Secret Key Cryptography

Raj Jain
Washington University in Saint Louis
Saint Louis, MO 63130
Jain@cse.wustl.edu

Audio/Video recordings of this lecture are available at:

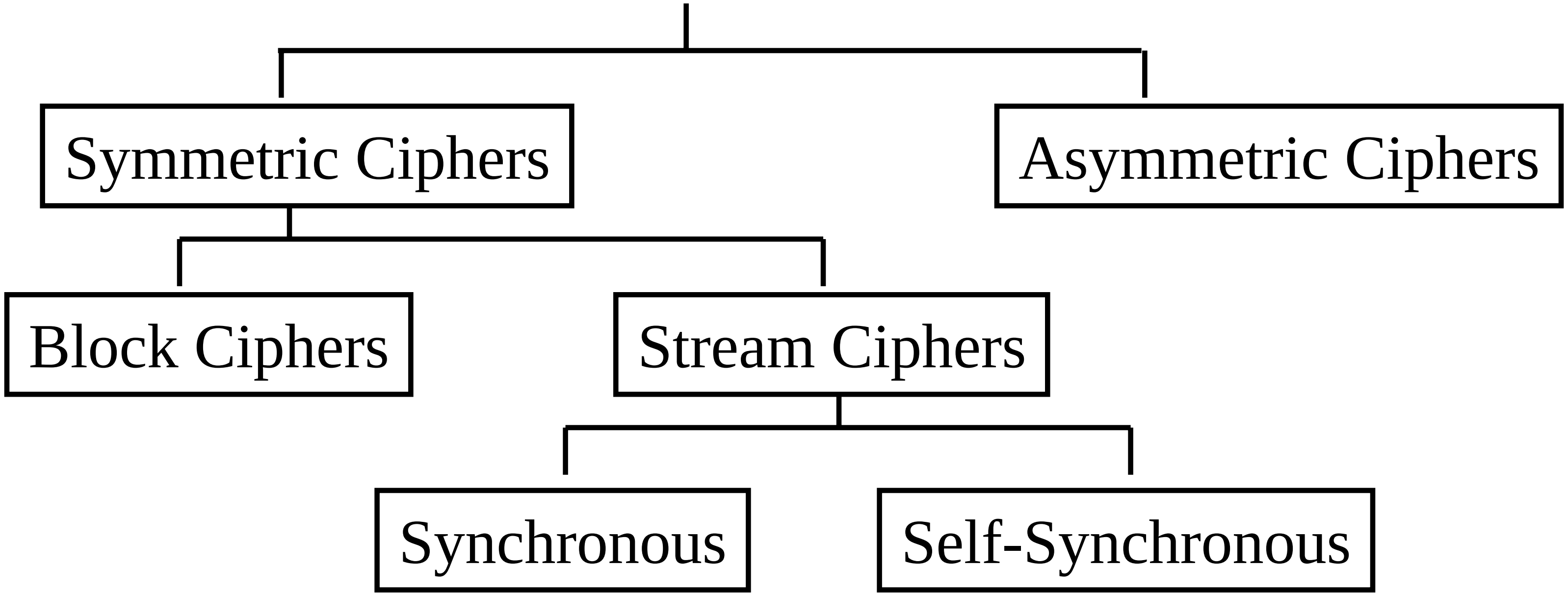
http://www.cse.wustl.edu/~jain/cse571-09/

Overview

1. Data Encryption Standard (DES)
2. International Data Encryption Algorithm (IDEA)
3. Advanced Encryption Standard (AES)
4. Ron’s Cipher 4 (RC4)

Ref: Chapter 3 of the textbook.

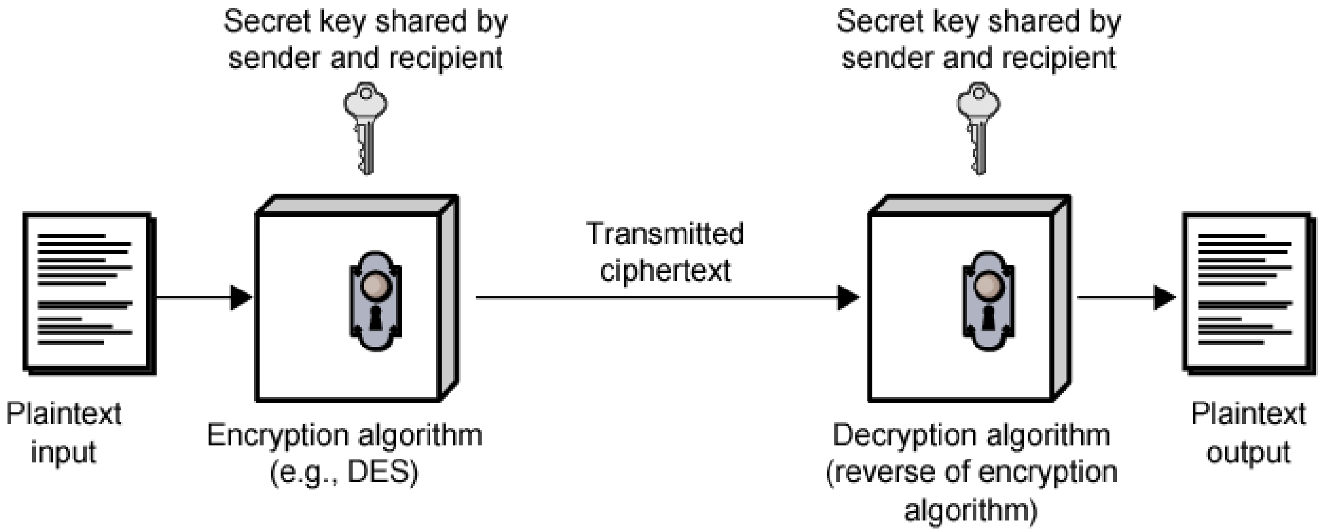
Encryption Schemes



- Symmetric = 1 Key/2 users = Secret Key
- Asymmetric = Public Key = Public and Private Keys
- Block: Message broken in to fixed size blocks
- Synchronous: Key stream depends on the key and IV
- Self-synchronous: Key stream depends on key, IV, and previous cipher text

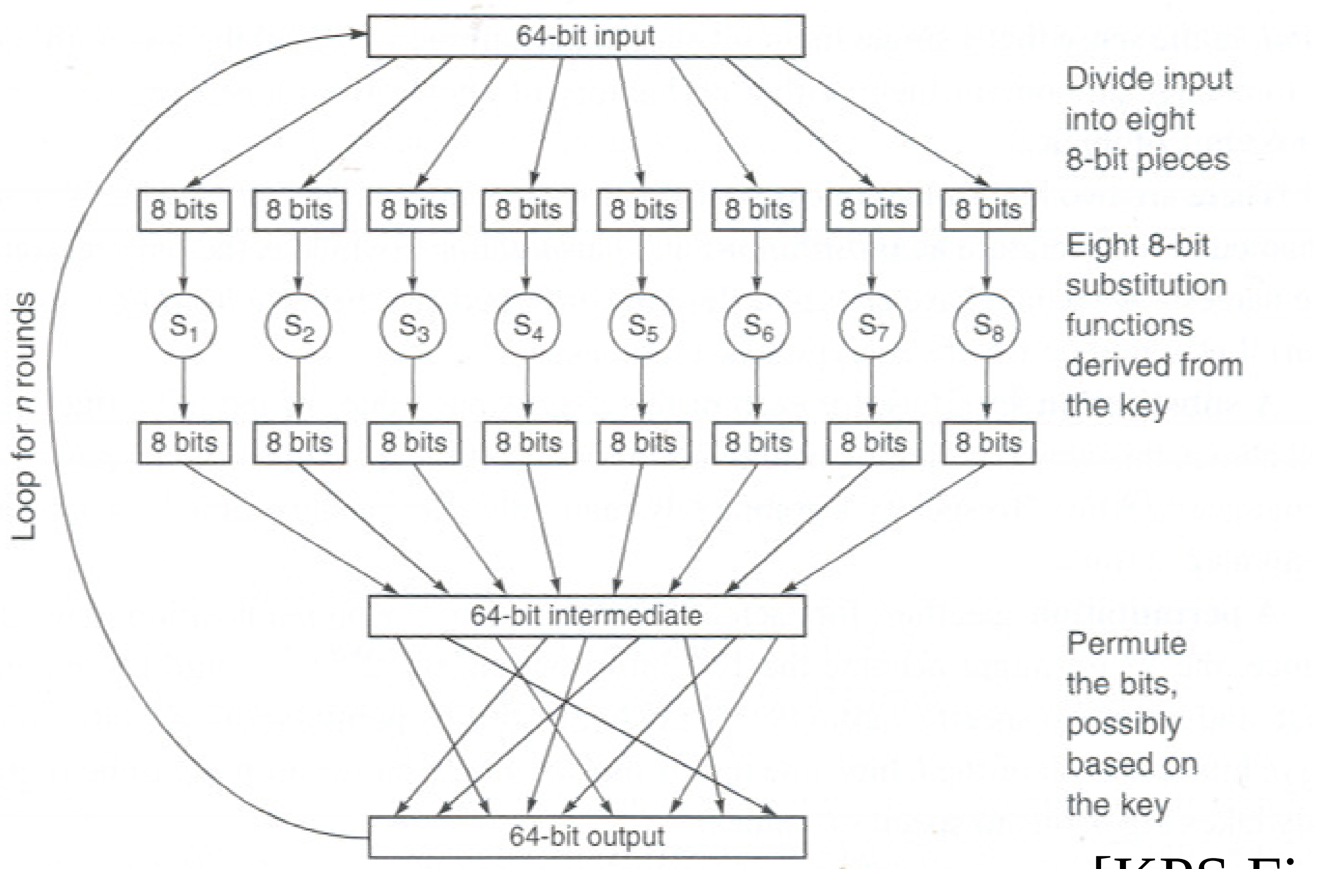
Secret Key Encryption

- Also known as symmetric encryption
- Encrypted_Message = Encrypt(Key, Message)
- Message = Decrypt(Key, Encrypted_Message)
- Example: Encrypt = division
- 433 = 48 R 1 (using divisor of 9)


Secret key shared by sender and recipient
Secret key shared by sender and recipient
Transmitted ciphertext
Plaintext input
Encryption algorithm (e.g., DES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Secret Key Cryptography

- Block Encryption



[KPS Fig 3-1]

Block Encryption (Cont)

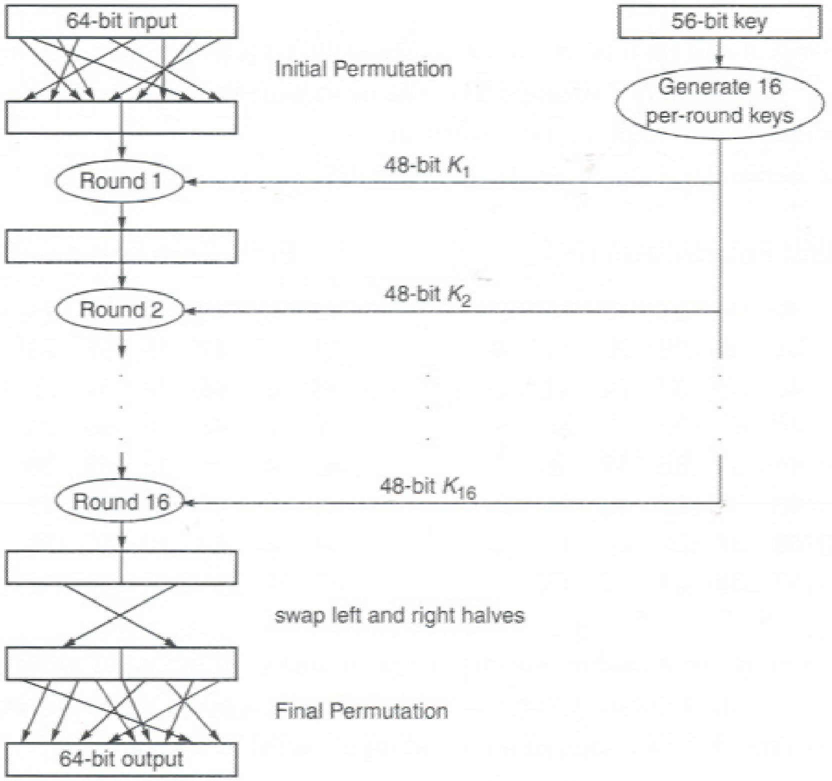
- Short block length ⇒ tabular attack
- 64-bit block
- Transformations:
  - Substitution: replace k-bit input blocks with k-bit output blocks
  - Permutation: move input bits around.
    1 → 13, 2 → 61, etc.
- Round: Substitution round followed by permutation round and so on. Diffusion + Confusion.

Data Encryption Standard (DES)

- Published by National Bureau of Standards in 1977
- For commercial and *unclassified* government applications
- 8 octet (64 bit) key.
  Each octet with 1 odd parity bit ⇒ 56-bit key
- Efficient hardware implementation
- Used in most financial transactions
- Computing power goes up 1 bit every 2 years
- 56-bit was secure in 1977 but is not secure today
- Now we use DES three times ⇒ Triple DES = 3DES

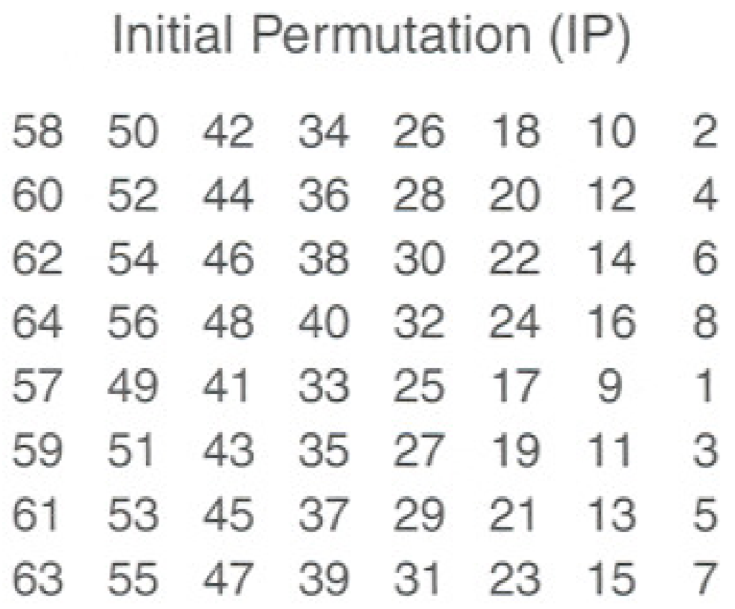
DES Steps

- Total 18 steps: Initial permutation, 16 mangler rounds, Inverse of initial permutation



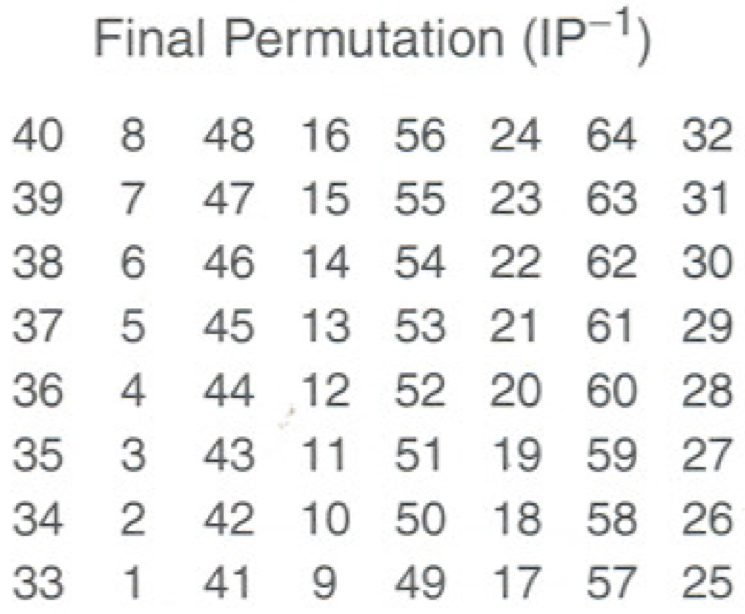
[KPS Fig 3-2]

Initial and Final Permutation



Initial Permutation (IP)

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

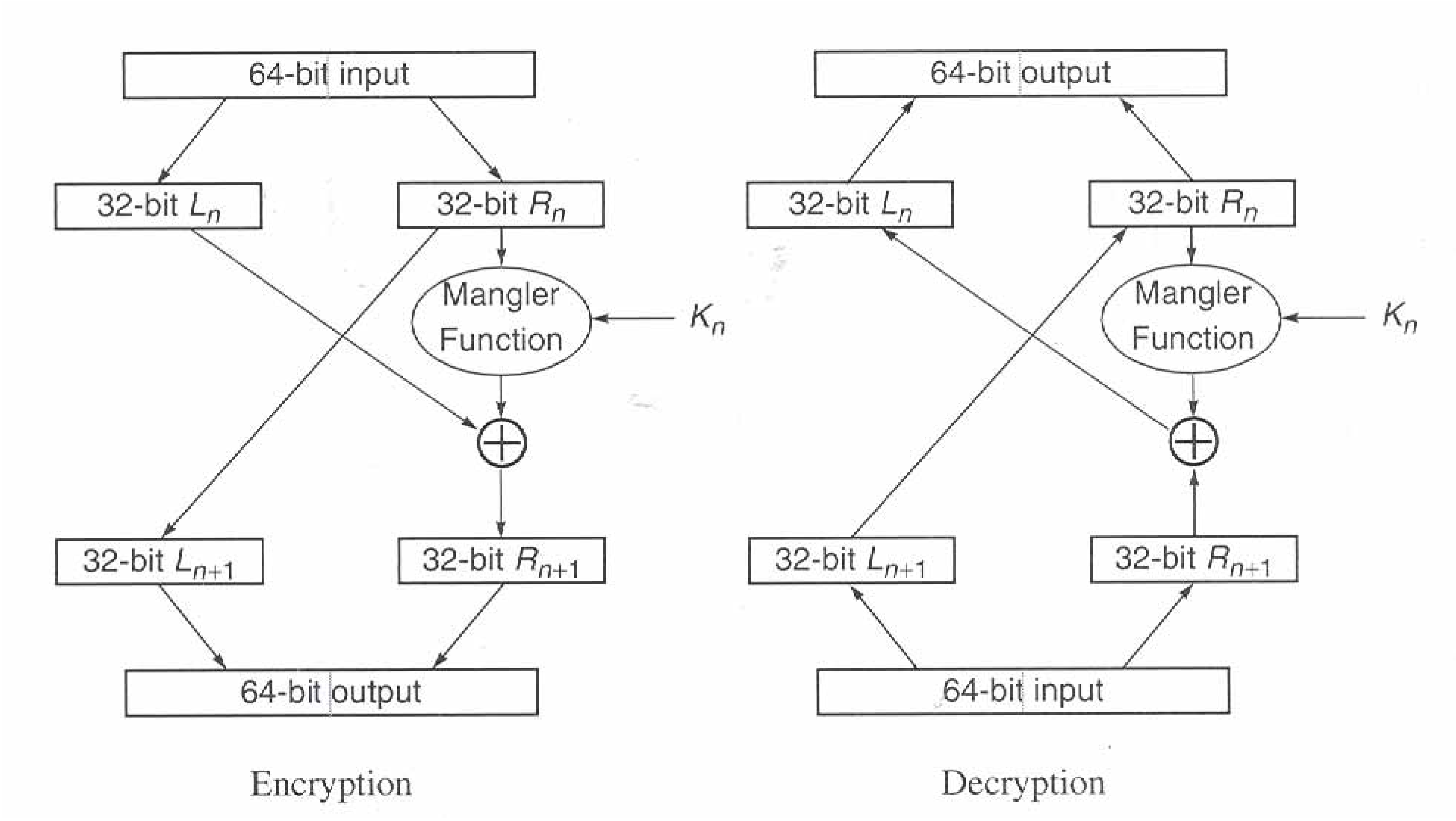


Final Permutation (IP^{-1})

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

- Input bit 58 goes to output bit 1
  Input bit 50 goes to output bit 2, …

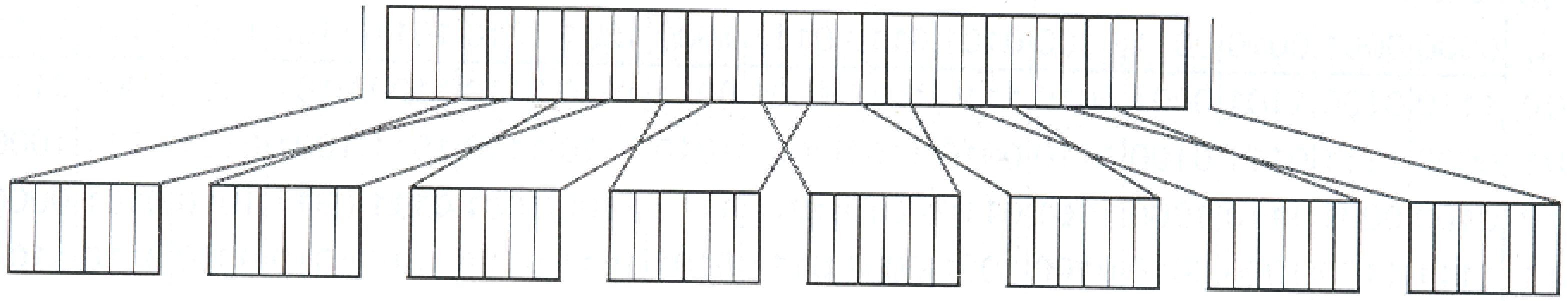
DES Round



[KPS Fig 3-6]

Mangler Function

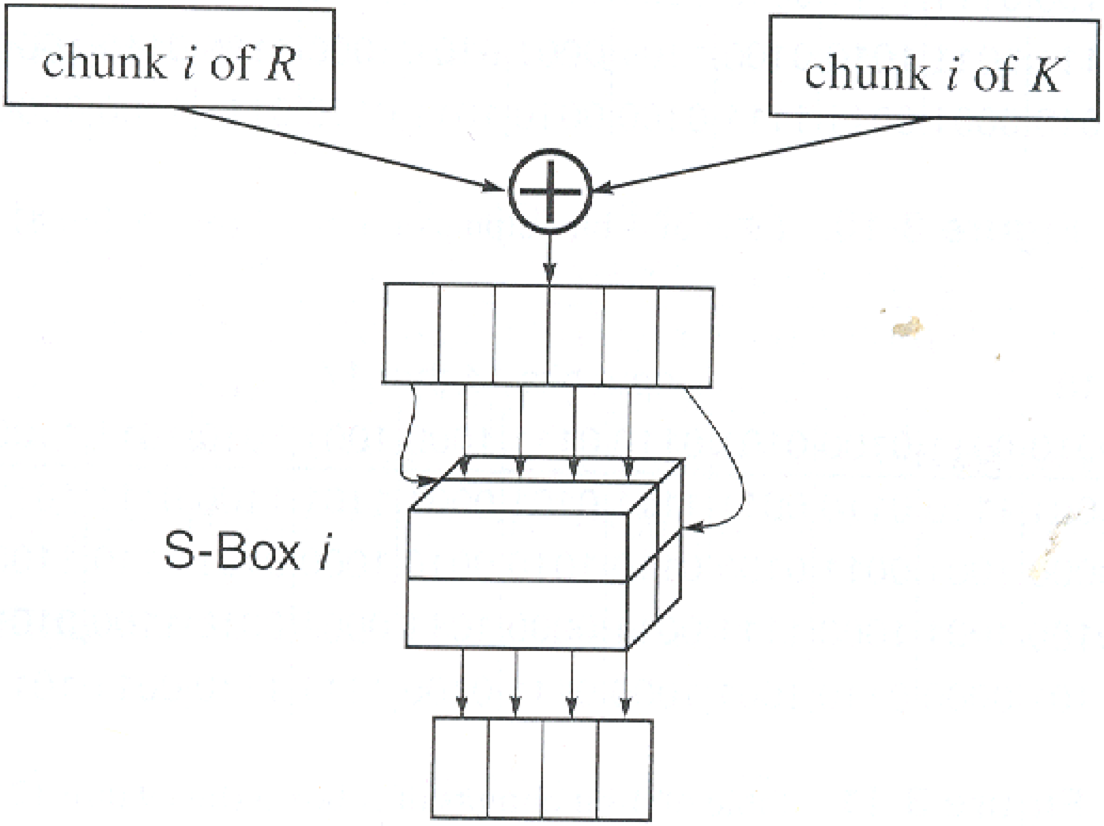
- 32-bit R_n and 48 bit K_n
- 32 bit $R_n = 8 \times 4$ bits $\Rightarrow 8 \times 6$ bits
- 48 bit key = 8×6 bits



[KPS Fig 3-7]

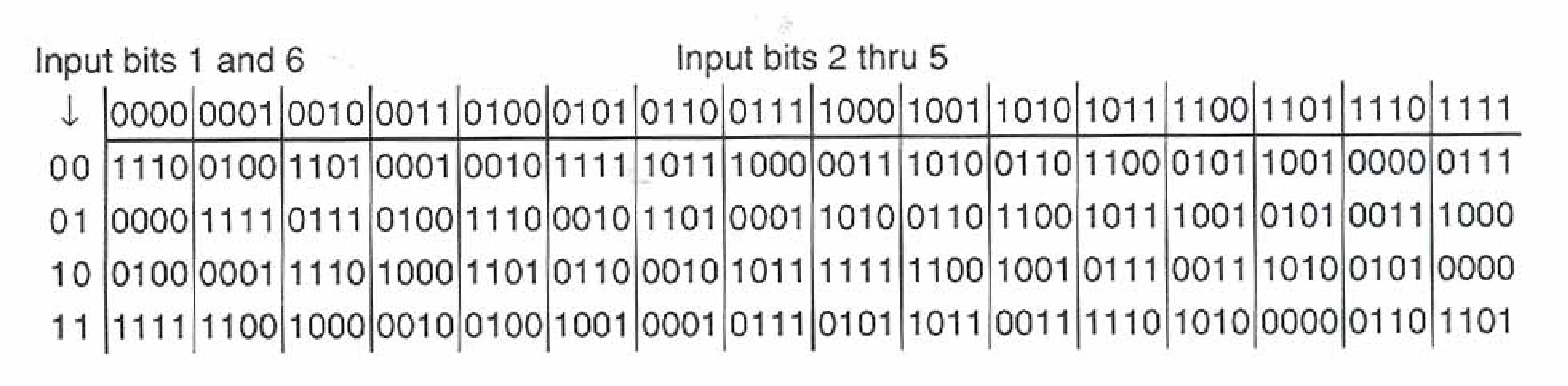
DES Substitution Box

- Xor and S-Box



DES S-Box (Cont)

- S-Box



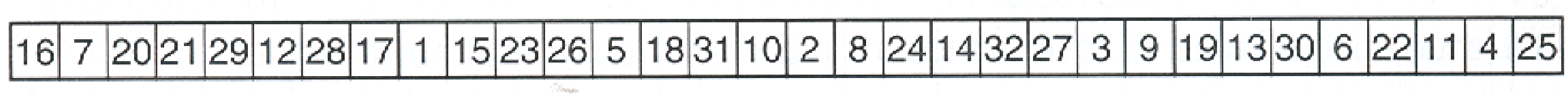
Input bits 1 and 6

Input bits 2 thru 5

↓	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	1110	0100	1101	0001	0010	1111	1011	1000	0011	1010	0110	1100	0101	1001	0000	0111
01	0000	1111	0111	0100	1110	0010	1101	0001	1010	0110	1100	1011	1001	0101	0011	1000
10	0100	0001	1110	1000	1101	0110	0010	1011	1111	1100	1001	0111	0011	1010	0101	0000
11	1111	1100	1000	0010	0100	1001	0001	0111	0101	1011	0011	1110	1010	0000	0110	1101

[KPS Fig 3-9]

- 3. Permutation



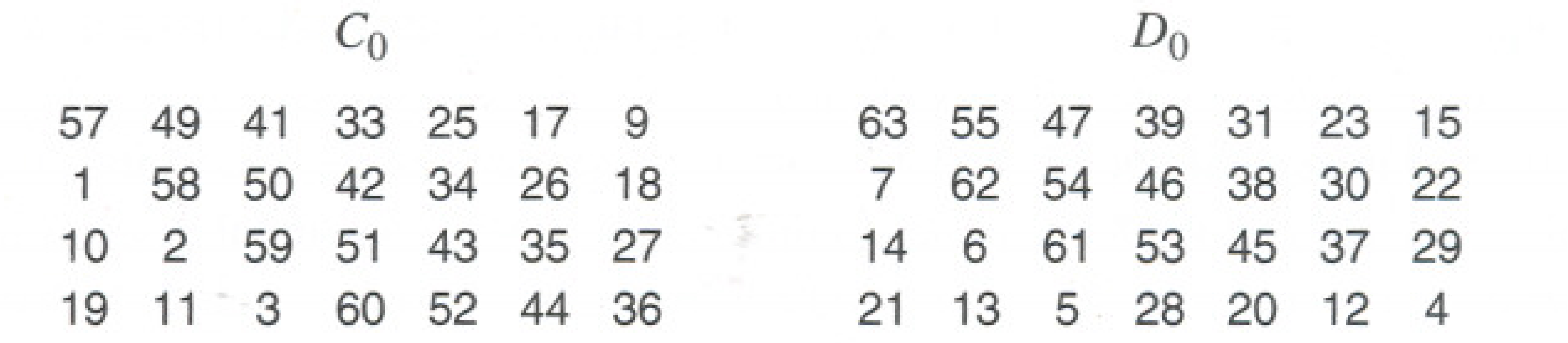
16	7	20	21	29	12	28	17	1	15	23	26	5	18	31	10	2	8	24	14	32	27	3	9	19	13	30	6	22	11	4	25

16th input bit is the 1st output bit, …

[KPS Fig 3-17]

Generation of Per-Round Keys

- Divide in to 28-bit halves
- Initial permutation:

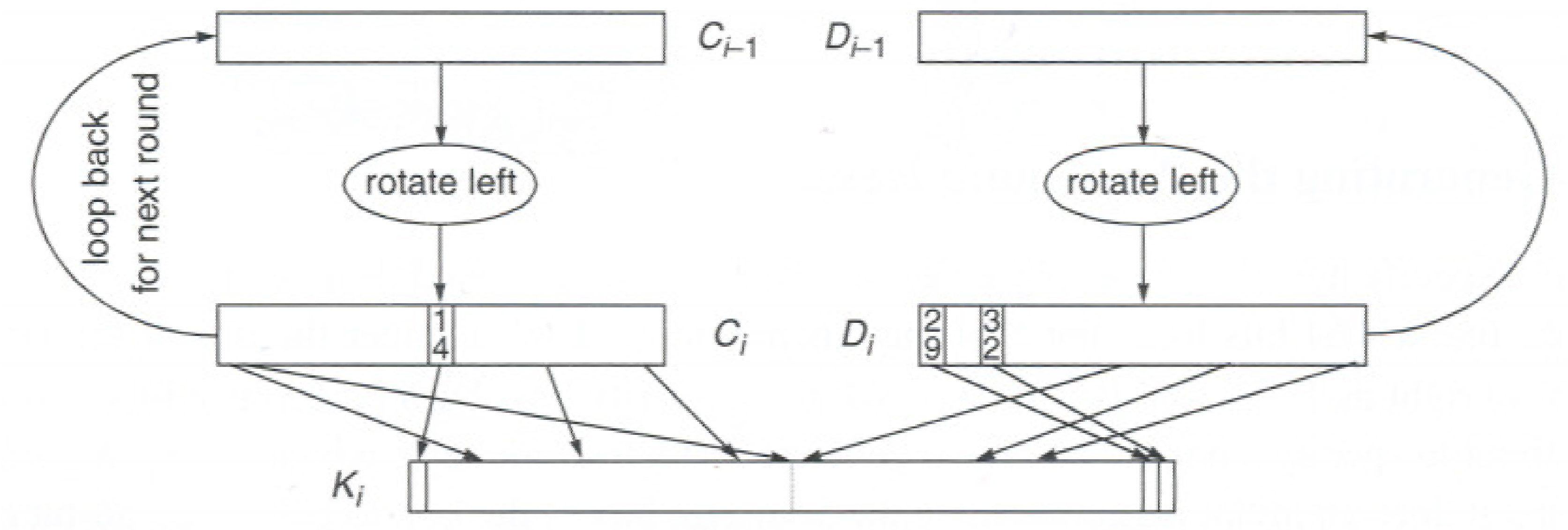


			C_0							D_0			
57	49	41	33	25	17	9	63	55	47	39	31	23	15
1	58	50	42	34	26	18	7	62	54	46	38	30	22
10	2	59	51	43	35	27	14	6	61	53	45	37	29
19	11	3	60	52	44	36	21	13	5	28	20	12	4

57th bit of key becomes the 1st bit of output
49th bit of key becomes the 2nd bit of output, …

Generation of Per-Round Keys (Cont)

- Rotate left by 1 or 2 bits:
  In rounds 1, 2, 9, and 16 rotate 1-bit left,
  in other rounds rotate 2-bit left

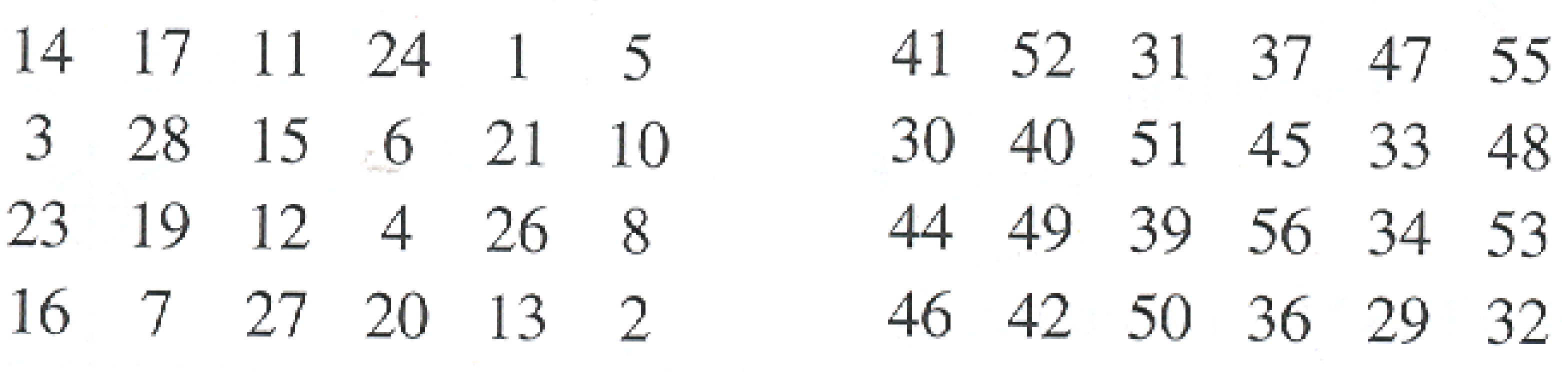


[KPS Fig 3-5]

Generation of Per-Round Keys (Cont)

- Final permutation: 4 bits are discarded from each half ⇒ 24 bits

  Left-Half   Right-Half



14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2

41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

  14th input bit becomes the 1st output bit, …

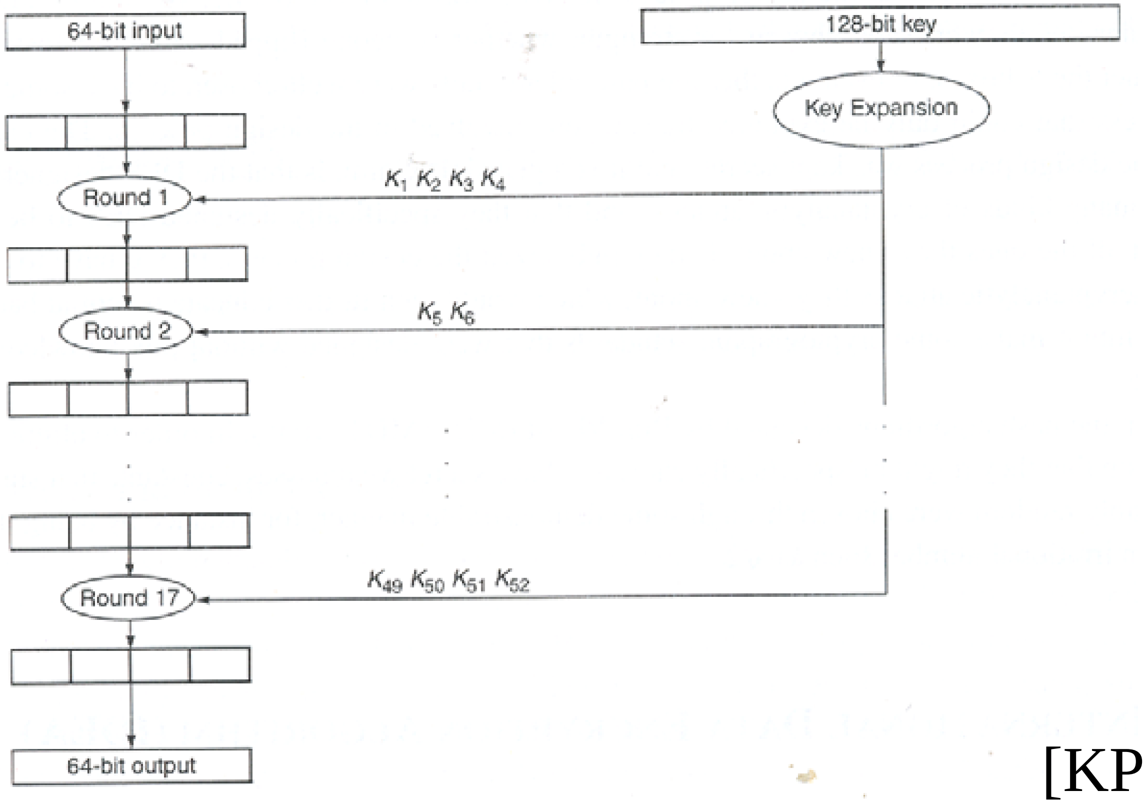
- Bits 9, 18, 22, 25 of left half are discarded
  Bits 35, 38, 53, and 54 of right half are discarded.

DES Decryption

- Identical to Encryption
- Keys are used in reverse order

International Data Encryption Algorithm

- IDEA. Designed for software implementation
- Encryption and Decryption are identical as in DES



[KPS Fig 3-18]

International Data Encryption Algorithm

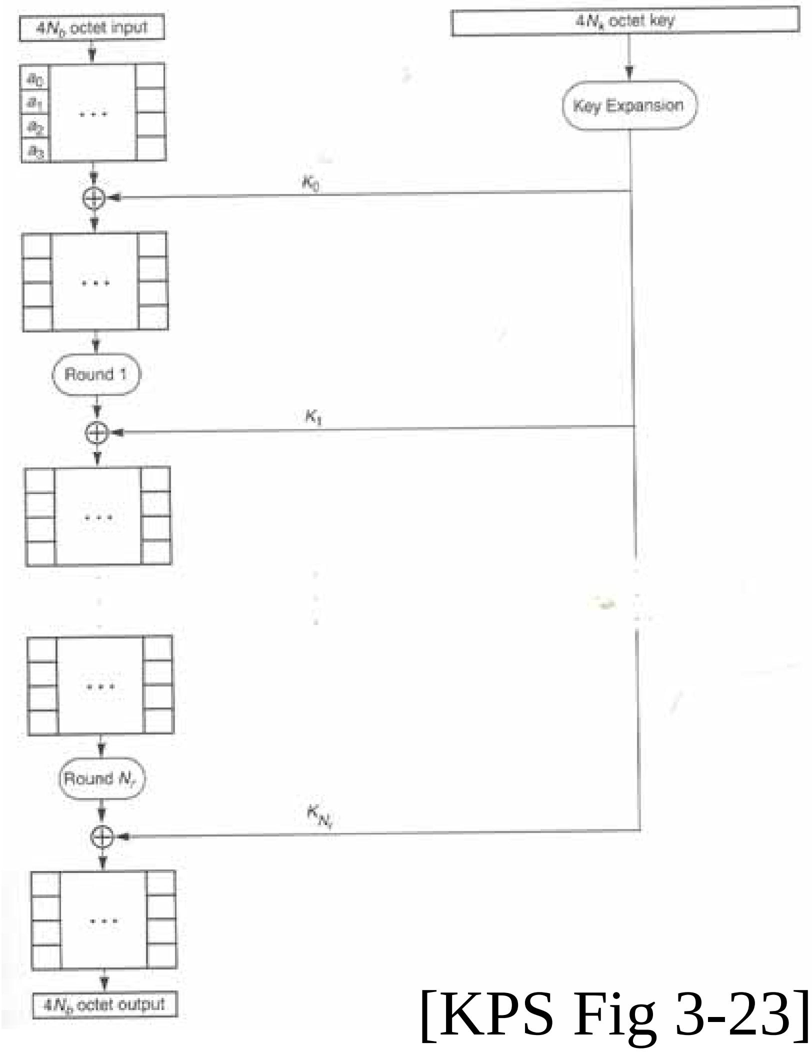
- 128-bit key is converted to 52 16-bit keys
- Inverse of the encryption key is used for decryption in the reverse order
- Has patent protection

Advanced Encryption Standard (AES)

- Published by NIST in Nov 2001
- Based on a competition won by Rijmen and Daemen (Rijndael)
- 22 submissions, 7 did not satisfy all requirements
  15 submissions 5 finalists: MARS, RC6, Rijndael, Serpent, Twofish. Winner: Rijndael.
- Rijndael allows many block sizes and key sizes
- AES restricts it to:
  - Block Size: 128 bits
  - Key sizes: 128, 192, 256 (AES-128, AES-192, AES-256)

Basic Structure of Rijndael

- Number of Rounds
  $N_r = 6 + \max\{N_b, N_k\}$
- N_b = 32-bit words in the the block
- N_k = 32-bit words in key
- 4 rows × N_b columns ($N_b = 4$ for AES)
- AES-128 with 128-bit key:
  - $N_b = 4$
  - $N_k = 4$
  - $N_r = 10$

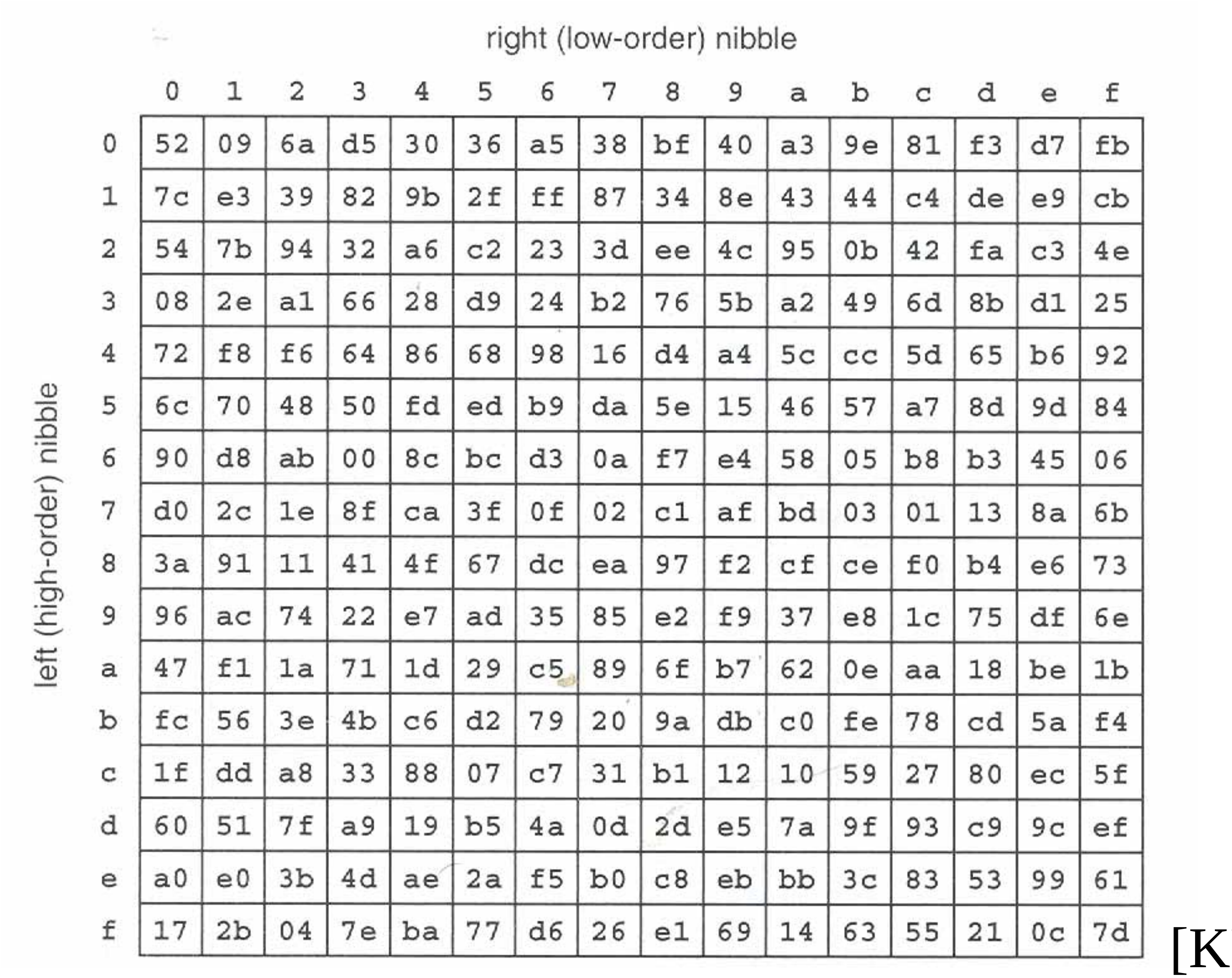


[KPS Fig 3-23]

AES Primitive Operations

- Xor
- Substitution box
- Rotation: column or row
- MixColumn:
  Replace 32-bit word with another 32-bit word

Rijndael S-Box



right (low-order) nibble

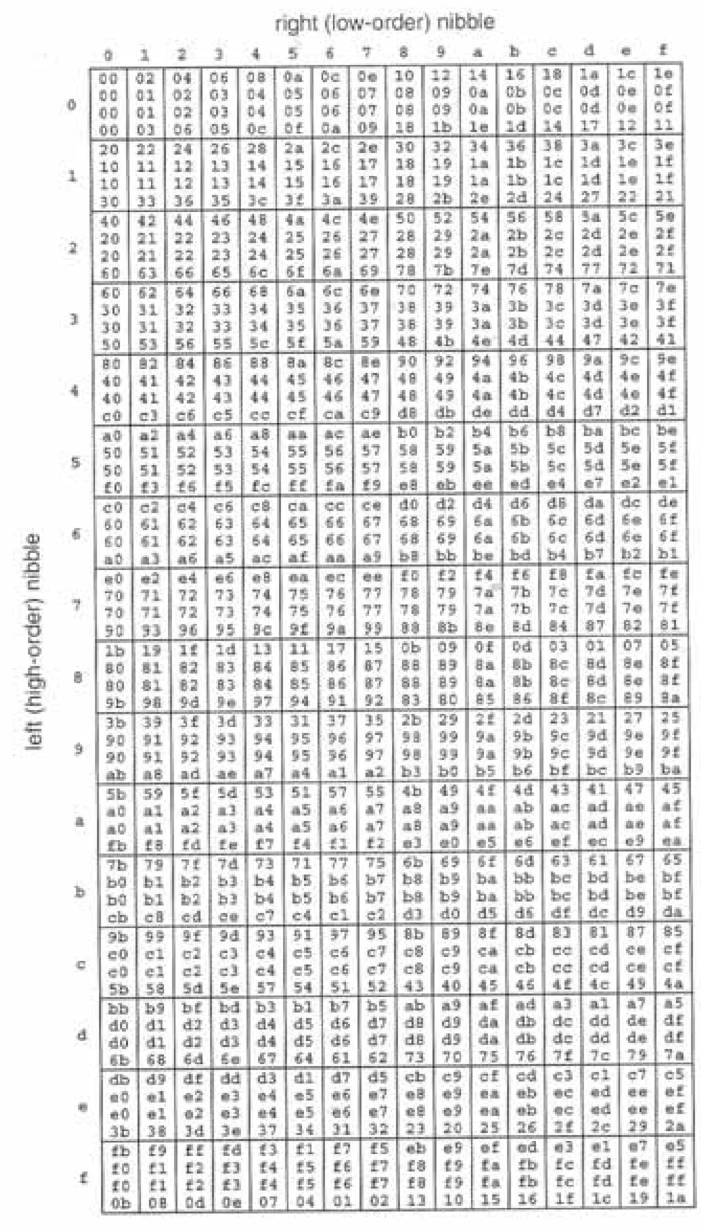
left (high-order) nibble

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

[KPS Fig 3-27]

MixColumn

- 4 Input octets are used as an index to retrieve a column from the table



right (low-order) nibble

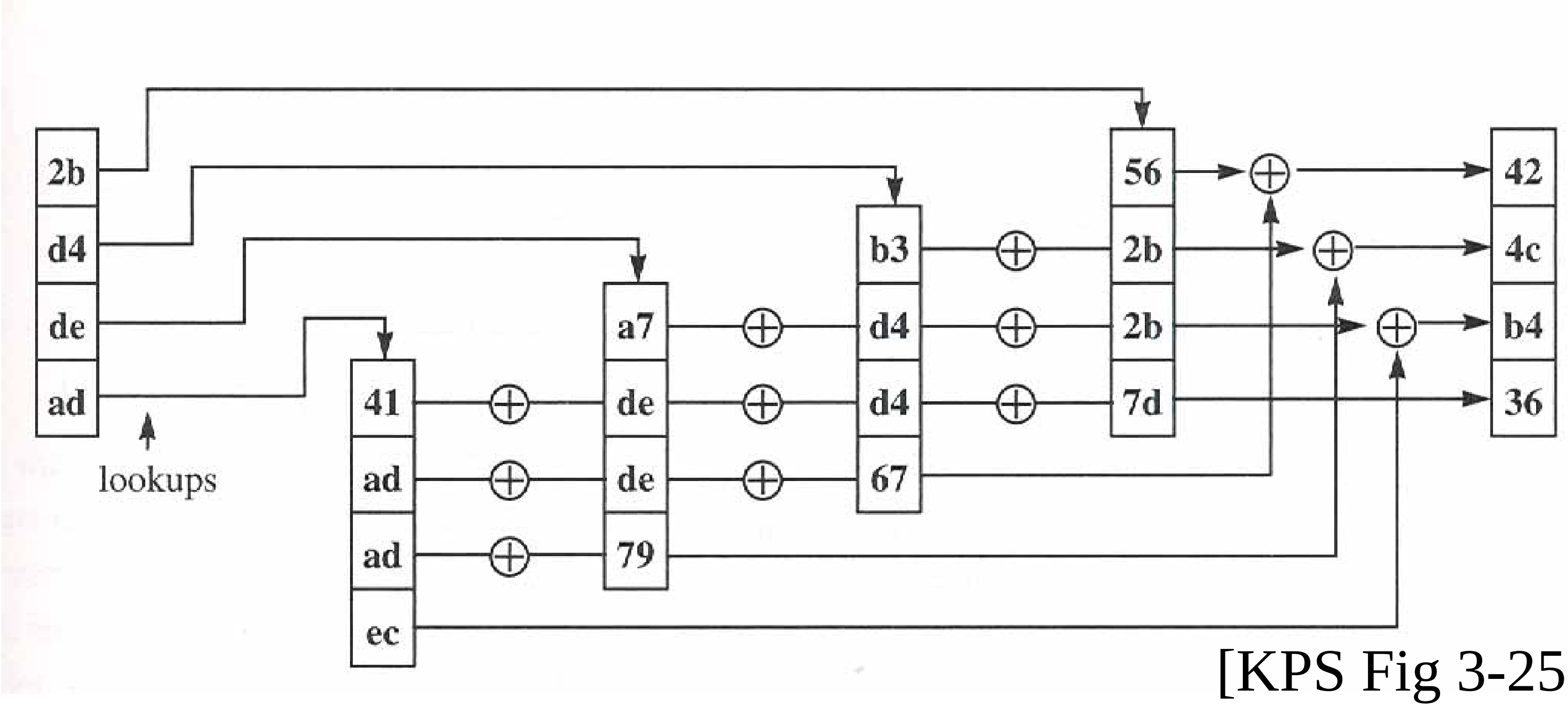
left (high-order) nibble

	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

[KPS Fig 3-26]

MixColumn (Cont)

- Retrieved column is rotated vertically so that its top octet is in the same row as the input octet
- Four rotated columns are xor'ed



[KPS Fig 3-25]

AES Decryption

- Inverse MixColumn
- Inverse S-Box
- Inverse Xor = Xor

Key Expansion

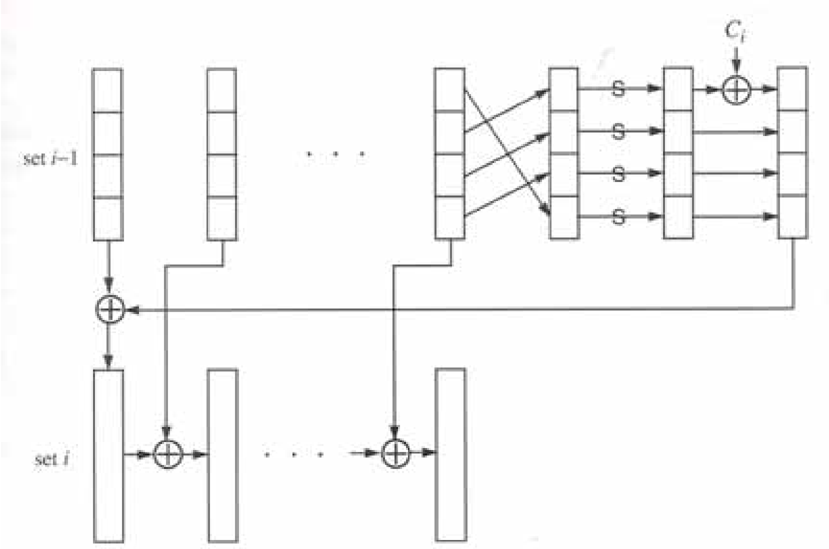
- Key flows in octet by octet in 4-octet columns.
- $(N_r+1)N_b$ columns
- Key expansion uses the same kind of primitive operations as the rounds
- Rows, columns, round keys are numbered starting at 0, round numbers start at 1

AES Key Expansion

- Column 0 of the ith set is obtained by rotating the last column of (i-1)th set upward by one cell, applying the S-Box to each octet, then Xor'ing a constant based on i into octet 0, and Xoring it with 0th column of (i-1)th set.
- Column j of the ith set is obtained by Xor'ing (j-1)th column with jth column of (i-1)th set

Set i-1

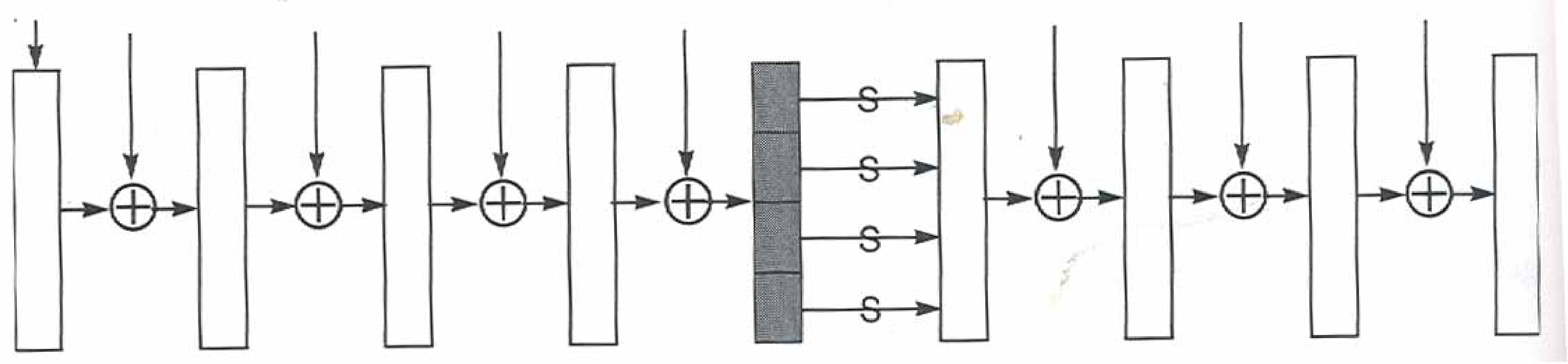
Set i



[KPS Fig 3-30]

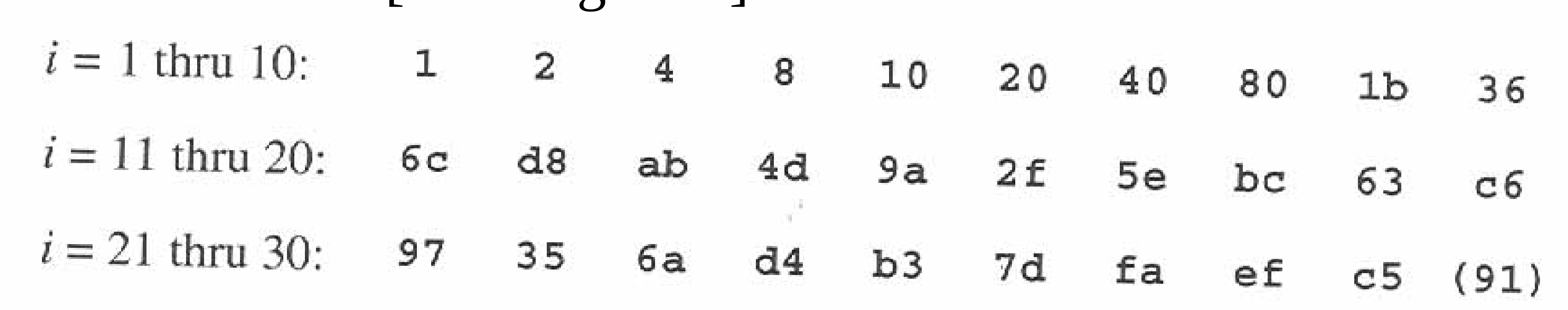
AES Key Expansion (Cont)

- If $N_k > 6$, then Column 4 is generated by applying S-box to each octet of the column



[KPS Fig 3-32]

- Constants: [KPS Fig 3-31]



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)

Rounds

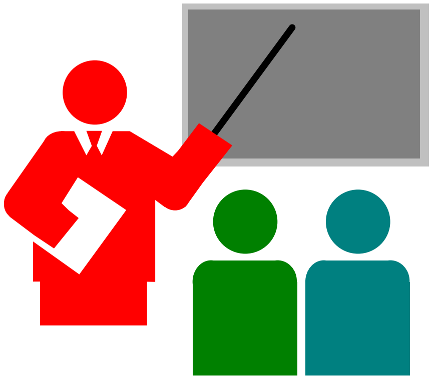
- 1. Each octet of the state has S-box applied to it
- 2. Rotation:
  - Row 1 is rotated left 1 column
  - Row 2 is rotated left 2+$\lfloor N_b/8 \rfloor$ columns
  - Row 3 is rotated left 3:$\lfloor N_b/7 \rfloor$ columns

    In AES-128, N_b=4 $\Rightarrow$ i^{th} row is rotated i columns
- 3. Each column of state has MixColumn applied to it.
- Round N_r omits this operation.

Ron's Cipher 4 (RC4)

- Stream Cipher
  - A pseudo-random stream is generated using a given key and xor'ed with the input
- Pseudo-random stream is called **One-Time pad**
- Key can be 1 to 256 octet
- See the C code in the book.

Summary



1. Block ciphers divide the input in fixed size blocks before encryption.
2. DES uses rotation, substitution, and mangler
3. DES uses 56-bit keys => No longer secure.
4. IDEA is international but protected by patent.
5. AES allows 128-bit, 192-bit, 256-bit keys.
6. RC4 is a stream cipher.

References

1. C. Kaufman, R. Perlman, and M. Speciner, “Network Security: Private Communication in a Public World,” 2nd Ed, Prentice Hall, 2002, ISBN: 0130460192
2. William Stallings, “Cryptography and Network Security,” 4th Ed, Prentice-Hall, 2006, ISBN:013187316
3. A. W. Dent and C. J. Mitchell, “User’s Guide to Cryptography and Standards,” Artech House, 2005, ISBN:1580535305
4. N. Ferguson and B. Schneier, “Practical Cryptography,” Wiley, 2003, ISBN:047122894X
5. Rijndael Animation, http://www.cs.bc.edu/~straubin/cs381-05/blockciphers/rijndael_ingles2004.swf

Homework 5

- Read chapter 3 of the textbook.
- Submit answer to Exercise 3.5 on page 92
- Exercise 3.5: Suppose the DES mangler function mapped every 32-bit value to zero, regardless of the value of its input. What function would DES compute?
- Hint:
  - 1. What is the net result of each round?
  - 2. What is the net result of 16 rounds?
  - 3. DES = Initial Permutation+16 rounds+Swap halves+Final Permutation
  - 4. Determine the bit positions 1..64 based after the above 4 operations.