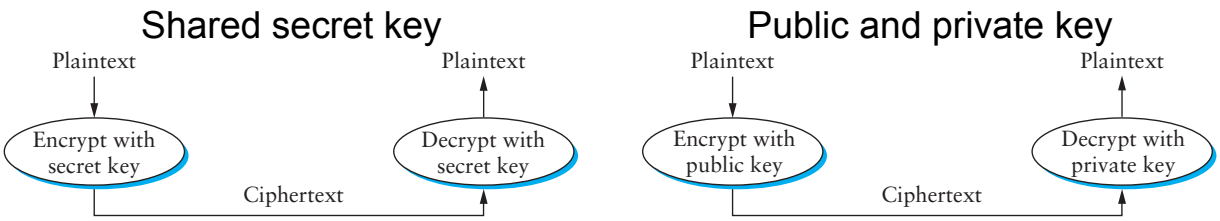
Encryption



Some terms

- Plaintext
- Ciphertext

DES – Data Encryption Standard

based on Lucifer encryption developed by IBM in mid-70's

- Lucifer had a 128-bit key
- DES has a 56-bit key (within a 64-bit sequence)
- some of the design decisions have been kept secret

FIPS publication 46-2, 30 December, 1993

Three phases of DES

1) 64 bits are shuffled
2) Sixteen rounds of shuffling and XORing the bits
3) 64 bits are reshuffled – inverse of step 1

Initial permutation							
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 (inverse) permutation							
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

That is, input bit 58 is output bit 1 of initial permutation

In each of the 16 rounds, a different 56 bit "key" is used:

$K_n = KS(n, KEY)$ for $n = 1$ to 16

and KS is the "key schedule"

Permuted Choice 1:

A permutation to choose 28 C-bits and 28 D-bits

C_0 bits						
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

D_0 bits						
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

Next the C and D bits go throw 16 left circular shifts

C_i = circular left shift(C_{i-1}, S_i)

D_i = circular left shift(D_{i-1}, S_i)

Iteration number	Number of shifts
1	1
2	1
3	2
4	2
5	2
6	2
7	2
8	2
9	1
10	2
11	2
12	2
13	2
14	2
15	2
16	1

Then Kn is chosen from a permutation of Cn .. Dn

Permuted Choice 2:

A permutation to 56-bit key for the stage

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

Are we there yet…

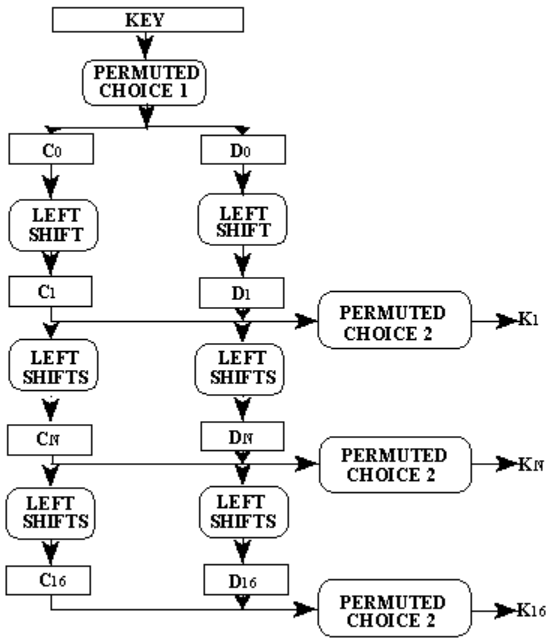


Figure 3 – FIPS 46

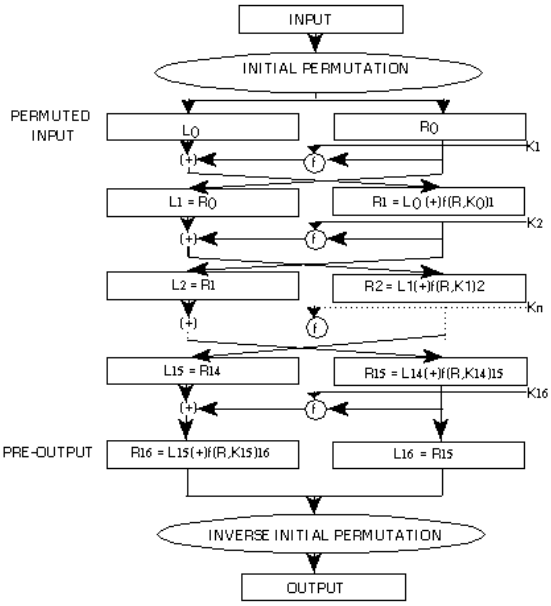
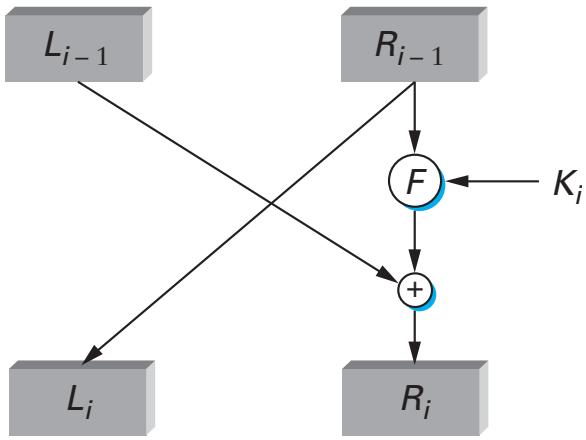


Figure 1 – FIPS 46

f, the "cipher function"

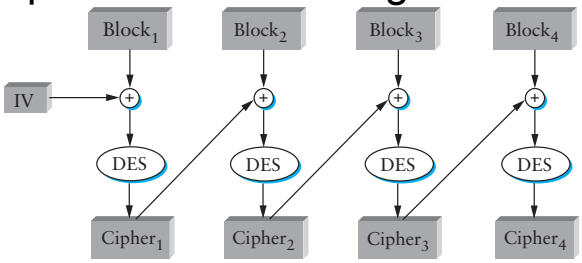
$$L_i = R_{i-1}$$
$$R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$$

Go to FIPS 46



Variations on DES

Cipher Block Chaining – CBC



Triple DES – 3DES

Sends the data through three keys
192 bits of encryption

RSA – Rivest Shamir Adelman

1) Choose two large prime numbers *p* and *q*
   Most likely with a probabilistic algorithm
   Or the famous recent polynomial test
2) $n = p * q$
3) Choose encryption key *e*,
   such that *e* and $(p - 1) \times (q - 1)$ are relatively prime
4) Compute decryption key *d*
   such that $d*e \bmod ((p - 1) \times (q - 1)) = 1$

Public key: (e, n)
Private key: (d, n)
Throw away *p* and *q*

Encryption of plaintext m: $c = m^e \bmod n$
Decryption of cyphertext c: $m = c^d \bmod n$

Message Digests and Secure Hashes

Transform long text sequences into short signatures
MD5 – RFC 1321, Ron Rivest
`openssl dgst -md5` on Linux