Fundamentals of Information & Network Security
ECE 471/571

Lecture #11,12: DES Security, and AES

Instructor: Ming Li
Dept of Electrical and Computer Engineering
University of Arizona

DES Summary

- Two techniques
  - Substitution provides the confusion
  - Transposition provides the diffusion
- Accomplish:
  - The output bits have no obvious relationship to the input bits
  - Spreading the effect of one input bit to other bits in the output.
- Implementation
  - Uses only standard arithmetic and logic operations
  - Repetitive algorithm: suitable for hardware

Multiple Encryption DES

- Encrypting twice with the same key
  - Problem?

$$\textbf{plaintext} \xrightarrow{K} \qquad \xrightarrow{K} \textbf{ciphertext}$$

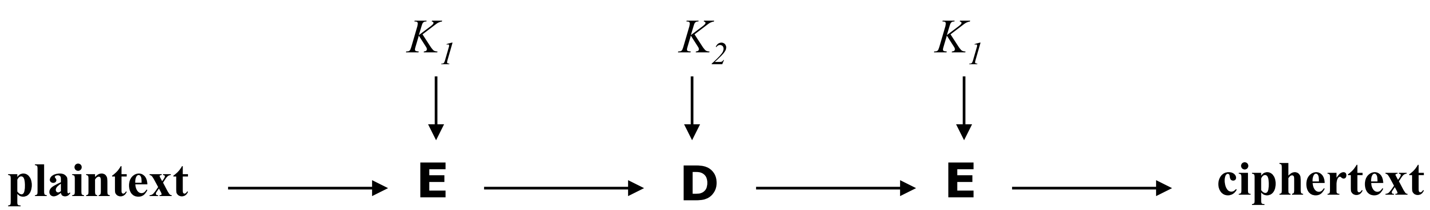
- Encrypting twice with two keys
  - Problem?
  - Meet-in-the-middle attack

$$\textbf{plaintext} \xrightarrow{K_1} \qquad \xrightarrow{K_2} \textbf{ciphertext}$$

(Read [Kaufman] 4.4.1.2 on page 111)

Triple DES

- Triple encryption with only two keys
  - 112-bit key, 64-bit data block
  - Why two keys, not three?
  - Why EDE, not EEE?

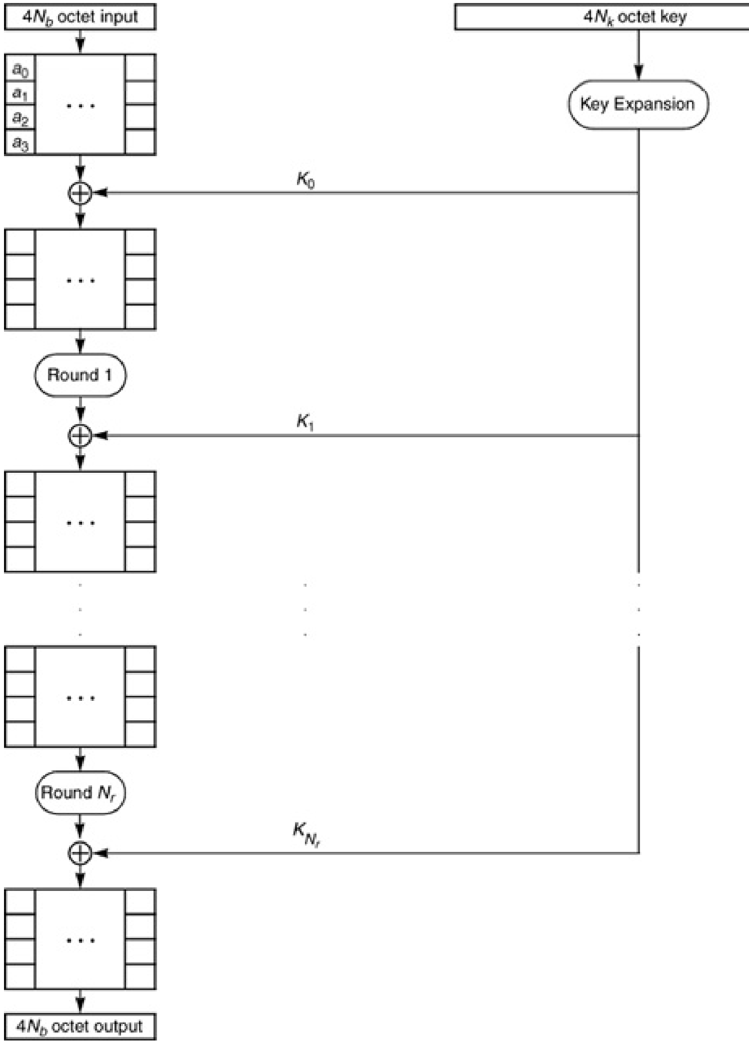


AES History

- NIST published RFP for Advanced Encryption Algorithm in 1997:
  - Fully specified and explained algorithm
  - Variable strength by key size (128, 192, 256 bits)
  - Efficient implementation on various software & hardware platforms
- In 1998, cryptographic community was asked to comment on 15 candidates.
- In 1999, out of 15, the selection was narrowed to 5 candidates: MARS, RC6, Rijndael, Serpent, and Twofish.
- Rijndael was selected in November 2001

Overview of Rijndael/AES

- <u>Key size</u>: 128-, 192-, or 256-bits.
- <u>Block size</u>: 128 bits
- <u>Number of rounds</u>:
  - AES 128 -- 10 rounds
  - AES 192 -- 12 rounds
  - AES 256 -- 14 rounds
- A 128-bit <u>round key</u> is used for each round
  - 128 bits = 16 bytes = 4 words
  - needs Nr+1 round keys for Nr rounds
  - If 10 rounds, needs 44 words for round keys



Overview of AES

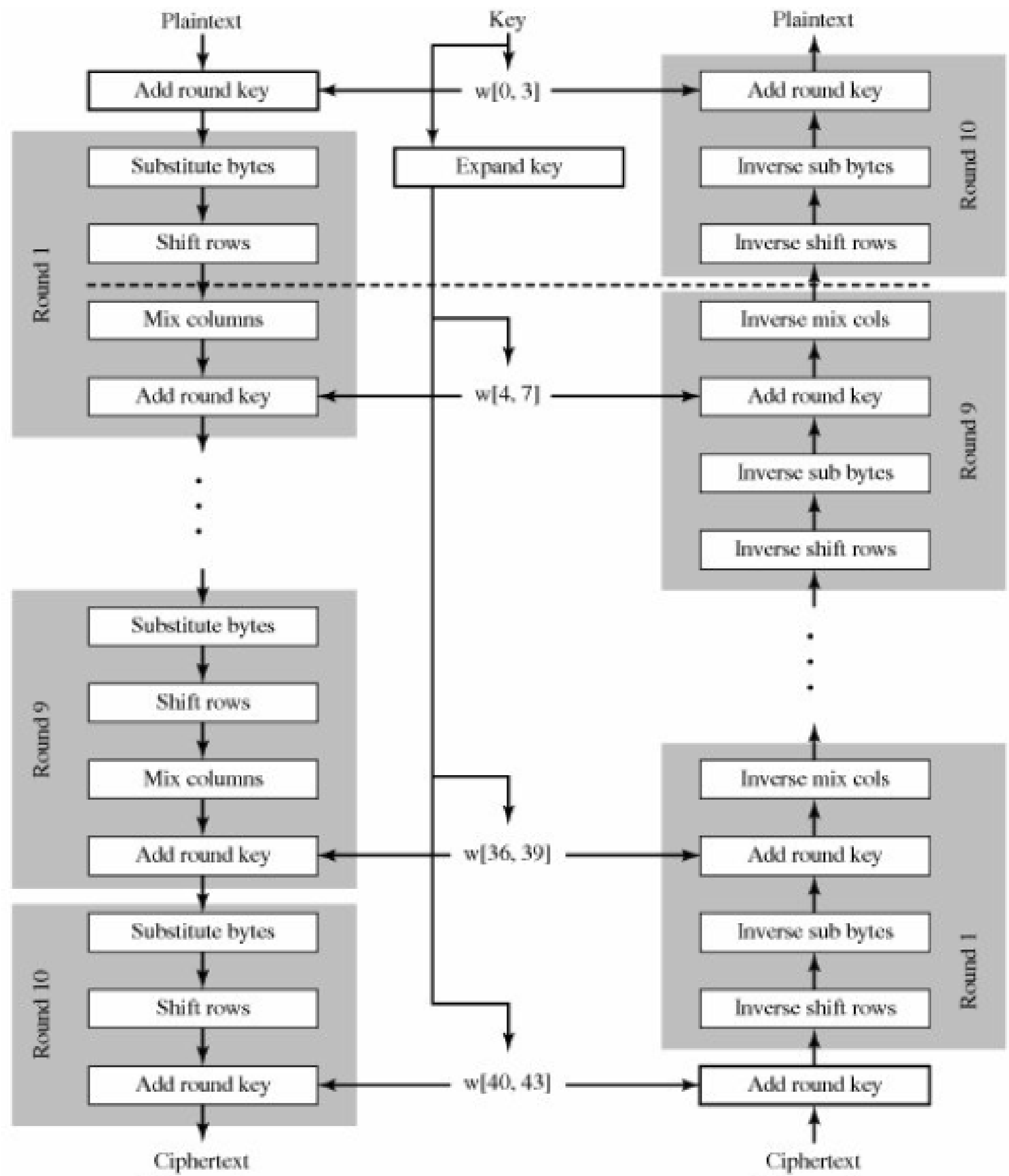
AES-128:

$N_b = 4$

$N_k = 4$

$N_r = 6+\max(N_b,N_k)$

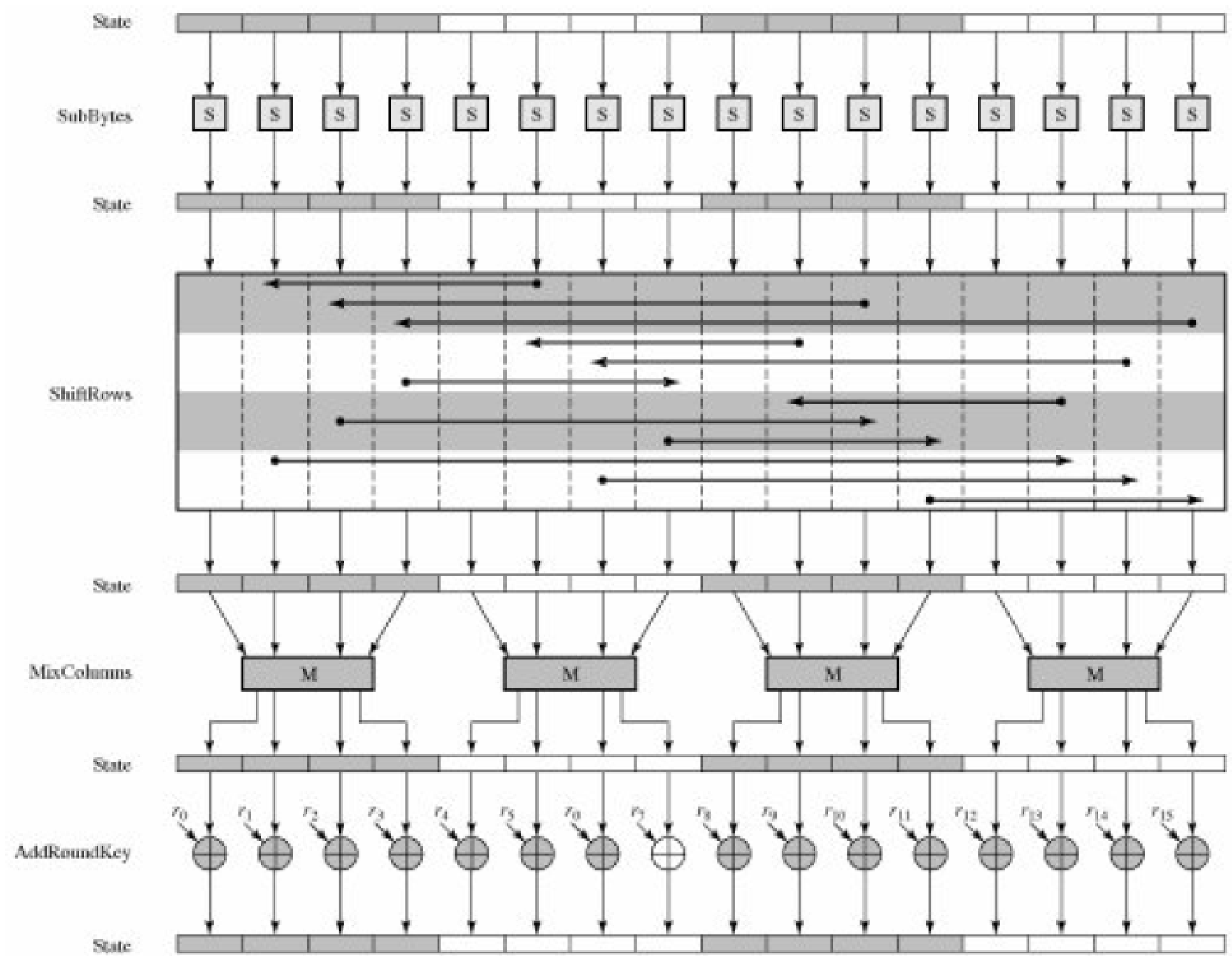
$= 10$



(a) Encryption

(b) Decryption

An Encryption Round



AddRoundKey

- Columnwise operation: the 128-bit state is bitwise XORed with the 128-bit round key

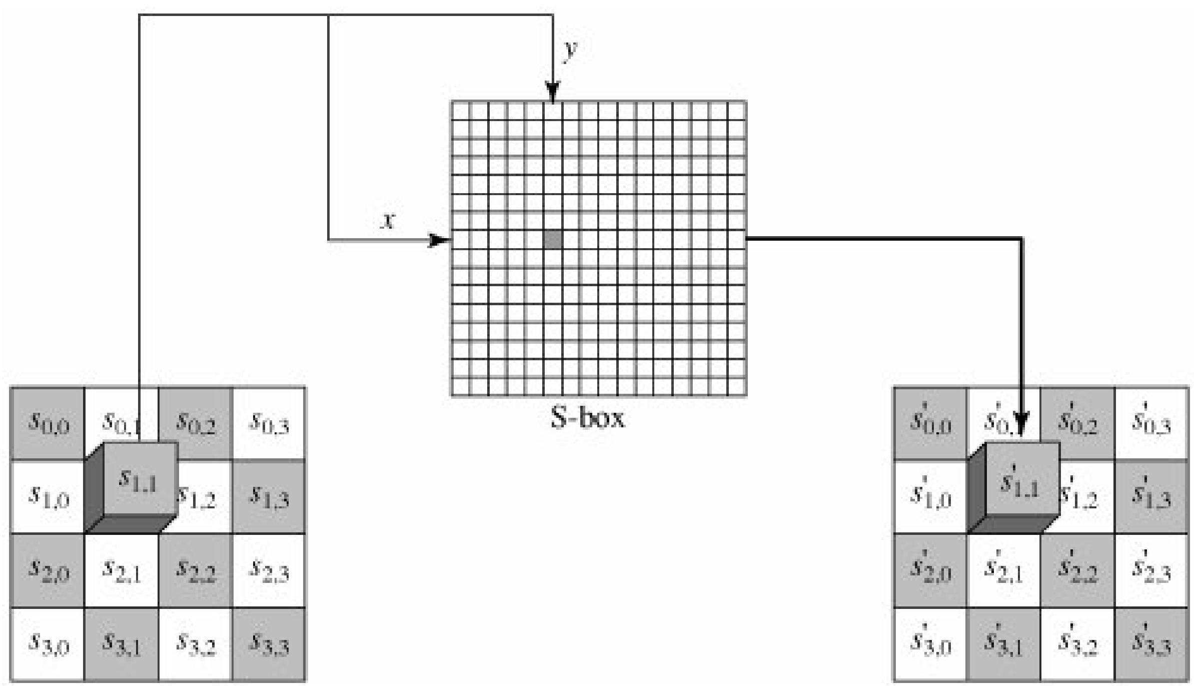
$$
\begin{array}{|c|c|c|c|}\hline 47 & 40 & A3 & 4C \\ \hline 37 & D4 & 70 & 9F \\ \hline 94 & E4 & 3A & 42 \\ \hline ED & A5 & A6 & BC \\ \hline \end{array}
\oplus
\begin{array}{|c|c|c|c|}\hline AC & 19 & 28 & 57 \\ \hline 77 & FA & D1 & 5C \\ \hline 66 & DC & 29 & 00 \\ \hline F3 & 21 & 41 & 6A \\ \hline \end{array}
=
\begin{array}{|c|c|c|c|}\hline EB & 59 & 8B & 1B \\ \hline 40 & 2E & A1 & C3 \\ \hline F2 & 38 & 13 & 42 \\ \hline 1E & 84 & E7 & D2 \\ \hline \end{array}
$$

State Matrix

Round Key Matrix

Substitute Bytes

- SubBytes: table lookup with a 16x16 S-box of bytes
- Substitute byte transformation:

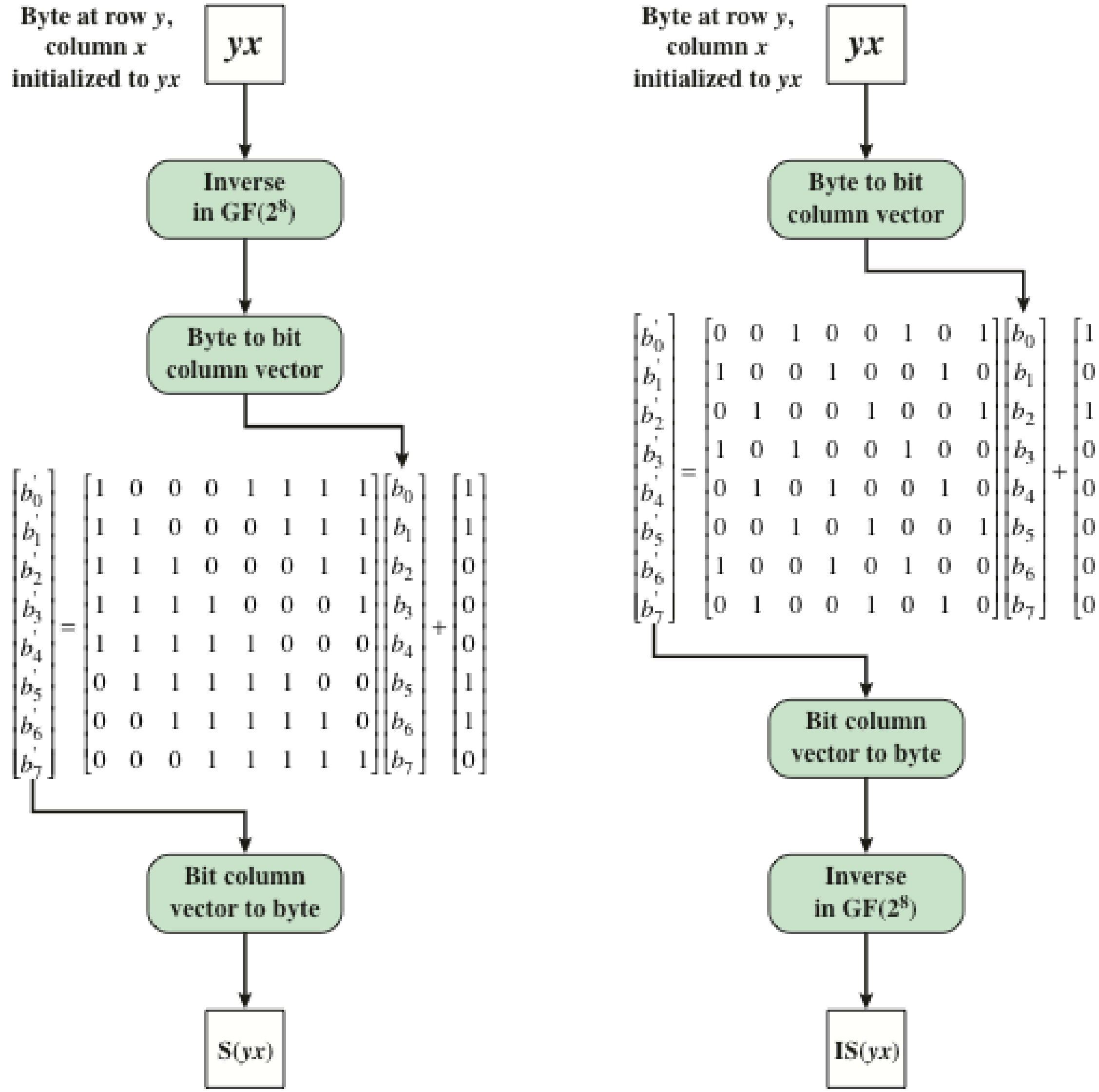


AES S-Box

- Input: 10001011(8b)→ (00111101) (3d)

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	64	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	09	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	0d	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

ByteSub( )
ShiftRows( )
MixColumns( )
AddRoundKey( )



(a) Calculation of byte at row y, column x of S-box

(a) Calculation of byte at row y, column x of IS-box

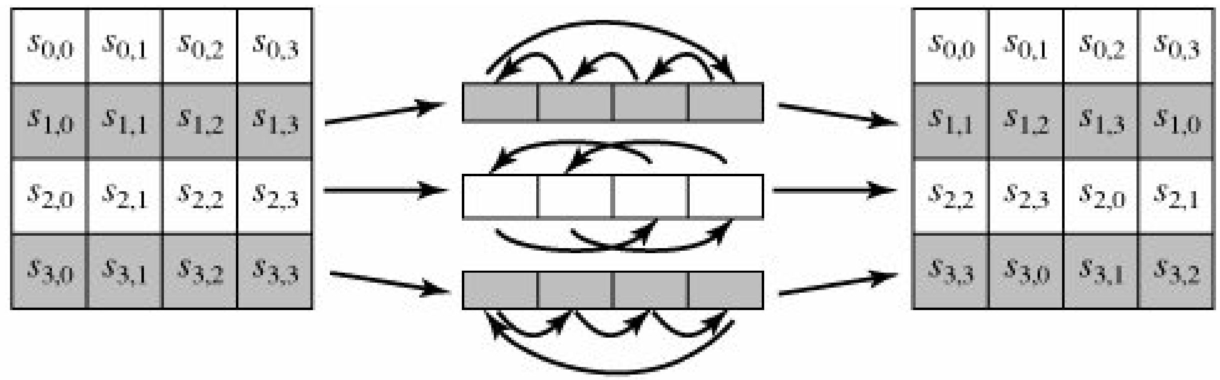
Figure 6.6 Construction of S-Box and IS-Box

S-Box Rationale

- The S-box is designed to be resistant to known cryptanalytic attacks
- The Rijndael developers sought a design that has a low correlation between input bits and output bits and the property that the output is not a linear mathematical function of the input
- The nonlinearity is due to the use of the multiplicative inverse

ShiftRows

- Shift row transformation:



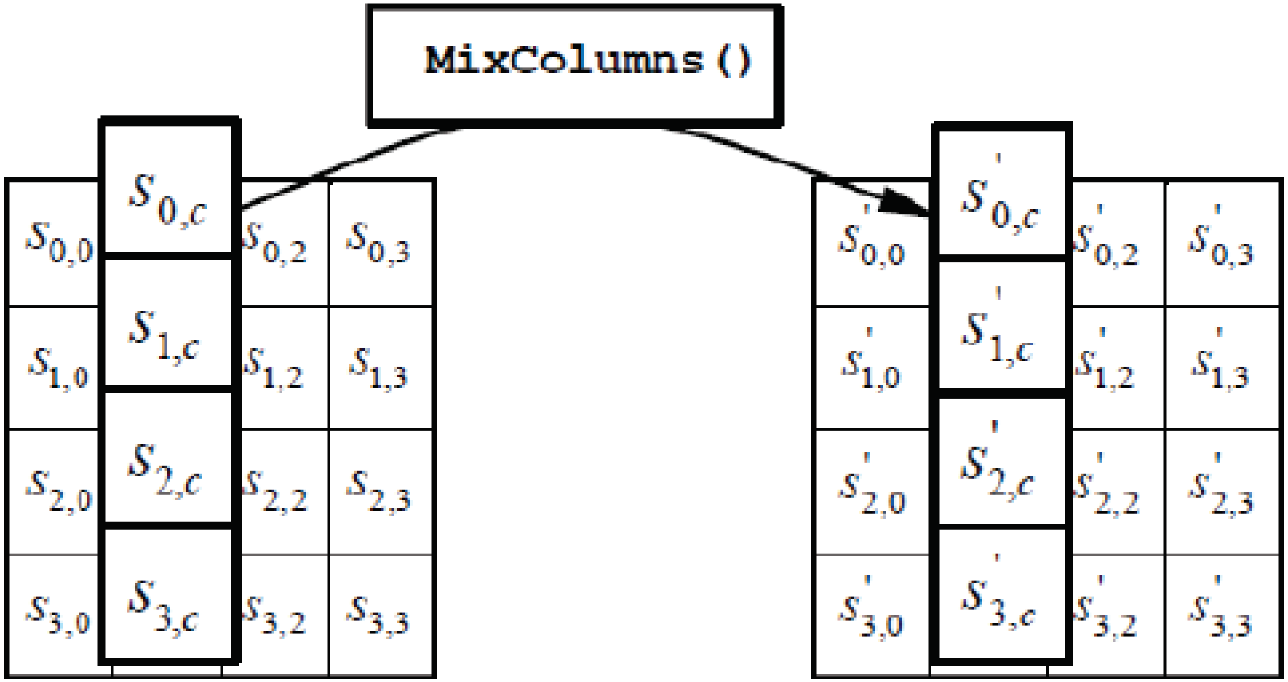
- Example:

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

Mixcolumn



- The MixColumn operation is omitted in the last, i.e., N_rth round

Mathematical Interpretation

- Regard a byte as an element of GF(2^8). Multiply this by a matrix, again with entries in GF(2^8), to produce the output/

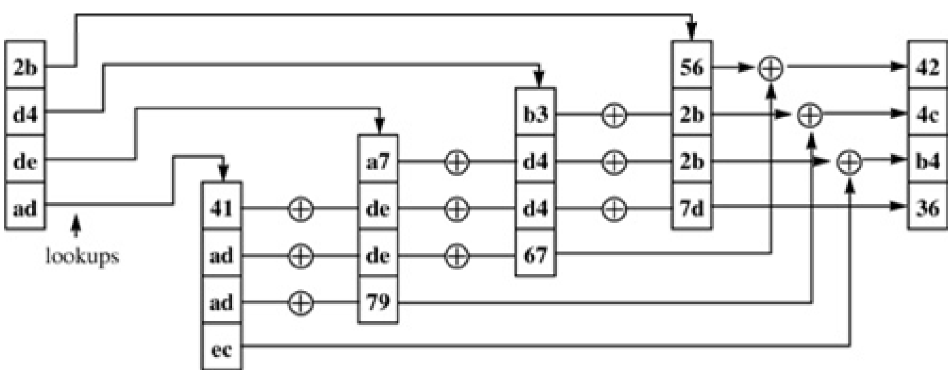
$$\begin{pmatrix} 00000010 & 00000011 & 00000001 & 00000001 \\ 00000001 & 00000010 & 00000011 & 00000001 \\ 00000001 & 00000001 & 00000010 & 00000011 \\ 00000011 & 00000001 & 00000001 & 00000010 \end{pmatrix} \begin{pmatrix} S_{0,0} & S_{0,1} & S_{0,2} & S_{0,3} \\ S_{1,0} & S_{1,1} & S_{1,2} & S_{1,3} \\ S_{2,0} & S_{2,1} & S_{2,2} & S_{2,3} \\ S_{3,0} & S_{3,1} & S_{3,2} & S_{3,3} \end{pmatrix}$$

ByteSub( )
ShiftRows( )
MixColumns( )
AddRoundKey( )

Mix Columns Rationale

- Coefficients of a matrix based on a linear code with maximal distance between code words ensures a good mixing among the bytes of each column
- The mix column transformation combined with the shift row transformation ensures that after a few rounds all output bits depend on all input bits

Mixcolumn Table Lookup



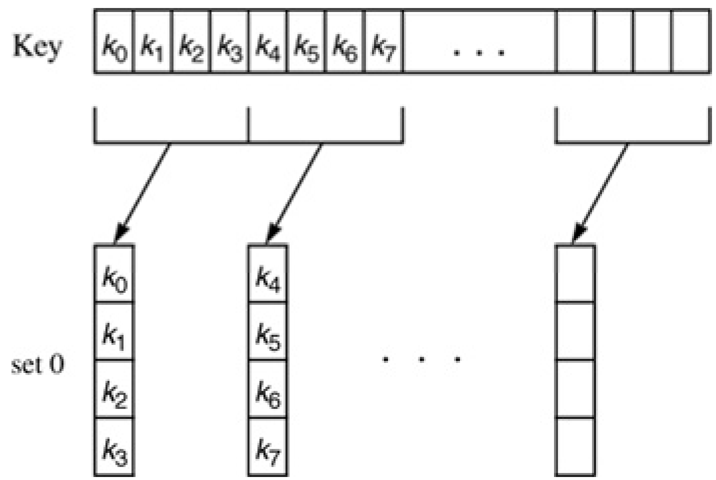
right (low-order) nibble

left (high-order) nibble

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	00 00 00 00	02 01 01 03	04 02 02 06	06 03 03 05	08 04 04 0c	0a 05 05 0f	0c 06 06 0a	0e 07 07 09	10 08 08 18	12 09 09 1b	14 0a 0a 1e	16 0b 0b 1d	18 0c 0c 14	1a 0d 0d 17	1c 0e 0e 12	1e 0f 0f 11
1	20 10 10 30	22 11 11 33	24 12 12 36	26 13 13 35	28 14 14 3c	2a 15 15 3f	2c 16 16 3a	2e 17 17 39	30 18 18 28	32 19 19 2b	34 1a 1a 2e	36 1b 1b 2d	38 1c 1c 24	3a 1d 1d 27	3c 1e 1e 22	3e 1f 1f 21
2	40 20 20 60	42 21 21 63	44 22 22 66	46 23 23 65	48 24 24 6c	4a 25 25 6f	4c 26 26 6a	4e 27 27 69	50 28 28 78	52 29 29 7b	54 2a 2a 7e	56 2b 2b 7d	58 2c 2c 74	5a 2d 2d 77	5c 2e 2e 72	5e 2f 2f 71
3	60 30 30 50	62 31 31 53	64 32 32 56	66 33 33 55	68 34 34 5c	6a 35 35 5f	6c 36 36 5a	6e 37 37 59	70 38 38 48	72 39 39 4b	74 3a 3a 4e	76 3b 3b 4d	78 3c 3c 44	7a 3d 3d 47	7c 3e 3e 42	7e 3f 3f 41
4	80 40 40 c0	82 41 41 c3	84 42 42 c6	86 43 43 c5	88 44 44 cc	8a 45 45 cf	8c 46 46 ca	8e 47 47 c9	90 48 48 d8	92 49 49 db	94 4a 4a de	96 4b 4b dd	98 4c 4c d4	9a 4d 4d d7	9c 4e 4e d2	9e 4f 4f d1
5	a0 50 50 f0	a2 51 51 f3	a4 52 52 f6	a6 53 53 f5	a8 54 54 fc	aa 55 55 ff	ac 56 56 fa	ae 57 57 f9	b0 58 58 e8	b2 59 59 eb	b4 5a 5a ee	b6 5b 5b ed	b8 5c 5c e4	ba 5d 5d e7	bc 5e 5e e2	be 5f 5f e1
6	c0 60 60 a0	c2 61 61 a3	c4 62 62 a6	c6 63 63 a5	c8 64 64 ac	ca 65 65 af	cc 66 66 aa	ce 67 67 a9	d0 68 68 b8	d2 69 69 bb	d4 6a 6a be	d6 6b 6b bd	d8 6c 6c b4	da 6d 6d b7	dc 6e 6e b2	de 6f 6f b1
7	e0 70 70 90	e2 71 71 93	e4 72 72 96	e6 73 73 95	e8 74 74 9c	ea 75 75 9f	ec 76 76 9a	ee 77 77 99	f0 78 78 88	f2 79 79 8b	f4 7a 7a 8e	f6 7b 7b 8d	f8 7c 7c 84	fa 7d 7d 87	fc 7e 7e 82	fe 7f 7f 81
8	1b 80 80 9b	19 81 81 98	1f 82 82 9d	1d 83 83 9e	13 84 84 97	11 85 85 94	17 86 86 91	15 87 87 92	0b 88 88 83	09 89 89 80	0f 8a 8a 85	0d 8b 8b 86	03 8c 8c 8f	01 8d 8d 8c	07 8e 8e 89	05 8f 8f 8a
9	3b 90 90 ab	39 91 91 a8	3f 92 92 ad	3d 93 93 ae	33 94 94 a7	31 95 95 a4	37 96 96 a1	35 97 97 a2	2b 98 98 b3	29 99 99 b0	2f 9a 9a b5	2d 9b 9b b6	23 9c 9c bf	21 9d 9d bc	27 9e 9e b9	25 9f 9f ba
a	5b a0 a0 fb	59 a1 a1 f8	5f a2 a2 fd	5d a3 a3 fe	53 a4 a4 f7	51 a5 a5 f4	57 a6 a6 f1	55 a7 a7 f2	4b a8 a8 e3	49 a9 a9 e0	4f aa aa e5	4d ab ab e6	43 ac ac ef	41 ad ad ec	47 ae ae e9	45 af af ea
b	7b b0 b0 cb	79 b1 b1 c8	7f b2 b2 cd	7d b3 b3 ce	73 b4 b4 c7	71 b5 b5 c4	77 b6 b6 c1	75 b7 b7 c2	6b b8 b8 d3	69 b9 b9 d0	6f ba ba d5	6d bb bb d6	63 bc bc df	61 bd bd dc	67 be be d9	65 bf bf da
c	9b c0 c0 5b	99 c1 c1 58	9f c2 c2 5d	9d c3 c3 5e	93 c4 c4 57	91 c5 c5 54	97 c6 c6 51	95 c7 c7 52	8b c8 c8 43	89 c9 c9 40	8f ca ca 45	8d cb cb 46	83 cc cc 4f	81 cd cd 4c	87 ce ce 49	85 cf cf 4a
d	bb d0 d0 6b	b9 d1 d1 68	bf d2 d2 6d	bd d3 d3 6e	b3 d4 d4 67	b1 d5 d5 64	b7 d6 d6 61	b5 d7 d7 62	ab d8 d8 73	a9 d9 d9 70	af da da 75	ad db db 76	a3 dc dc 7f	a1 dd dd 7c	a7 de de 79	a5 df df 7a
e	db e0 e0 3b	d9 e1 e1 38	df e2 e2 3d	dd e3 e3 3e	d3 e4 e4 37	d1 e5 e5 34	d7 e6 e6 31	d5 e7 e7 32	cb e8 e8 23	c9 e9 e9 20	cf ea ea 25	cd eb eb 26	c3 ec ec 2f	c1 ed ed 2c	c7 ee ee 29	c5 ef ef 2a
f	fb f0 f0 0b	f9 f1 f1 08	ff f2 f2 0d	fd f3 f3 0e	f3 f4 f4 07	f1 f5 f5 04	f7 f6 f6 01	f5 f7 f7 02	eb f8 f8 13	e9 f9 f9 10	ef fa fa 15	ed fb fb 16	e3 fc fc 1f	e1 fd fd 1c	e7 fe fe 19	e5 ff ff 1a

Key Expansion

- 128-bit or 4 cols. of 4-byte key is expanded to 44 cols.
- In general, needs $(N_r+1)N_b$ columns of key



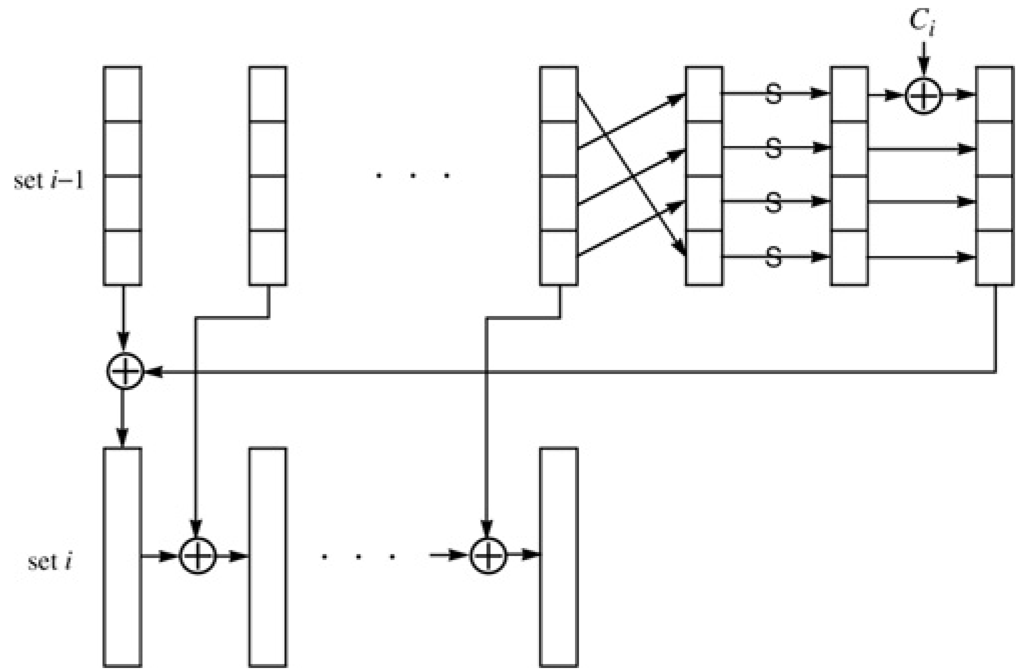


Figure 3-31. Rijndael key-expansion constants C_i

i = 1 thru 10:	1	2	4	8	10	20	40	80	1b	36
i = 11 thru 20:	6c	d8	ab	4d	9a	2f	5e	bc	63	c6
i = 21 thru 30:	97	35	6a	d4	b3	7d	fa	ef	c5	(91)

Key Expansion (I)

- The original key has 128 bits, which is arranged into a 4 by 4 matrix of bytes.
- This matrix is expanded by adding 40 more columns.
- Label the first four columns W(0), W(1), W(2), W(3).
- The new columns are generated recursively.
  - If i is not a multiple of 4

    $W(i) = W(i-4) \oplus W(i-1)$
  - If i is multiple of 4

    $W(i) = W(i-4) \oplus T(W(i-1))$

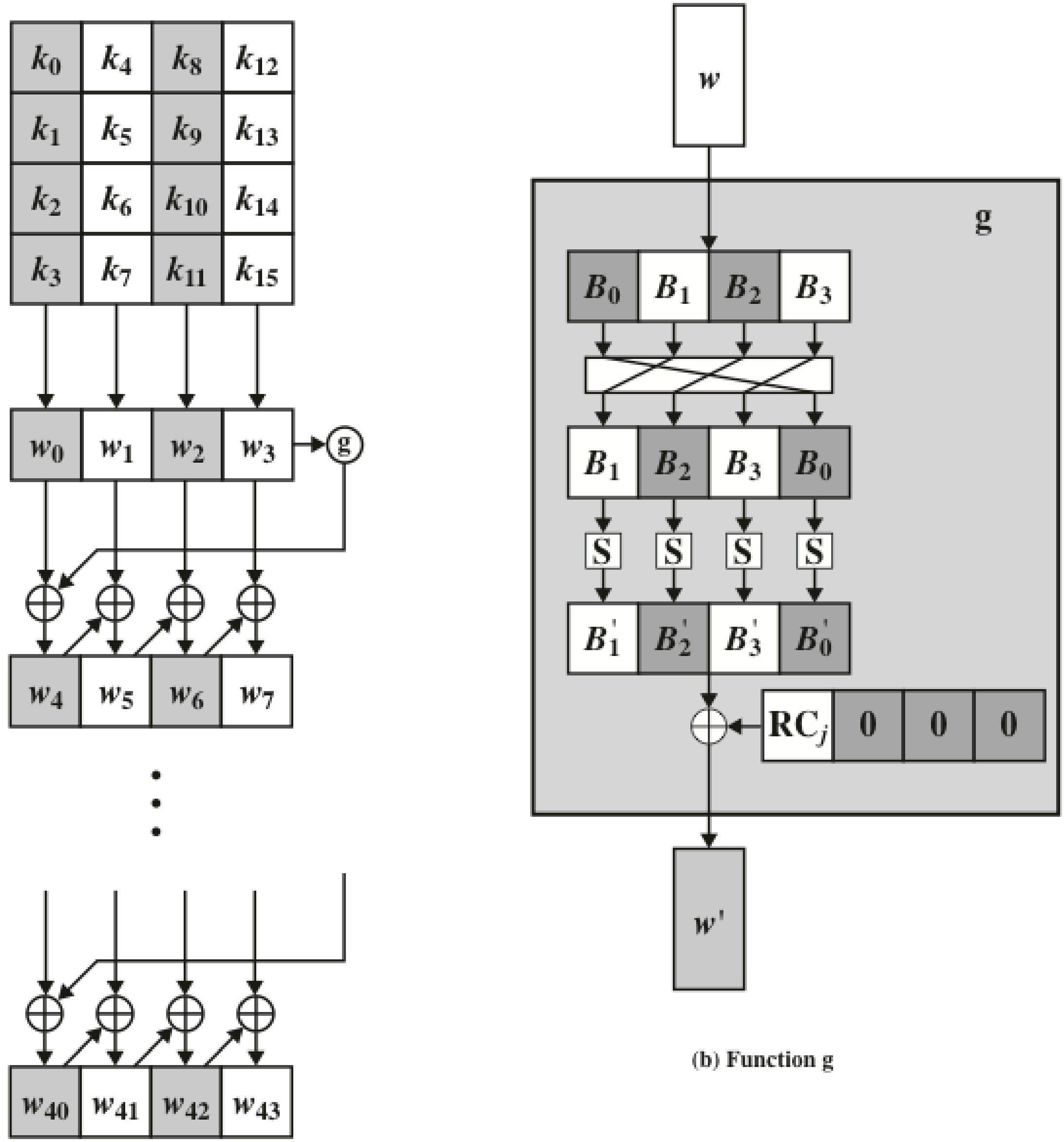
$$W(4) = W(0) \oplus T(W(3))$$
$$W(5) = W(1) \oplus W(4)$$
$$W(6) = W(2) \oplus W(5)$$
$$W(7) = W(3) \oplus W(6)$$

Key Expansion (II)

- T(W(i-1)) is the transform of W(i-1) obtained as follows.
  - Let element of column W(i-1) be *a,b,c,d*
  - Shift these cyclically to obtain *b,c,d,a*
  - Replace each of these bytes with corresponding element in the S-box, and get 4 bytes *e,f,g,h*
  - Compute the round constant in GF(2^8)

    $$r(i) = 00000010^{(i-4)/4}$$
  - Then, T(W(i-1)) is the column vector

    $$(e \oplus r(i), f, g, h)$$
- The round key for the ith round consists of the columns: W(4i), W(4i+1), W(4i+2), W(4i+3)



(b) Function g

(a) Overall algorithm

Figure 6.9 AES Key Expansion

Summary: Four Stages

One permutation and three substitutions

- Substitute bytes: uses an S-box to perform a byte-by-byte substitution of the block
- ShiftRows: a simple permutation
- MixColumns: a substitution that makes use of arithmetic over GF(2^8)
- AddRoundKey: a simple bitwise XOR of the current block with a portion of the expanded key
- Each stage is easily reversible—decryption

Rijndael Cryptanalysis

- Resistant to linear and differential cryptanalysis
- Academic break on weaker version of the cipher, 9 rounds