\mathbf{w}_{11}$
. . .	. . .			
N_r	$\mathbf{w}_{4N_r}$	$\mathbf{w}_{4N_r+1}$	$\mathbf{w}_{4N_r+2}$	$\mathbf{w}_{4N_r+3}$

AES Key Expansion



AES Key Substitution box

		y														
		0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
x	**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

AES Key Round constant

- RCON is a word in which the three rightmost bytes are zero
- It is different for each round and defined as:

  RCon[j] = (RCon[j],0,0,0)

  where RCon[1] =1 , RCon[j] = 2 * RCon[j-1]

Note: Initial Transformation takes $(00\ 00\ 00\ 00)_{16}$ as the RC.

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

Comparison of AES and DES

Basis For Comparison	DES (Data Encryption Standard)	AES (Advanced Encryption Standard)
Basic	The data block in **DES** is split into two halves.	The entire block in **AES** is processed as a single matrix.
Principle	It works on ***Feistel Cipher structure.***	The **substitution** and **permutation** principles are used in AES.
Year of Creation	**DES *(Data Encryption Standard)*** creation year is **1976.**	**AES (Advanced Encryption Standard)** creation year is **1999.**
Designed By	DES (Data Encryption Standard) was designed by **IBM.**	AES (Advanced Encryption Standard) was designed by **Vincent Rijmen** and **Joan Daeman.**
Rounds	16 rounds	10 rounds for 128-bit algo 12 rounds for 192-bit algo 14 rounds for 256-bit algo
Speed	DES is slower than AES.	AES is faster than DES.
Security	Because DES uses a smaller key, it is ***less secure.***	Because AES uses a large secret key, it is ***more secure.***
Key size	In comparison to **AES,** the key size of **DES** is lower.	In comparison to **DES, AES** has a larger key size,
Rounds Names	Expansion Permutation, Xor, S-box, P-box, Xor and Swap.	Subbytes, Shiftrow, Mix columns, Add roundkeys.
Plaintext	Plaintext is of **64 bits.**	Plaintext can be of **128,192,** or **256** bits.
Identified Attacks	Linear crypt-analysis, Differential crypt-analysis, and Brute-force.	There is no identified attack.
Block Size	128 bits	64 bits
Originate From	DES originate from the Lucifer cipher.	AES originate from the square cipher.

Key Differences Between DES and AES

References

- **William Stallings, “Cryptography and Network Security, Principles and Practice”, 6th Edition, Pearson Education, March 2013**
- **Behrouz A. Ferouzan, “Cryptography & Network Security”, Tata McGraw Hill**

THANK YOU