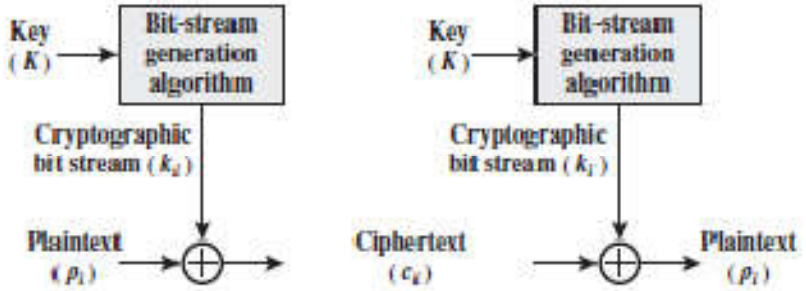
Symmetric Ciphers

CLASSICAL ENCRYPTION TECHNIQUES

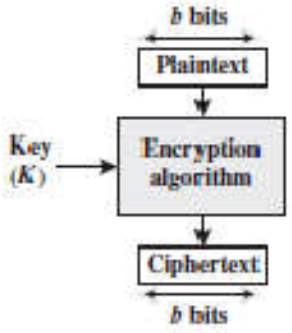
Block Cipher Principles

Stream cipher

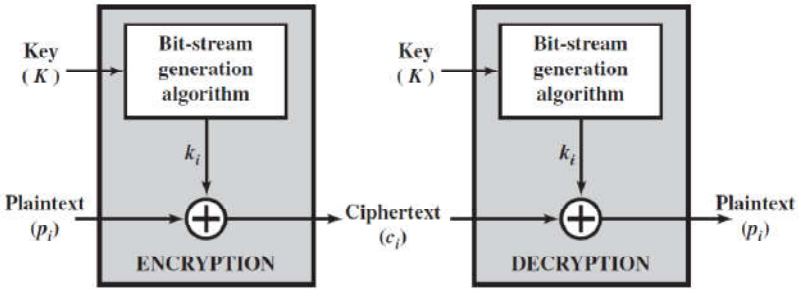
- autokeyed Vigenère cipher
- Vernam cipher



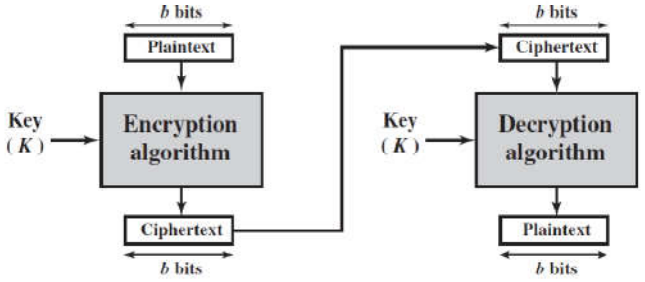
Block cipher



Block Cipher Principless



(a) Stream cipher using algorithmic bit-stream generator



(b) Block cipher

Block Cipher Principles

Plain text block size = n bit

Probable ciphered block = 2^n

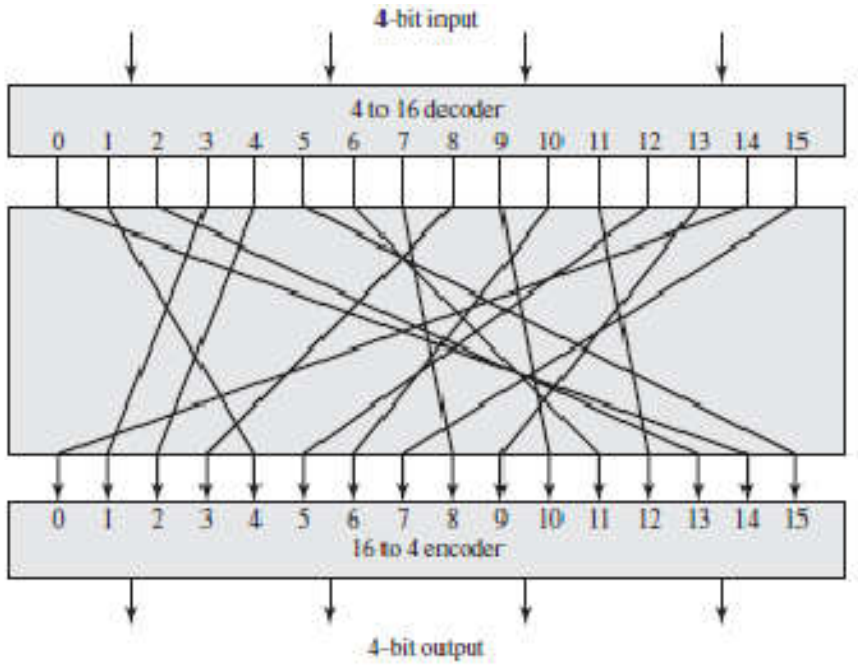
singular and Non-singular transformation

Reversible Mapping

Plaintext	Ciphertext
00	11
01	10
10	00
11	01

Irreversible Mapping

Plaintext	Ciphertext
00	11
01	10
10	01
11	01



Block Cipher Principles

Small block size vulnerable to statistical analysis just like classical substitution technique

Arbitrary substitution for large block size is impractical

- Key length = 4 bits * 16 rows = 64 bits
- For n-bit ideal block cipher key length= $n*2^n$ bits

Plaintext	Ciphertext
0000	1110
0001	0100
0010	1101
0011	0001
0100	0010
0101	1111
0110	1011
0111	1000
1000	0011
1001	1010
1010	0110
1011	1100
1100	0101
1101	1001
1110	0000
1111	0111

Ciphertext	Plaintext
0000	1110
0001	0011
0010	0100
0011	1000
0100	0001
0101	1100
0110	1010
0111	1111
1000	0111
1001	1101
1010	1001
1011	0110
1100	1011
1101	0010
1110	0000
1111	0101

Block Cipher Principles

$$y1 = k11x1 + k12x2 + k13x3 + k14x4$$

$$y2 = k21x1 + k22x2 + k23x3 + k24x4$$

$$y3 = k31x1 + k32x2 + k33x3 + k34x4$$

$$y4 = k41x1 + k42x2 + k43x3 + k44x4$$

xi – 4 bit input block, yi = 4 bit ciphered block, kij= binary coeficientes mod 2

Block size = n, key size = n^2
Vulnerable to cryptanalysis

Feistal Cipher

Block length => n, key length => k, possible transformation => 2^k (instead of 2^n)

Substitution

- Each plaintext element or group of elements is uniquely replaced by a corresponding ciphertext element or group of elements.

Permutation

- The order in which the elements appear in the sequence is changed

Based on Shannon's proposal

Shannon's proposal

Shannon refers to as a strongly ideal cipher, all statistics of the ciphertext are independent of the particular key used

Diffusion

- Achieved by having each plaintext digit affect the value of many ciphertext digits
- The statistical structure of the plaintext is dissipated into long-range statistics of the ciphertext

$$y_n = \left(\sum_{i=1}^{k} m_{n+i} \right) \bmod 26$$

- Frequencies in the ciphertext will be more nearly equal than in the plaintext
- Achieved by repeatedly performing some permutation on the data followed by applying a function to that permutation
- Every block cipher involves a transformation of a block of plaintext into a block of ciphertext, where the transformation depends on the key
- The mechanism makes the statistical relationship between the plaintext and ciphertext as complex as possible in order to thwart attempts to deduce the key

Shannon’s proposal

Confusion

- The mechanism make the relationship between the statistics of the ciphertext and the value of the encryption key as complex as possible
- The key was used to produce that ciphertext is so complex as to make it difficult to deduce the key.
- Achieved by the use of a complex substitution algorithm

Fiestel Cypher Structure

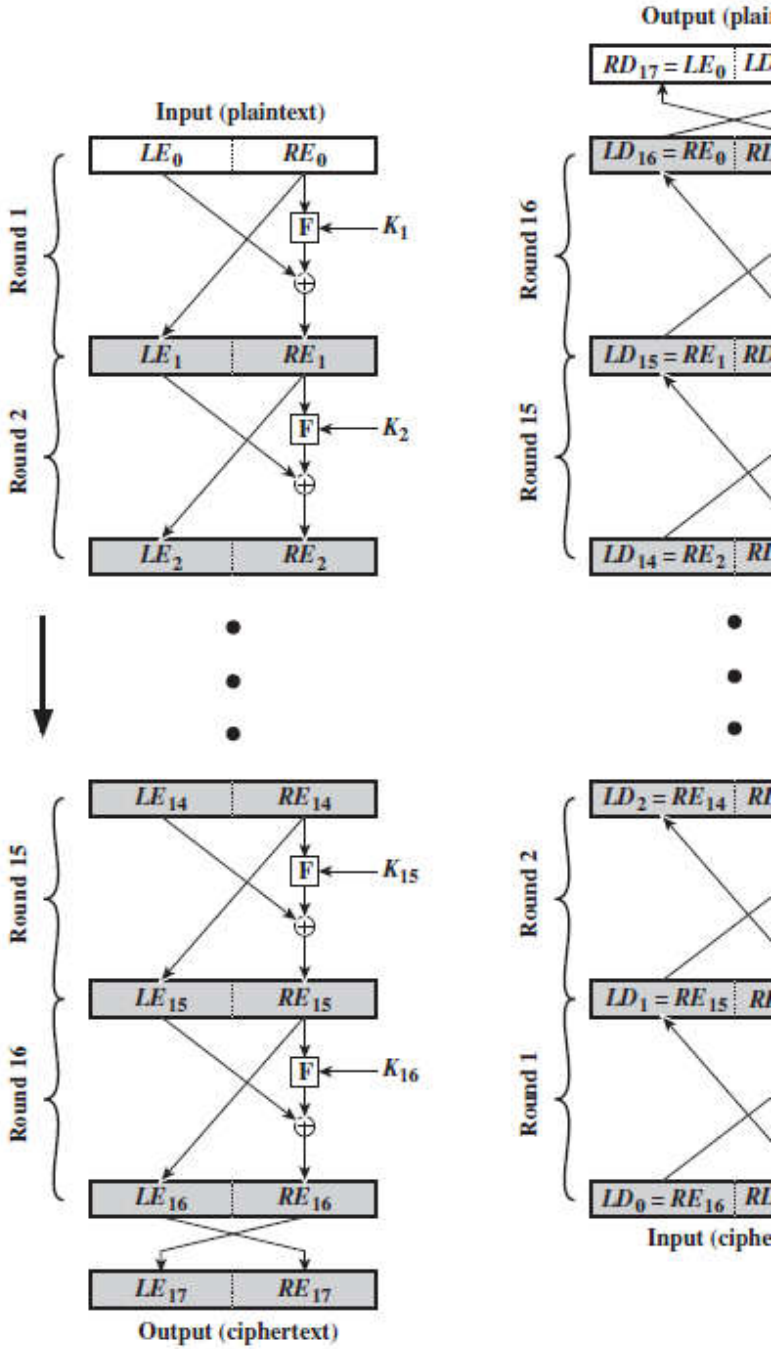
Input => 2w bit and Key=> K

All rounds have the same structure

Substitution

- Round function

Permutation



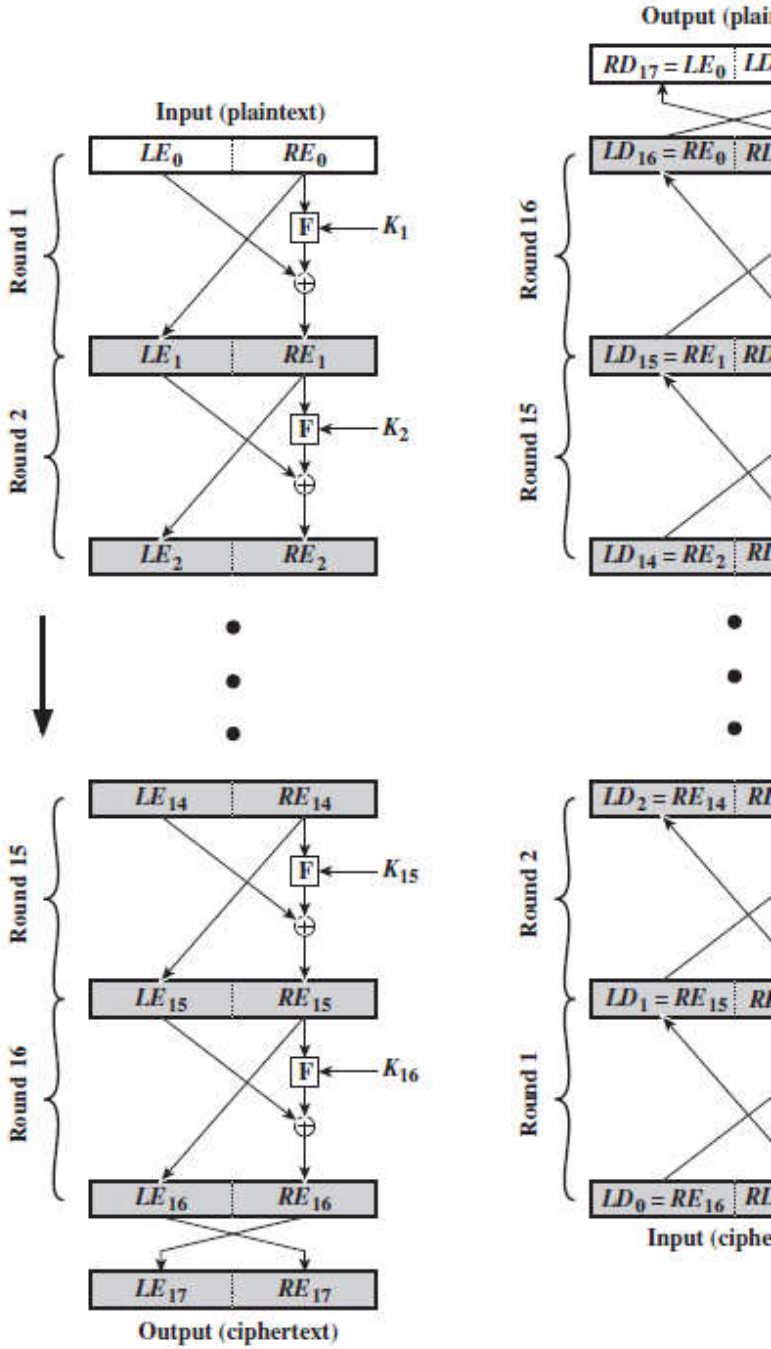
Fiestel Cypher Structure

Key parameters

- Block size
- Key size
- Number of rounds
- Subkey generation algorithm
- Round function F

Other consideration

- Fast software encryption / decryption
- Ease of analysis



Fiestel Decrypt. Alg.

Encryption process

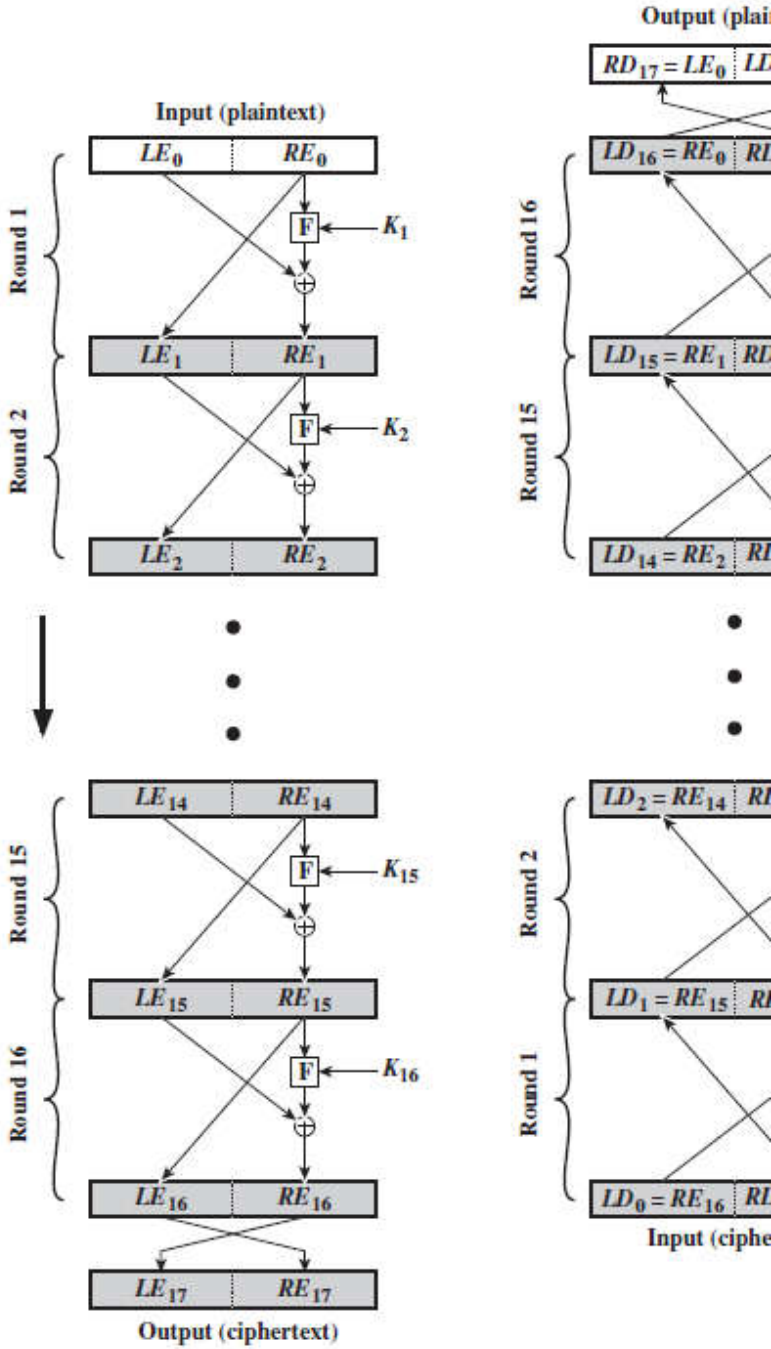
$$LE16 = RE15$$
$$RE16 = LE15 \oplus F(RE15, K16)$$

Decryption process

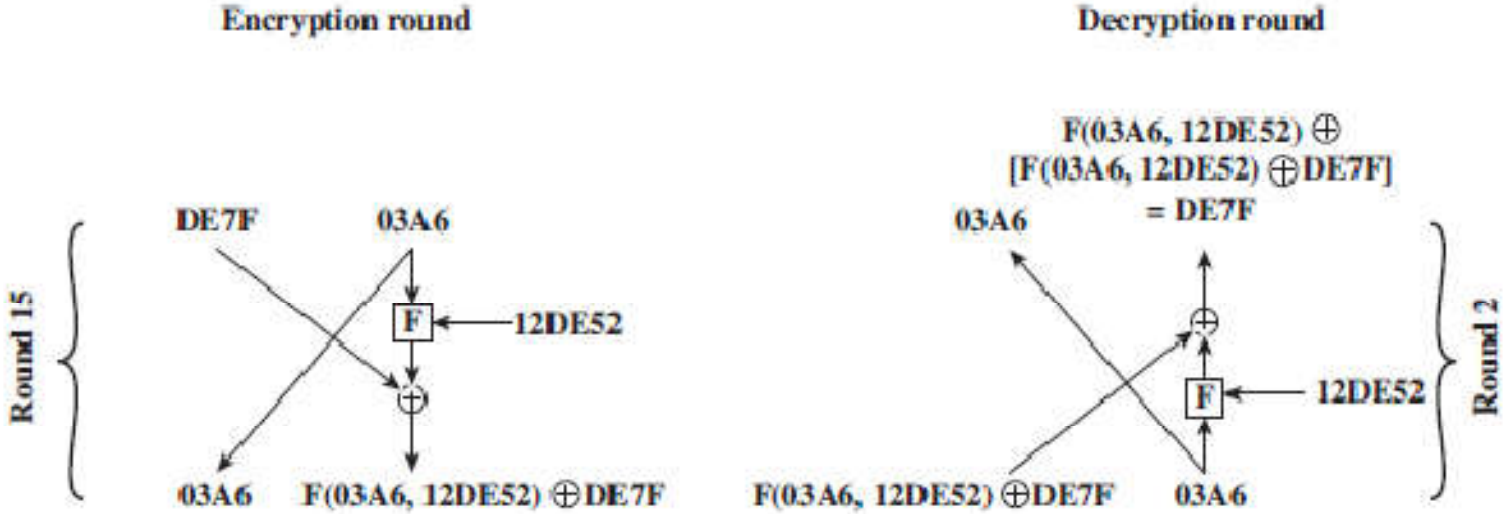
$$RD1 = LD1 = RD0 = LE16 = RE15$$
$$LD0 \oplus F(RD0, K16)$$
$$RE16 \oplus F(RE15, K16)$$
$$[LE15 \oplus F(RE15, K16)] \oplus F(RE15, K16)$$
$$LE15$$

i-th iteration of the algorithm

$$LE_i = RE_{i-1}$$
$$RE_i = LE_{i-1} \oplus F(RE_{i-1}, K_i)$$
$$RE_{i-1} = LE_i$$
$$LE_{i-1} = RE_i \oplus F(RE_{i-1}, K_i) = RE_i \oplus F(LE_i, K_i)$$



Fiestel Decrypt. Alg.



Data Encryption Standard (DES)

Background

National Institute of Standards and Technology (NIST)

Primary critisim

- Reduced Key size (56 bit) than IBM's original LUCIFER algorithm (128 bits)
- Classified S-BOX structure

Tripple DES

DES Encryption

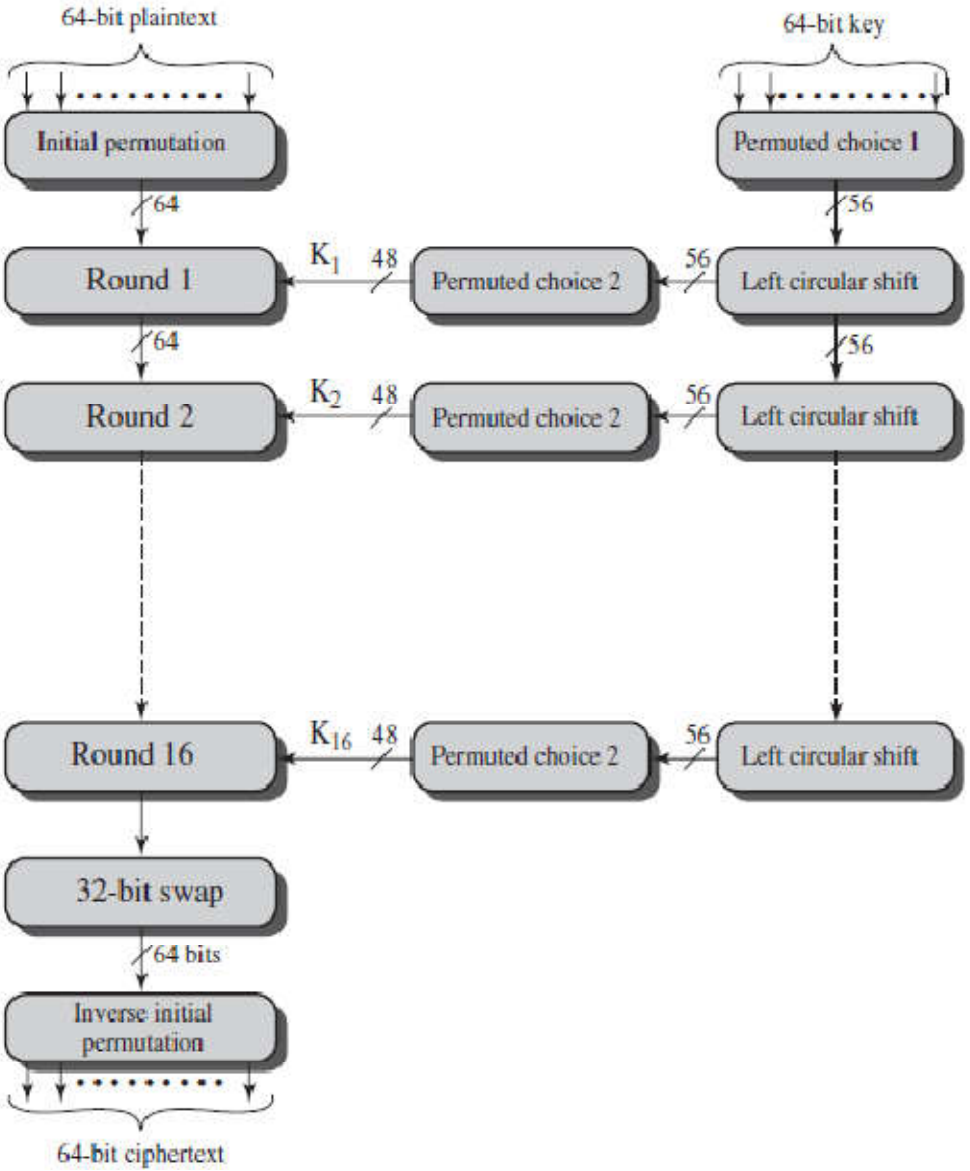
Plaintext => 64 bit

- Function expects 54 bits
- 8 bits can be used for other purposes (parity bits)

Initial permutation

Rounds

Inverse initial permutation



DES

(a) 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

(b) Inverse Initial 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

DES

(c) Expansion Permutation (E)

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

(d) Permutation Function (P)

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

DES-Single Round

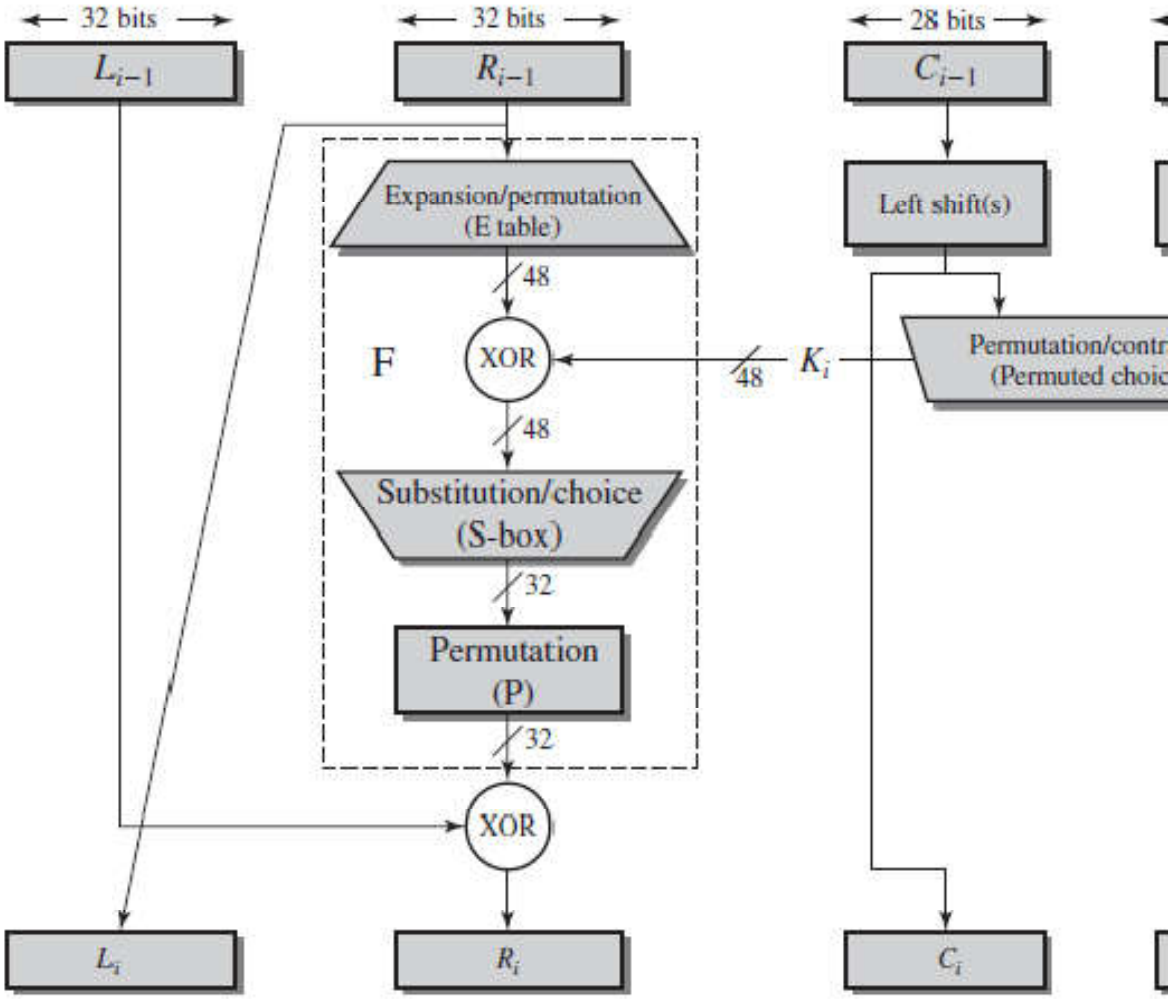
The left and right halves of each 64-bit intermediate value are treated as separate 32-bit quantities, labeled L (left) and R (right)

Key expansion of the R input

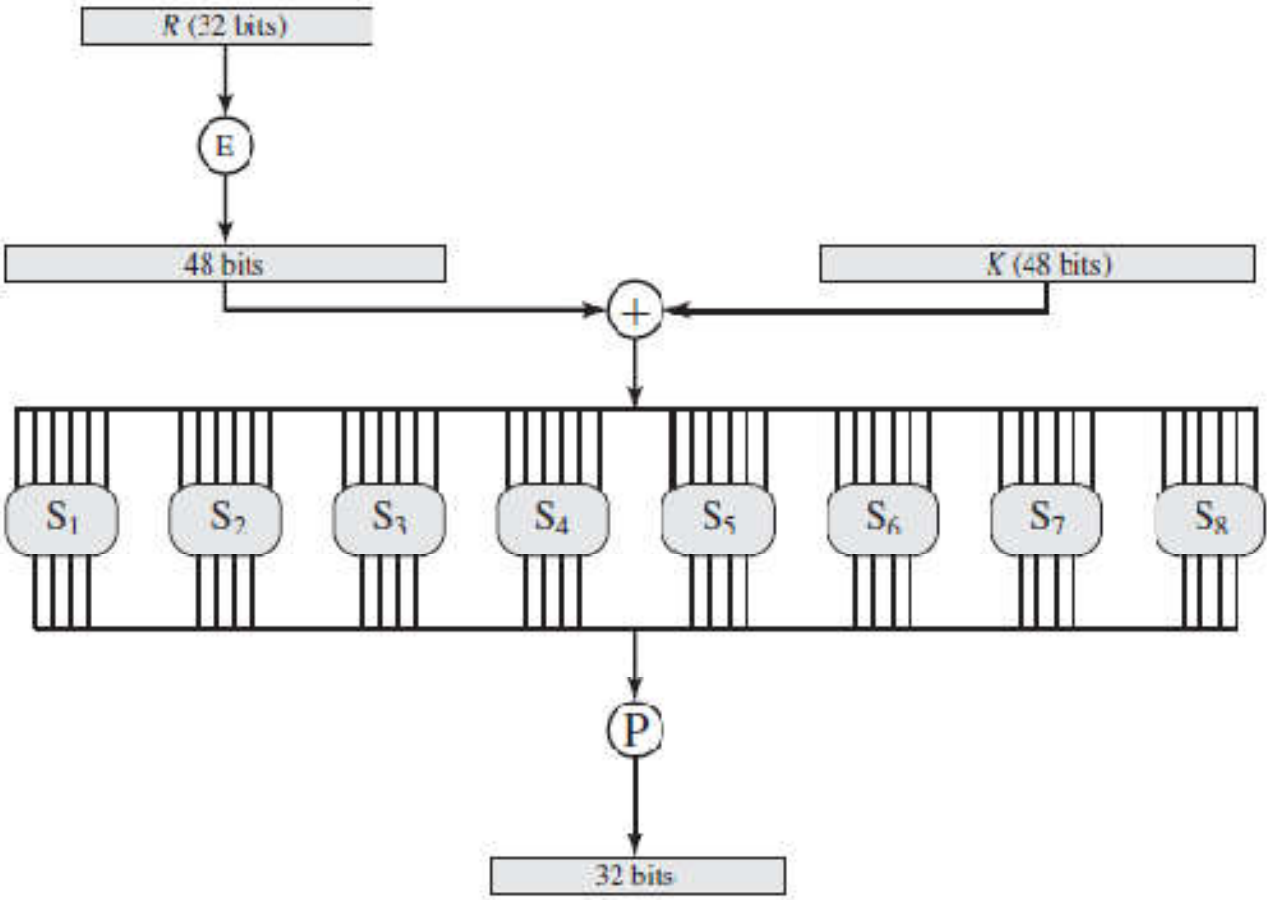
R is XORed with PC of Key

Substitution

permutation



F(R,K)



S-Box

S_1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	1

Key Generation

64 bit Key

54 bit used (every 8th bit is ignored)

(a) Input Key

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

(b) Permuted Choice One (PC-1)

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

(c) Permuted Choice Two (PC-2)

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

(d) Schedule of Left Shifts

Round Number	1	2	3	4	5	6	7	8	9	10	11	12	13
Bits Rotated	1	1	2	2	2	2	2	2	1	2	2	2	2

DES example

Plaintext:	02468aceeca86420
Key:	0f1571c947d9e859
Ciphertext:	da02ce3a89ecac3b

The Avalanche Effect

A small change in either the plaintext or the key should produce a significant change in the ciphertext.

Plaintext => **12468aceeca86420**

Key => **0f1571c947d9e859**

Round	K_i	L_i	
IP		5a005a00	
1	1e030f03080d2930	3cf03c0f	
2	0a31293432242318	bad22845	
3	23072318201d0c1d	99e9b723	
4	05261d3824311a20	0bae3b9e	
5	3325340136002c25	42415649	
6	123a2d0d04262a1c	18b3fa41	
7	021f120b1c130611	9616fe23	
8	1c10372a2832002b	67117cf2	
9	04292a380c341f03	c11bfc09	
10	2703212607280403	887fbc6c	
11	2826390c31261504	600f7e8b	
12	12071c241a0a0f08	f596506e	
13	300935393c0d100b	738538b8	
14	311e09231321182a	c6a62c4e	
15	283d3e0227072528	56b0bd75	
16	2921080b13143025	75e8fd8f	
IP^{-1}		da02ce3a	

DES – Change in plaintext

Change=> 4th bit of plaintext

Round		δ
	02468aceeca86420 12468aceeca86420	1
1	3cf03c0fbad22845 3cf03c0fbad32845	1
2	bad2284599e9b723 bad3284539a9b7a3	5
3	99e9b7230bae3b9e 39a9b7a3171cb8b3	18
4	0bae3b9e42415649 171cb8b3ccaca55e	34
5	4241564918b3fa41 ccaca55ed16c3653	37
6	18b3fa419616fe23 d16c3653cf402c68	33
7	9616fe2367117cf2 cf402c682b2cefbc	32
8	67117cf2c11bfc09 2b2cefbc99f91153	33

Round	
9	c11bfc09887fbc6 99f911532eed7d9
10	887fbc6c600f7e8 2eed7d94d0f2309
11	600f7e8bf596506 d0f23094455da9c
12	f596506e738538b 455da9c47f6e3cf
13	738538b8c6a62c4 7f6e3cf34bc1a8d
14	c6a62c4e56b0bd7 4bc1a8d91e07d40
15	56b0bd7575e8fd8 1e07d4091ce2e6d
16	75e8fd8f2589649 1ce2e6dc365e5f5
IP^{-1}	da02ce3a89ecac3 057cde97d7683f2

DES – Change in key

Change => 4th bit of key

Old key=> **0f1571c947d9e859**

New key => **1f1571c947d9e859**

Round		δ
	02468aceeca86420 02468aceeca86420	0
1	3cf03c0fbad22845 3cf03c0f9ad628c5	3
2	bad2284599e9b723 9ad628c59939136b	11
3	99e9b7230bae3b9e 9939136b768067b7	25
4	0bae3b9e42415649 768067b75a8807c5	29
5	4241564918b3fa41 5a8807c5488dbe94	26
6	18b3fa419616fe23 488dbe94aba7fe53	26
7	9616fe2367117cf2 aba7fe53177d21e4	27
8	67117cf2c11bfc09 177d21e4548f1de4	32

Round	
9	c11bfc09887fbc6c 548f1de471f64dfd
10	887fbc6c600f7e8b 71f64dfd4279876c
11	600f7e8bf596506e 4279876c399fdc0d
12	f596506e738538b8 399fdc0d6d208dbb
13	738538b8c6a62c4e 6d208dbbb9bdeeaa
14	c6a62c4e56b0bd75 b9bdeeaad2c3a56f
15	56b0bd7575e8fd8f d2c3a56f2765c1fb
16	75e8fd8f25896490 2765c1fb01263dc4
IP^{-1}	da02ce3a89ecac3b ee92b50606b62b0b

Strength of DES

The Use of 56-Bit Keys

- key length =>56 bits (2^{56} possible keys)

The nature of the DES

Timing analysis

- A timing attack exploits the fact that an encryption or decryption algorithm often takes slightly different amounts of time on different inputs

The Use of 56-Bit Keys

key length =>56 bits (2^{56} possible keys)

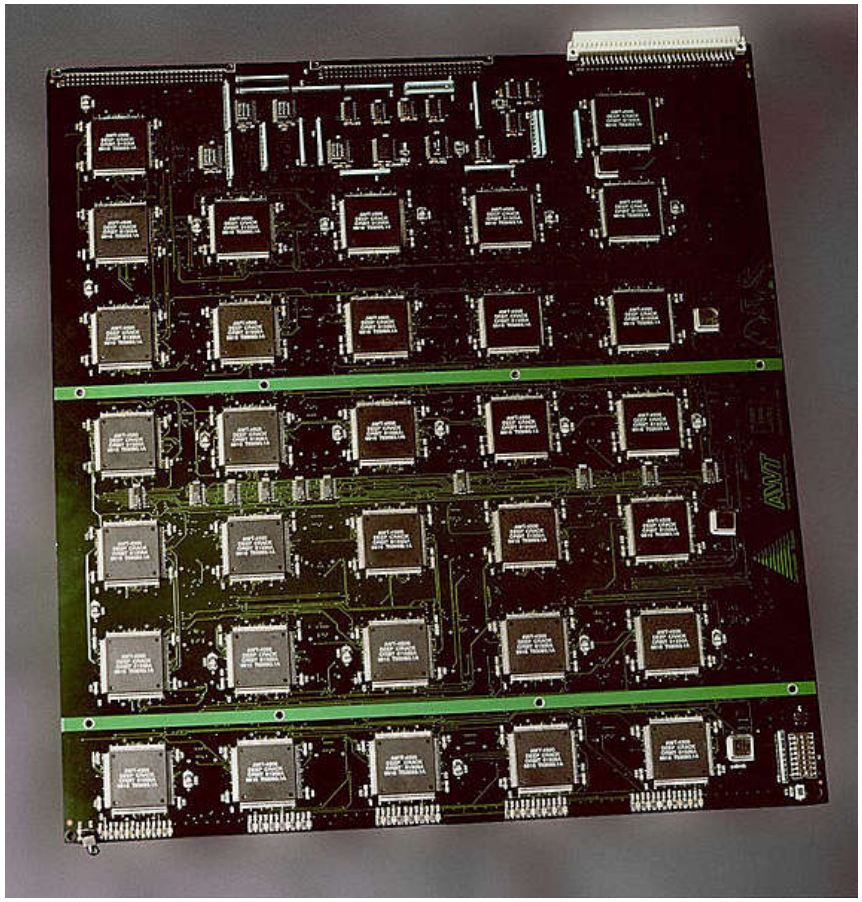
1977, Diffie and Hellman postulated that the technology existed to build a parallel machine with 1 million encryption devices, each of which could perform one encryption per microsecond

- Average search time => 10 hours
- Estimated cost => $20 million

Jult 1998, DES proved insecure

- Electronic Frontier Foundation (EFF) announced that it had broken a DES encryption using aspecial-purpose “DES cracker” machine
- Search time => less than 3 days
- Estimated cost => $250,000
- EFF approach addresses automated techniques to search within the recovered plaintext

DES Cracker



DES Design Criteria

Number of Rounds

- The greater the number of rounds, the more difficult it is to perform cryptanalysis, even for a relatively weak F.
- The criterion should be that the number of rounds is chosen so that known cryptanalytic efforts require greater effort than a simple brute-force key search attack

DES Design Criteria

Design of Function F

- The heart of a Feistel block cipher is the function F, which provides the element of confusion in a Feistel cipher
- One obvious criterion is that F be nonlinear.
- The more difficult it is to approximate F by a set of linear equations, the more nonlinear F is
- The algorithm to have good avalanche properties
  - Any output bit *j* of an S-box should change with probability 1/2 when any single input bit *i* is inverted for all *i*, *j*.

DES Design Criteria

Key Schedule Algorithm

- With any Feistel block cipher, the key is used to generate one subkey for each round
- Select subkeys to maximize the difficulty of deducing individual subkeys and the difficulty of working back to the main key.
- Adams suggests [ADAM94] that, at minimum, the key schedule should guarantee key/ciphertext Strict Avalanche Criterion and Bit Independence Criterion

Reference books

Cryptography and Network Security Principles and Practices

- William Stallings

Network Security PRIVATE Communication in a PUBLIC World

- Chalie Kaufman, Radia Perlman, Mike Speciner