INFORMATION SECURITY FALL 2022

Week # 3

Lecture # 7, 8 and 9

Dr. Aqsa Aslam

PART ONE: Computer Security Technology and Principles

CHAPTER 2

CRYPTOGRAPHIC TOOLS

Topics from text book:

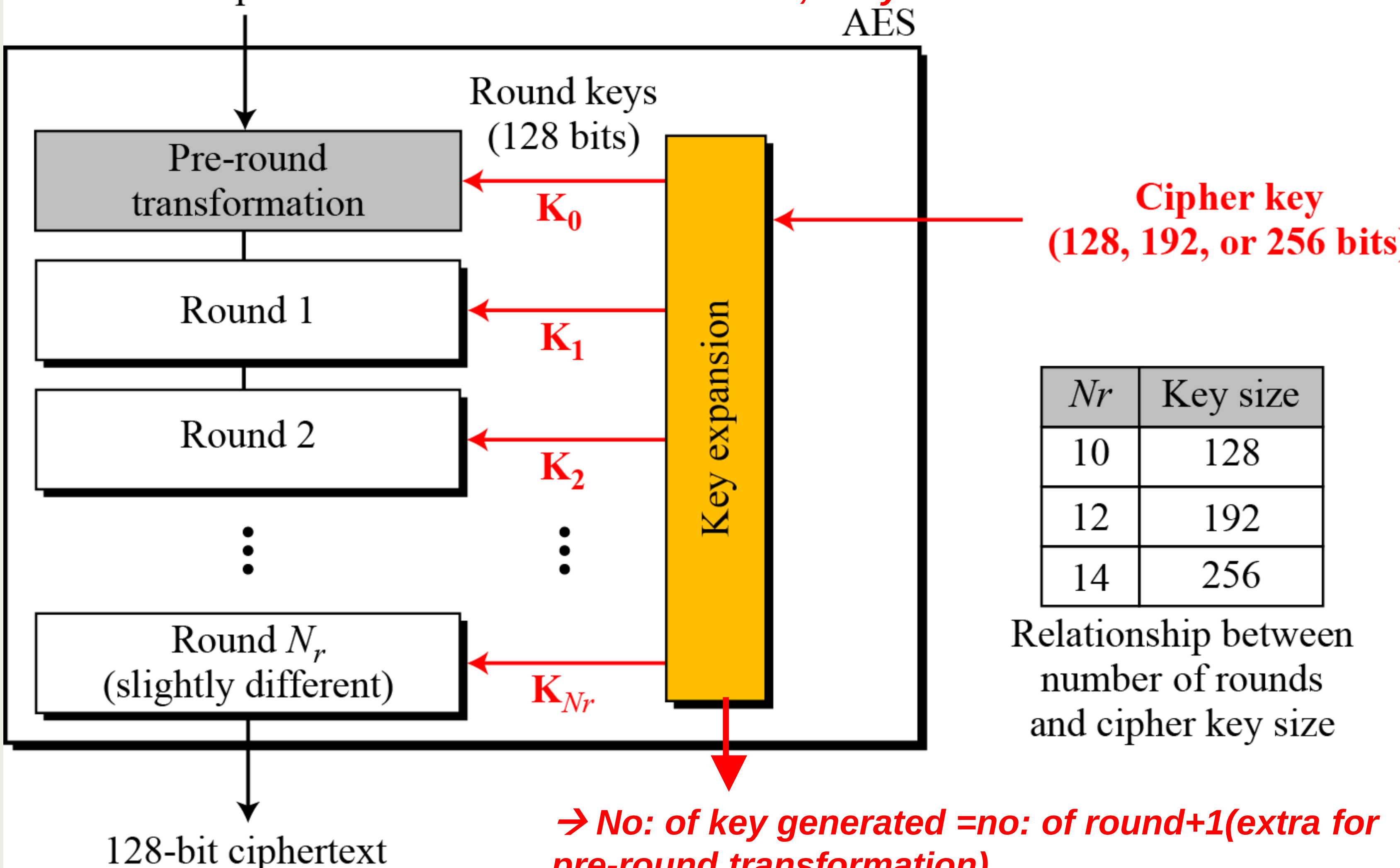
- Chapter # 2
- Chapter # 20
- Chapter # 21

ADVANCED ENCRYPTION STANDARD

- The **Advanced Encryption Standard (AES)** was issued as a federal information processing standard FIPS 197 (*Advanced Encryption Standard*, November 2001).
  - ***It is intended to replace DES and triple DES with an algorithm that is more secure and efficient.***
- AES is a non-Feistel cipher that encrypts and decrypts a **data block of 128 bits.**
- AES has defined three versions, with 10, 12, and 14 rounds.
  - Each version uses a different cipher key size (128, 192, or 256).

Figure 7.1 *General design of AES encryption cipher*

→ ***Fixed size=128 bit i-e., 16bytes***



Nr	Key size
10	128
12	192
14	256

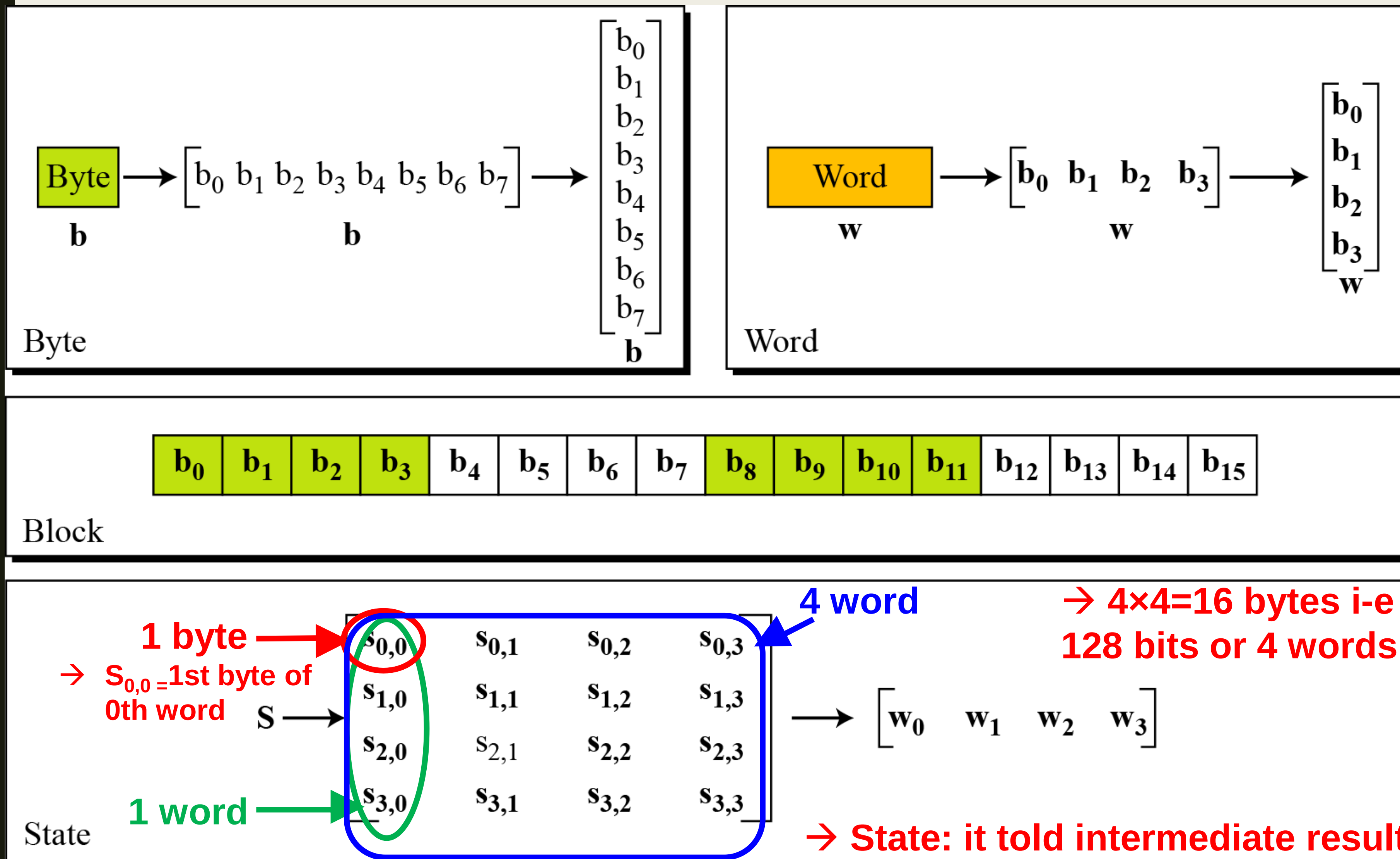
Relationship between number of rounds and cipher key size

→ ***No: of key generated =no: of round+1(extra for pre-round transformation)***

7.1.4 Data Units.

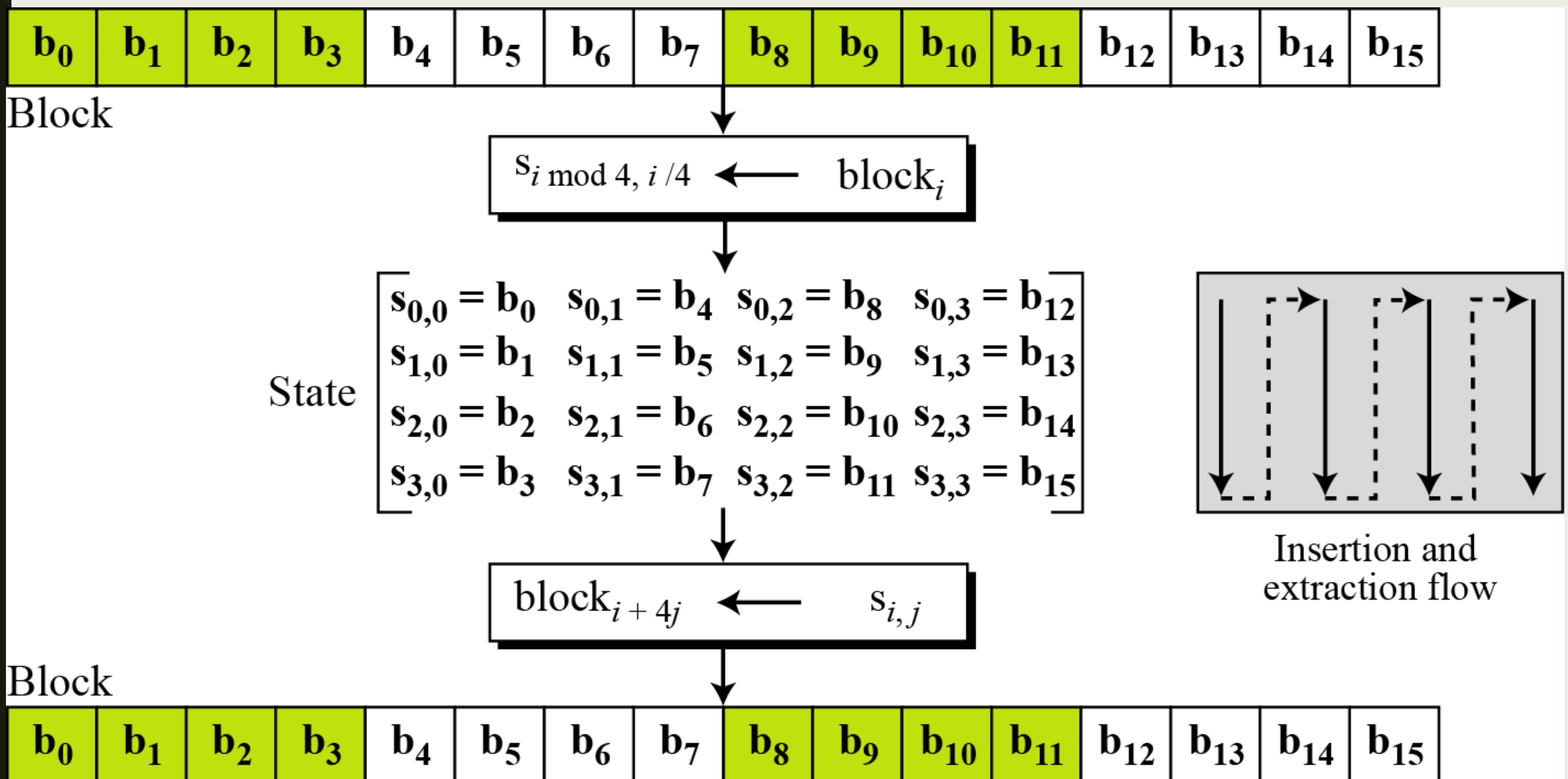
→ 1 byte= group of 8 bit
→ 1 word=4 bytes=32 bit
→ Block size=128 bit data

Figure 7.2 *Data units used in AES*



7.1.4 Data Units.

Figure 7.3 ***Block-to-state and state-to-block transformation***



7.1.4 Continue

Example 7.1 *Continue*

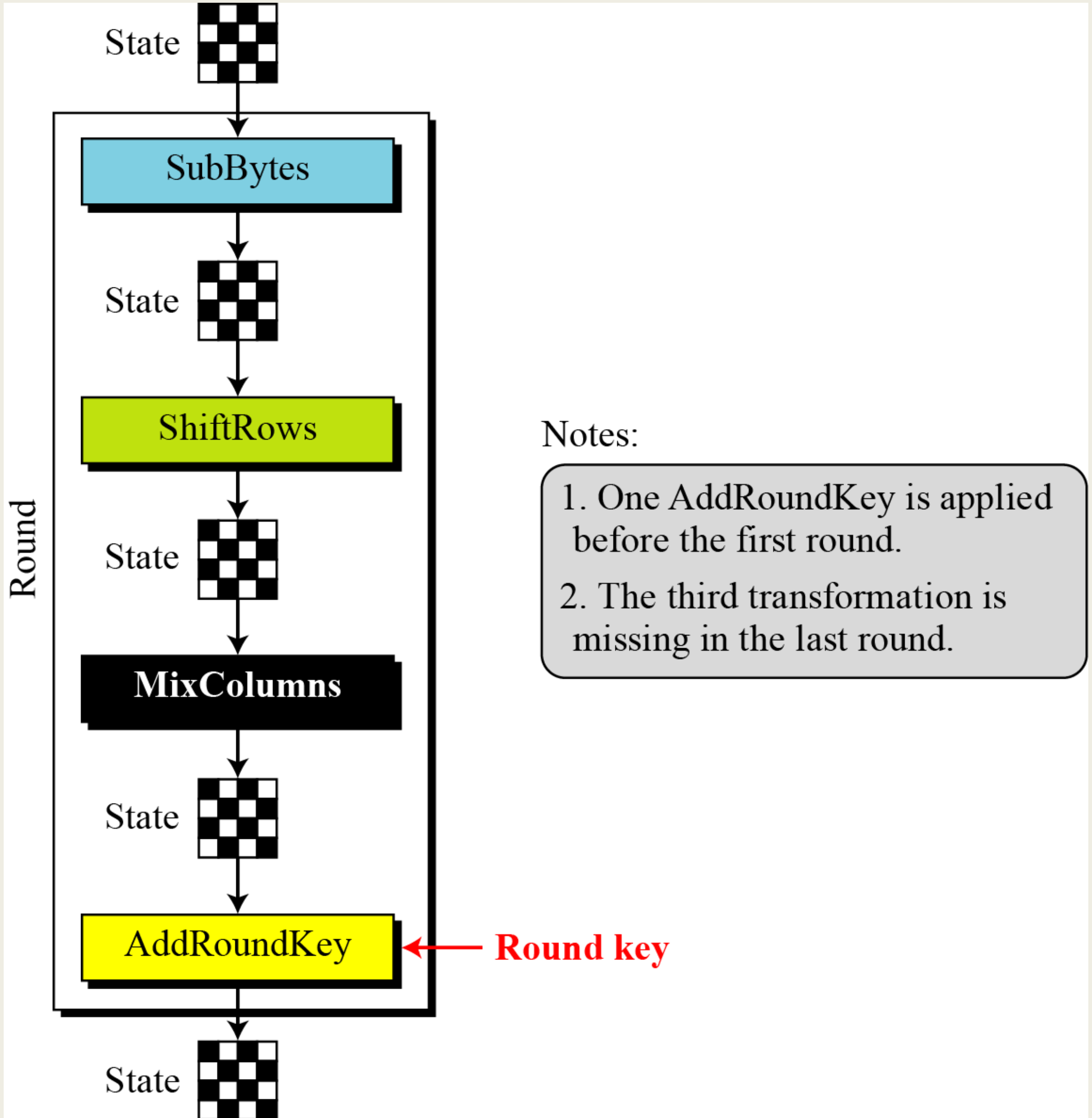
Figure 7.4 ***Changing plaintext to state***

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

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

7.1.5 Structure of Each Round

Figure 7.5 ***Structure of each round at the encryption site***



AES - Steps

- **KeyExpansion**—round keys are derived from the cipher key using Rijndael's key schedule.
- **Initial Round**
  - ***AddRoundKey***—*each byte of the state is combined with the round key using bitwise xor.*
- **Round**
  - *Four different stages are used, one* ***of permutation*** *and* ***three of substitution:***
    - **Substitute Bytes:** Uses a table, referred to as an S-box,3 to perform a byteby-byte substitution of the block
    - **Shift Rows:** A simple permutation that is performed row by row
    - **Mix Columns:** A substitution that alters each byte in a column as a function of all of the bytes in the column
    - **Add Round key:** A simple bitwise XOR of the current block with a portion of the expanded key
- **Final Round (no Mix-Columns)**
  - ***SubBytes***
  - ***ShiftRows***
  - ***AddRoundKey***

TRANSFORMATIONS

– *Four different stages are used, one* ***of permutation*** *and* ***three of substitution:***

  - **Substitute Bytes:** Uses a table, referred to as an S-box,3 to perform a byteby-byte substitution of the block
  - **Shift Rows:** A simple permutation that is performed row by row
  - **Mix Columns:** A substitution that alters each byte in a column as a function of all of the bytes in the column
  - **Add Round key:** A simple bitwise XOR of the current block with a portion of the expanded key

7.2.1 Substitution

AES, like DES, uses substitution. AES uses two invertible transformations.

SubBytes

The first transformation, SubBytes, is used at the encryption site. To substitute a byte, we interpret the byte as two hexadecimal digits.

Note

The SubBytes operation involves 16 independent byte-to-byte transformations.

7.2.1 Continue

*SubBytes is simply a table lookup using a 16×16 matrix of byte values called an **s-box**. This matrix consists of all the possible combinations of an 8 bit sequence (28= 16×16 = 256).*

Figure 7.6 ***SubBytes transformation***

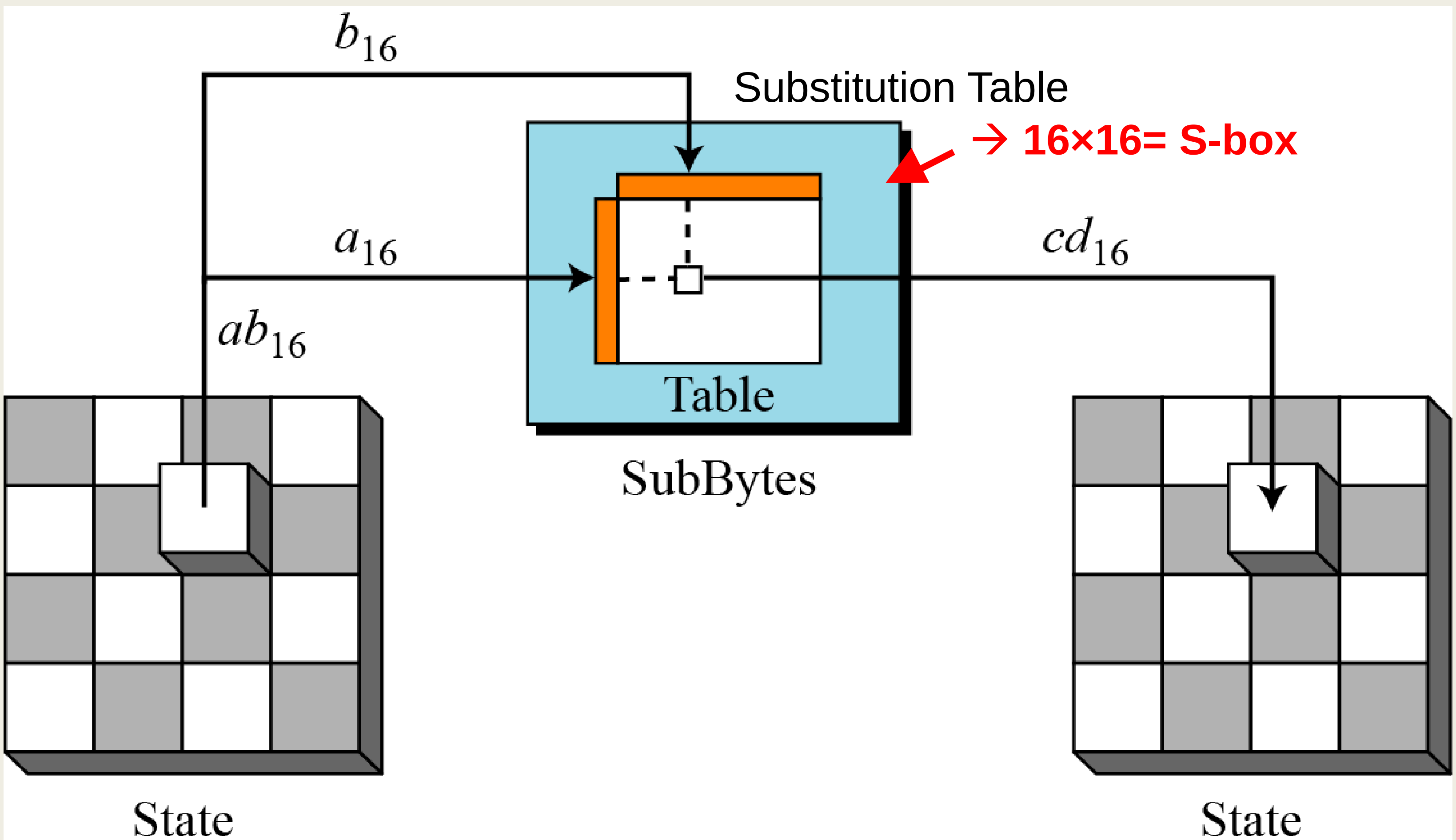


Table 7.1 *SubBytes transformation table*

16×16= S-box

	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

→ 16 bytes

→ Initial byte represent rows and last part represent column e.g **000 0010**. (0 row and 2 column)

Table 7.1 *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

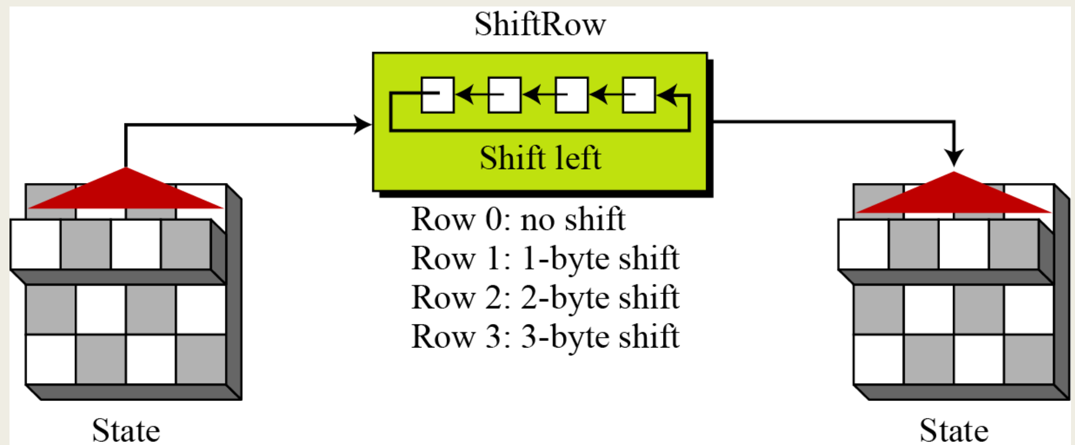
$$\text{State}\begin{bmatrix} 00 & 12 & 0C & 08 \\ 04 & 04 & 00 & 23 \\ 12 & 12 & 13 & 19 \\ 14 & 00 & 11 & 19 \end{bmatrix} \underset{\text{InvSubByte}}{\overset{\text{SubByte}}{\rightleftarrows}} \begin{bmatrix} 63 & C9 & FE & 30 \\ F2 & F2 & 63 & 26 \\ C9 & C9 & 7D & D4 \\ FA & 63 & 82 & D4 \end{bmatrix}\text{State}$$

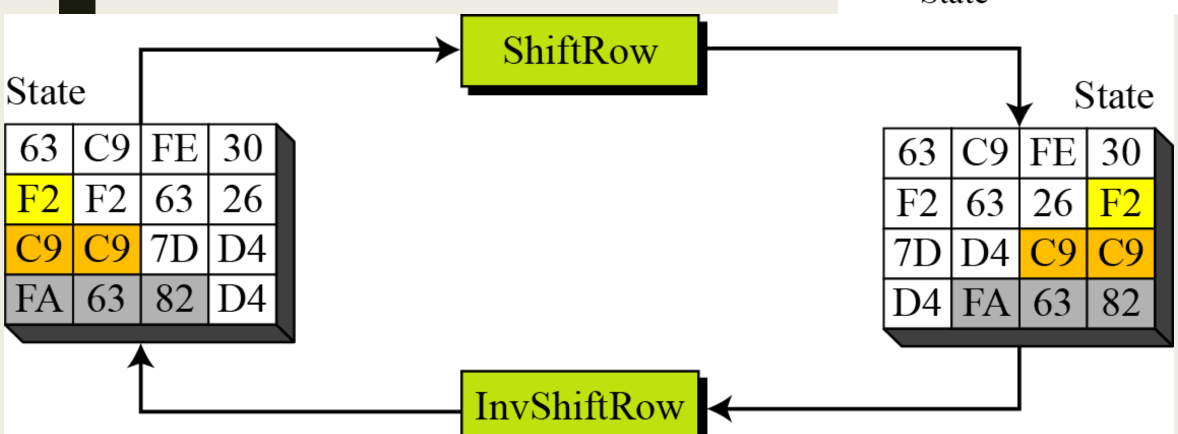
7.2.2 Permutation

- *Another transformation found in* ***a round is shifting,*** *which permutes the bytes*
- *In the encryption, the transformation is called ShiftRows*

→ Permutation perform on a byte level
→ Shift is done to the left
→ Shift depends on the row of the matrix

Figure 7.9 ***ShiftRows transformation***





MixColumns

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

Example

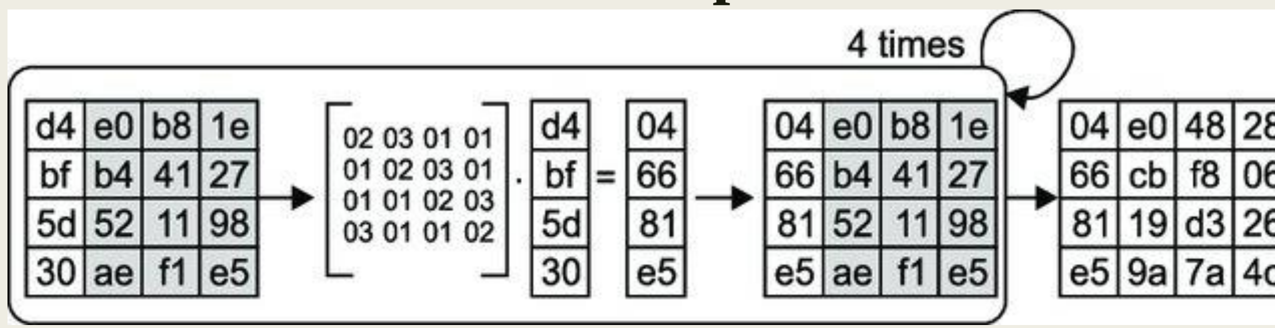
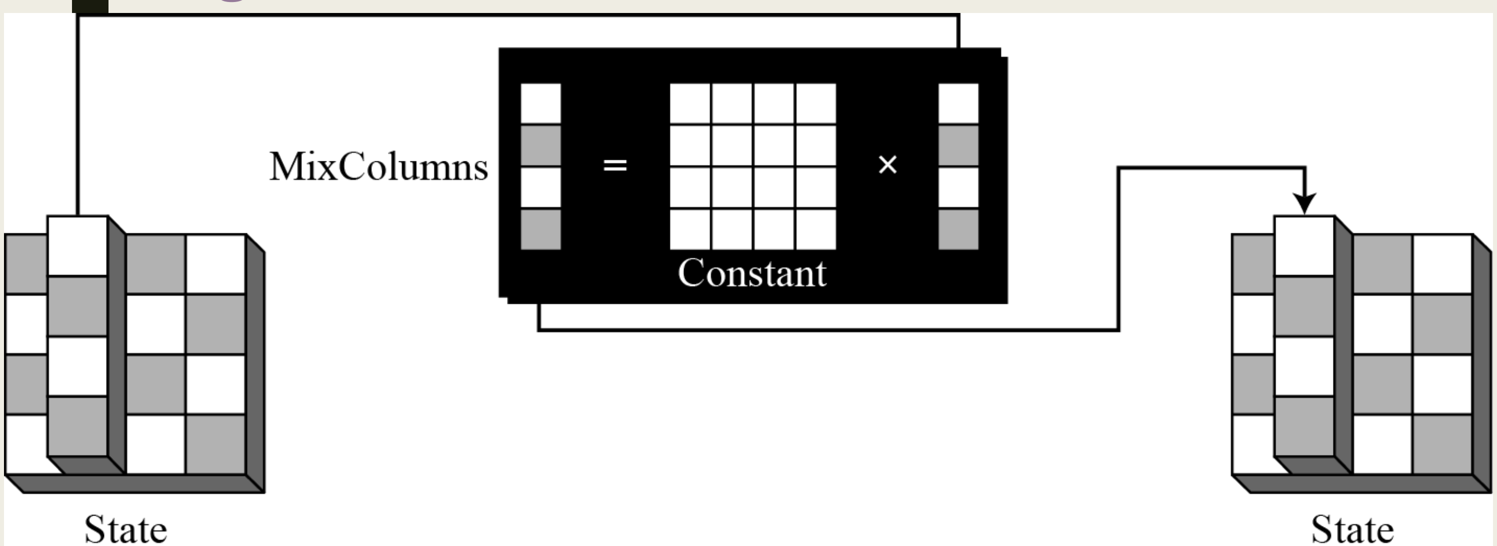


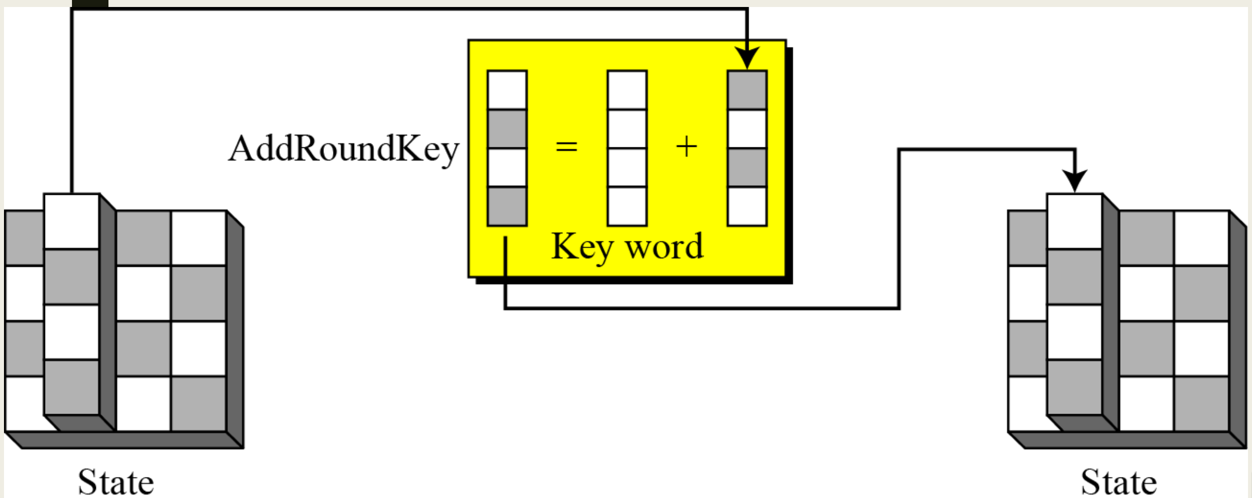
Figure 7.13 *MixColumns transformation*

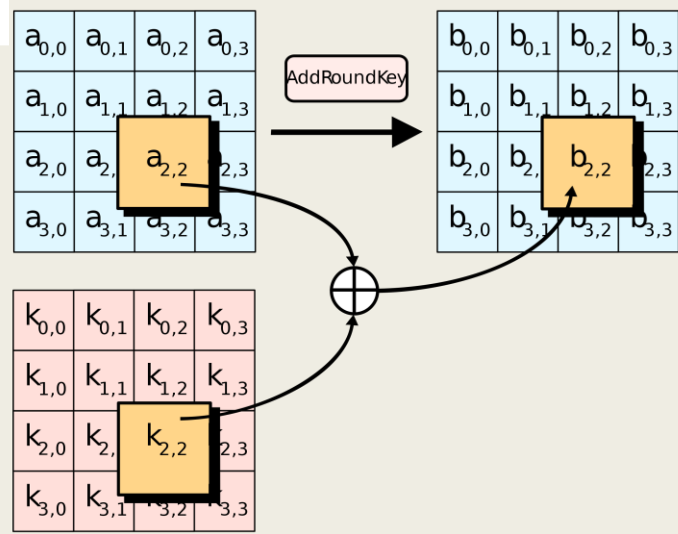


AddRoundKey

In the forward add round key transformation, called AddRoundKey, the 128 bits of State are bitwise XORed with the 128 bits of the round key.

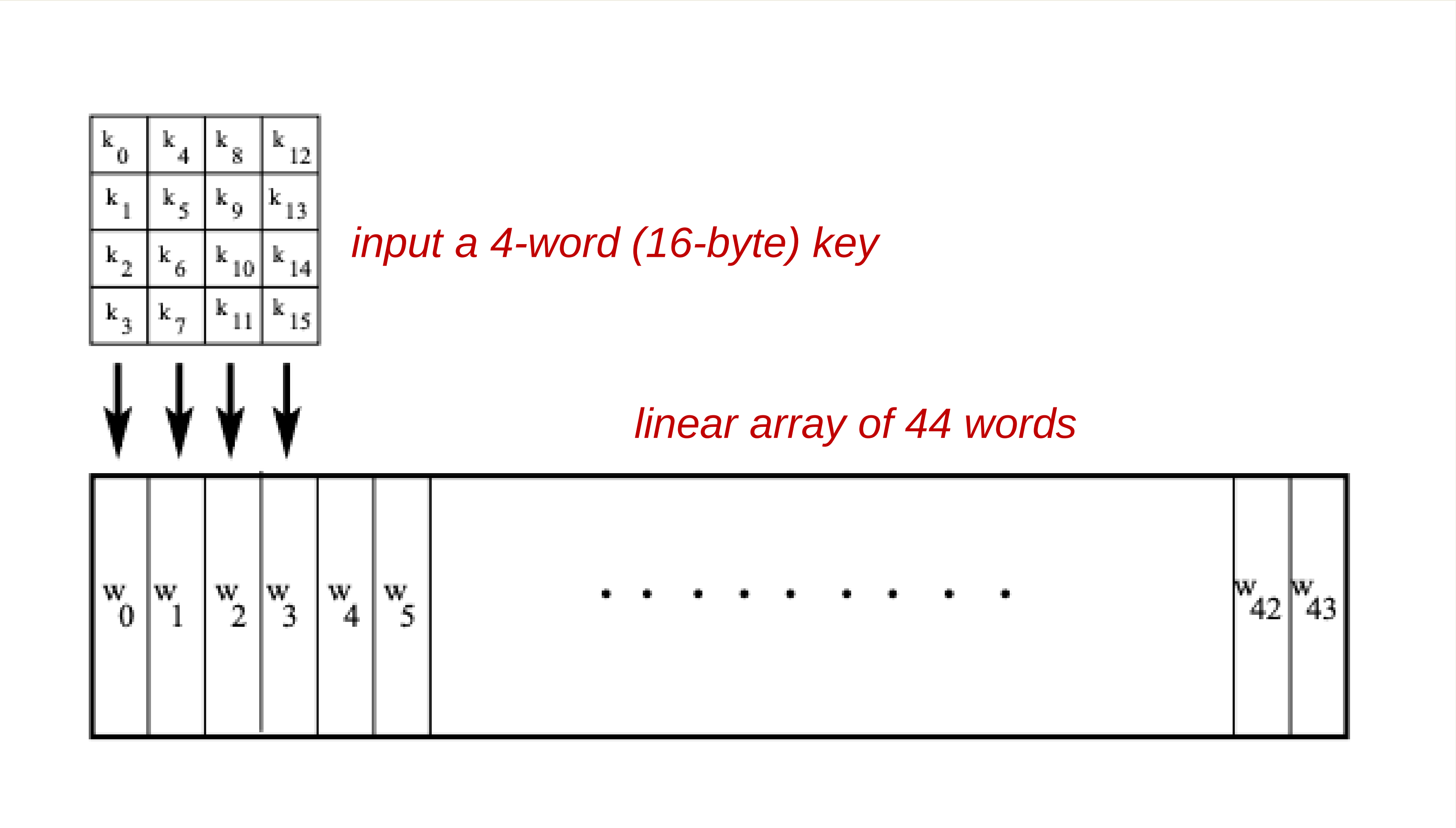
Figure 7.15 ***AddRoundKey transformation***





AES Key Expansion

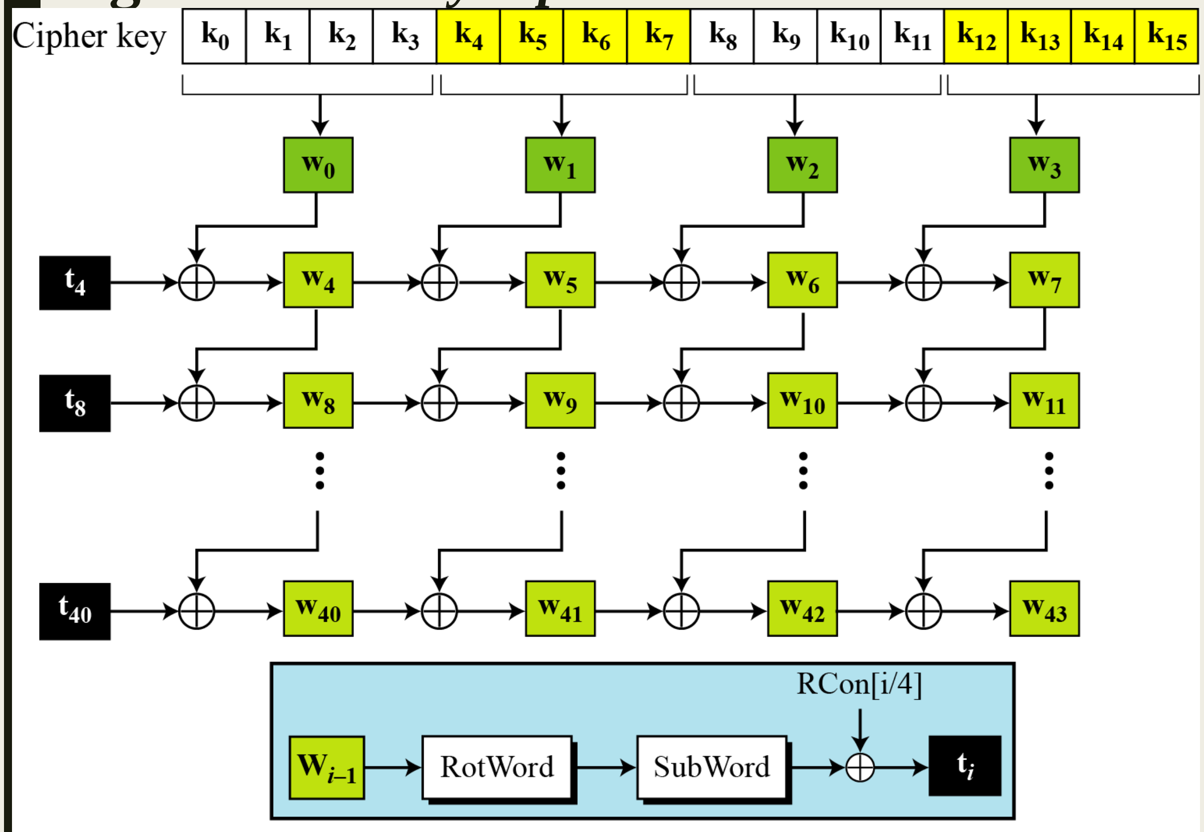
- *To create round keys for each round, AES uses a key-expansion process*. The AES key expansion algorithm takes ***as input a 4-word (16-byte) key*** and produces a ***linear array of 44 words***. *This is sufficient to provide a 4-word round key for the initial Add Round Key stage and each of the 10 rounds of the cipher.*



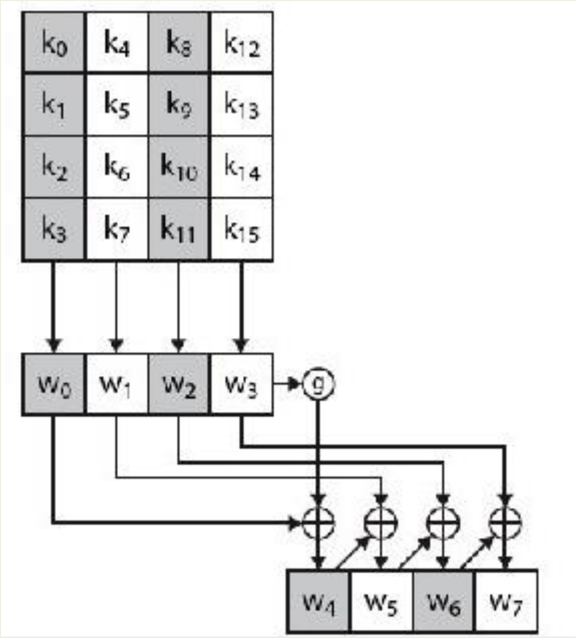
AES Key Expansion

- *To create round keys for each round, AES uses a key-expansion process*. The AES key expansion algorithm takes *as input a 4-word (16-byte) key* and produces a *linear array of 44 words*. *This is sufficient to provide a 4-word round key for the initial Add Round Key stage and each of the 10 rounds of the cipher.*

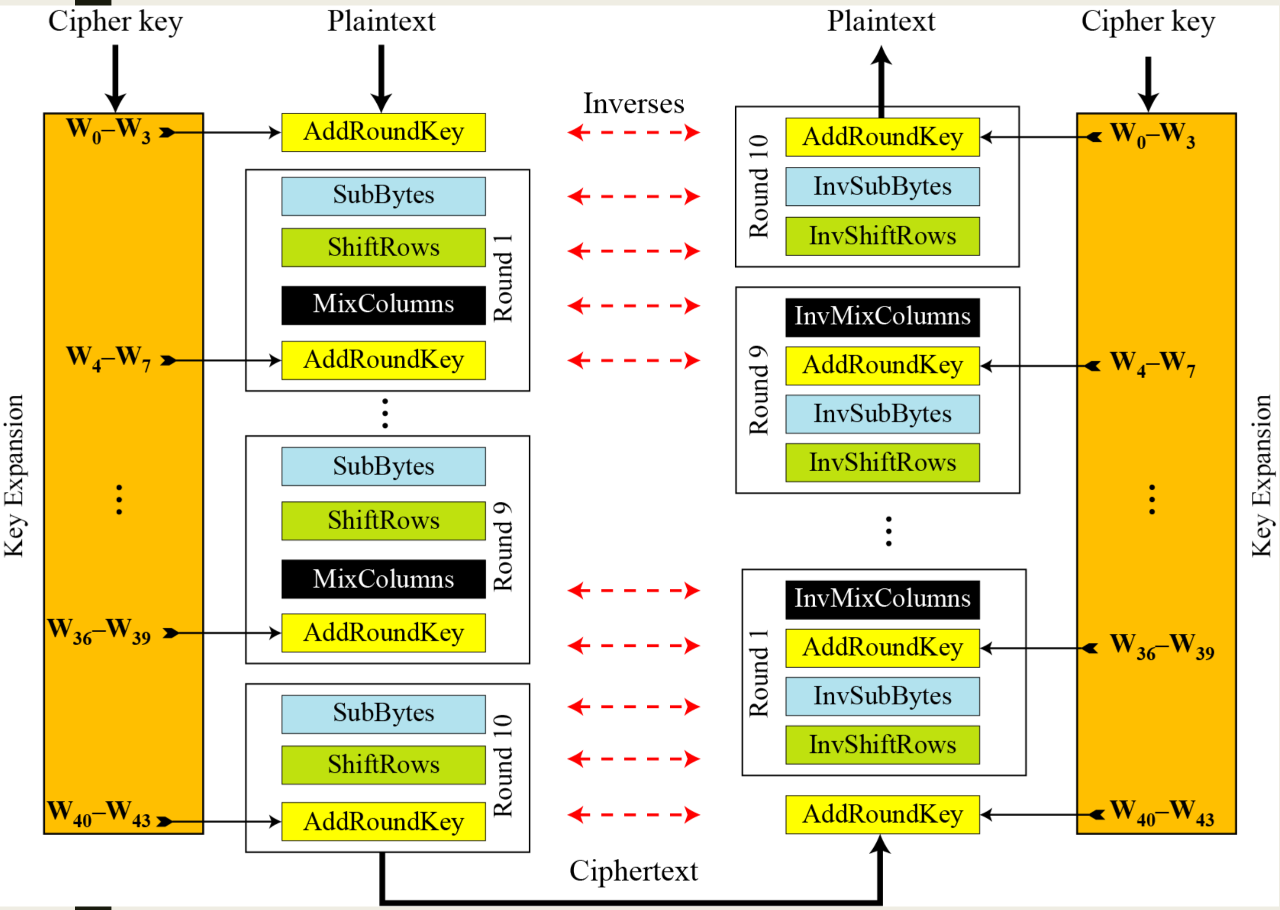
Figure 7.16 ***Key expansion in AES***

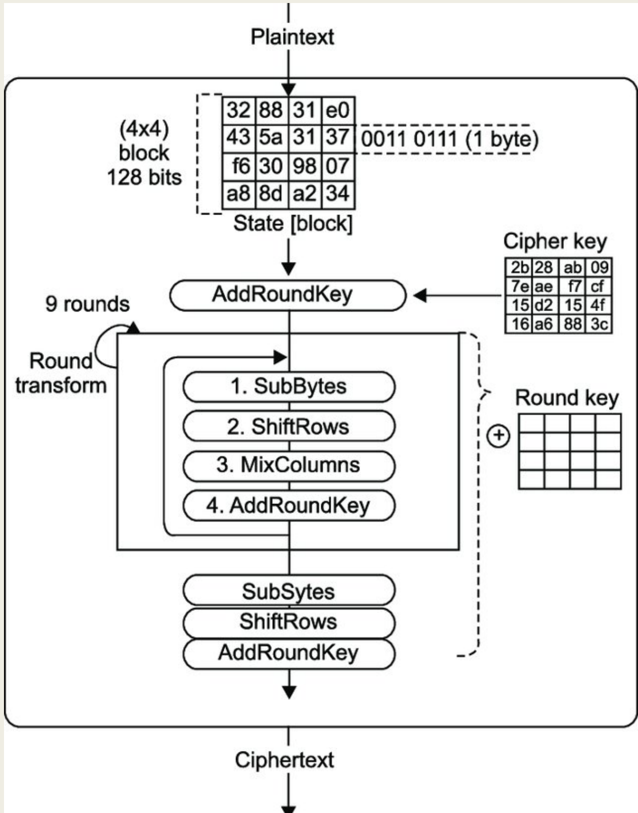


Making of t_i (temporary) words $i = 4\ N_r$



Ciphers and inverse ciphers of the original design





Claude Shannon (1949) gave two properties that a good cryptosystem should have to hinder statistical analysis: **diffusion** and **confusion**.

- **Diffusion** means that if we change a character of the plaintext, then several characters of the ciphertext should change, and similarly, if we change a character of the ciphertext, then several characters of the plaintext should change.

Plaintext 1:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
Plaintext 2:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	01
Ciphertext 1:	63	2C	D4	5E	5D	56	ED	B5	62	04	01	A0	AA	9C	2D	8D
Ciphertext 2:	26	F3	9B	BC	A1	9C	0F	B7	C7	2E	7E	30	63	92	73	13

- **Confusion** means that the key does not relate in a simple way to the ciphertext. In particular, each character of the ciphertext should depend on several parts of the key.

Confusion = Substitution a --> b, **Diffusion = Transposition or Permutation** abcd --> dacb

Table 20.3 **Block Cipher Modes of Operation**

Mode	Description	Typical Application
Electronic Code book (ECB)	Each block of 64 plaintext bits is encoded independently using the same key.	• Secure transmission of single values (e.g., an encryption key)
Cipher Block Chaining (CBC)	The input to the encryption algorithm is the XOR of the next 64 bits of plaintext and the preceding 64 bits of ciphertext.	• General-purpose block-oriented transmission • Authentication
Cipher Feedback (CFB)	Input is processed *s* bits at a time. Preceding ciphertext is used as input to the encryption algorithm to produce pseudorandom output, which is XORed with plaintext to produce next unit of ciphertext.	• General-purpose stream-oriented transmission • Authentication
Output Feedback (OFB)	Similar to CFB, except that the input to the encryption algorithm is the preceding DES output.	• Stream-oriented transmission over noisy channel (e.g., satellite communication)
Counter (CTR)	Each block of plaintext is XORed with an encrypted counter. The counter is incremented for each subsequent block.	• General-purpose block-oriented transmission • Useful for high-speed requirements