Modern Symmetric Ciphers

Data and Information Management: ELEN 3015

School of Electrical and Information Engineering,
University of the Witwatersrand

Terminology

Little Endian

Big Endian

NB: Cryptography $\rightarrow$ Little Endian format

Terminology

Big Endian: Most significant byte first

Little Endian: Least significant byte first

(Most modern computer processors agree on bit ordering "inside" individual bytes)

1. Symmetric Ciphers

Def - Symmetric Cipher: Cipher that uses same key for encryption and decryption

Def - Modern Cryptography: Cryptosystems where the security resides in the key and not in the algorithm

1. DES - Data Encryption Standard

- Standard based on DEA
- First Cryptographic standard
- Developed by IBM and NSA (USA)

1. DES - Data Encryption Standard

Motivation:

- Public / Commercial cryptography was unreliable
- Need for a verifiable standard
- Interoperability between cryptosystems

1. DES - Data Encryption Standard

Specifications:

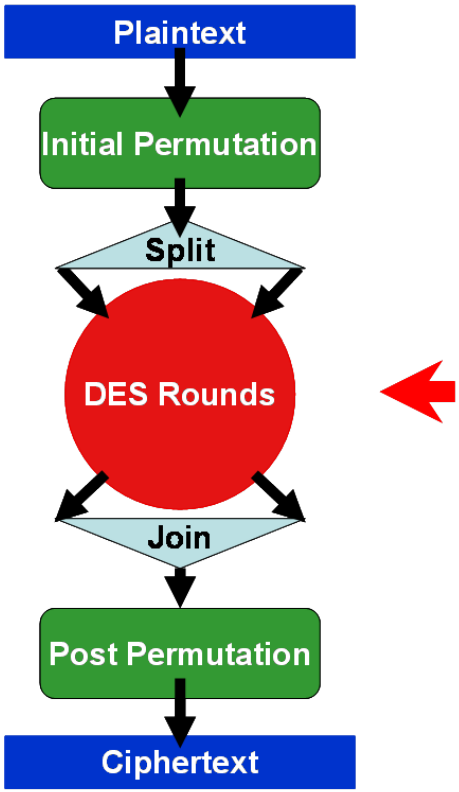
- High level of security
- Completely specified and easy to understand
- Security must reside in the key
- Available to all users
- Adaptable
- Economically implementable
- Efficient
- Ability to be validated
- Be exportable

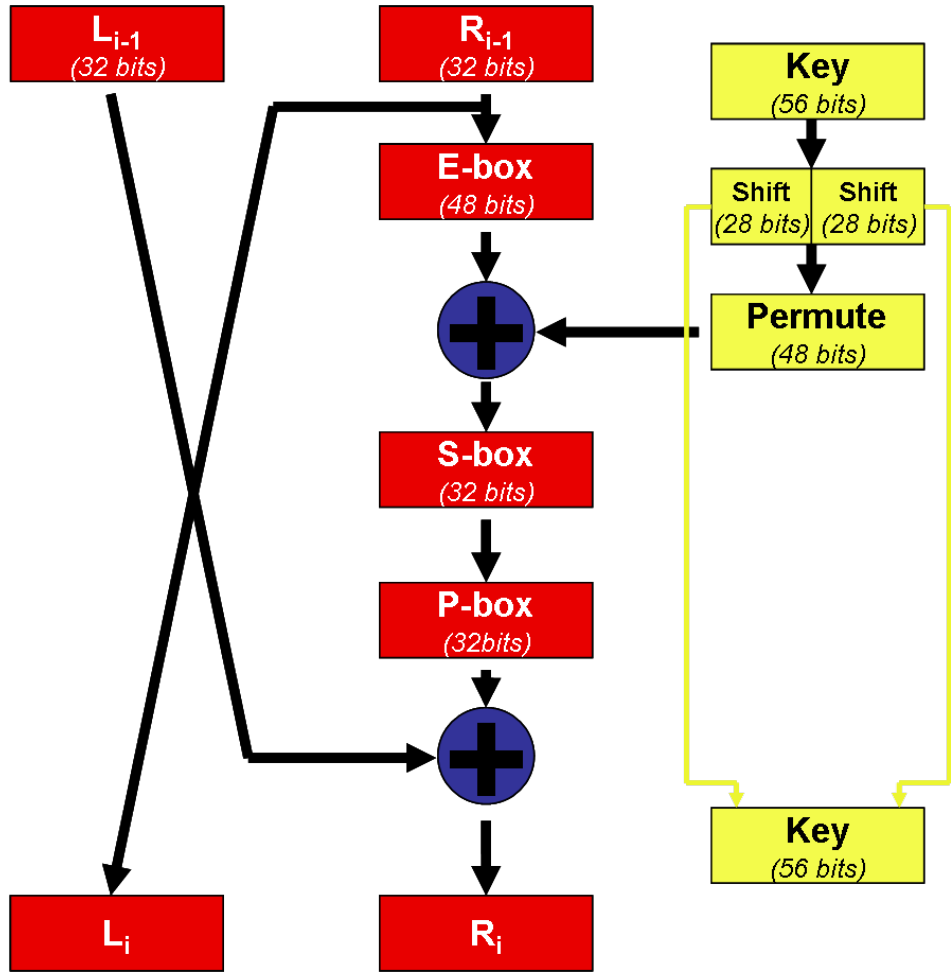
2. DES - Overview

2.1. Block and key structure

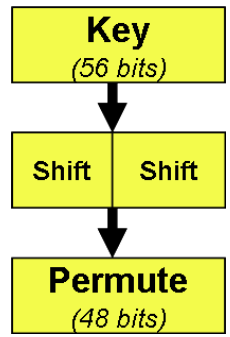
- Based on substitution and permutation
- Block Cipher - works on 64 bit blocks
- Output - also 64 bits
- Symmetric - Keys and algorithm
- Key length 56 bits (64 including parity)
- Security lies entirely in key
- Simple and repetitive, perfect for hardware implementation
- Round - fundamental building block (DEA - 16 rounds)

DES - Operation





DES - Key Schedule



DES - Key Schedule

Key $\rightarrow$ 64 bits

Remove parity bits (Reduce to 56 bits)

For eack key K_i

- split 56-bit key into two halves (28 bits each)
- Each halve is circularly shifted left by 1 or 2 bits (depends on round) (K_{r_i})
- After shift, 48 bits selected with compression permutation (K_{k_i})

K_{k_i} is input to feistel function

K_{r_i} is input to next round of key schedule

DES - Key Schedule

Table: Key Permutation

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

DES - Key Schedule

Table: Number of Key Bits Shifted per Round

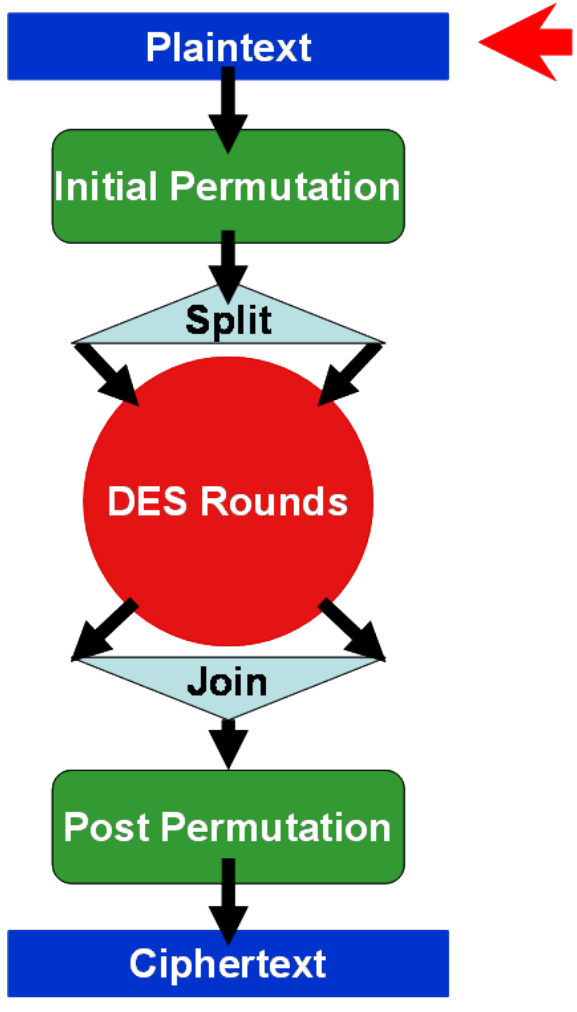
Round	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Shifts	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

DES - Key Schedule

Table: Compression Permutation

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

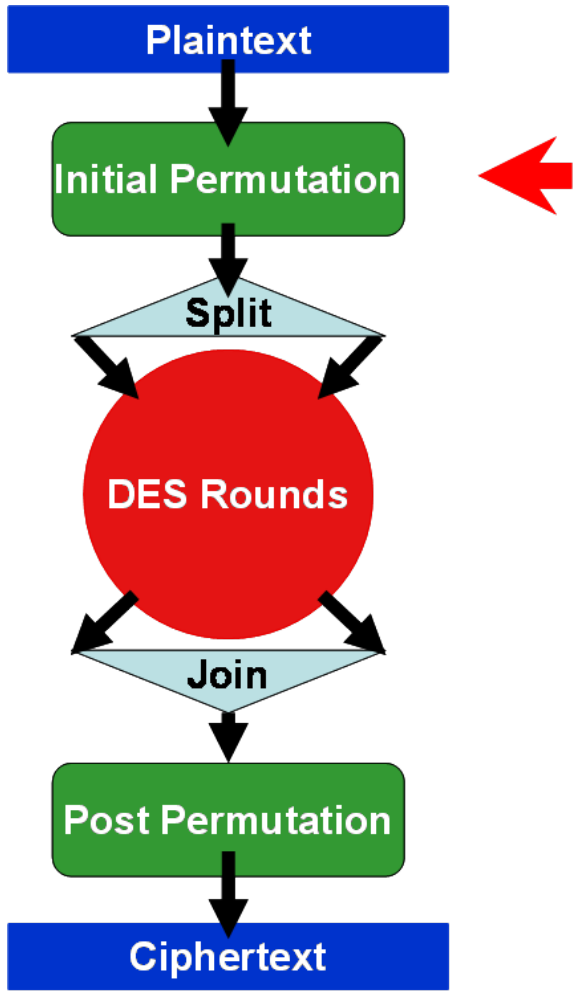
DES - Input


Plaintext
Initial Permutation
Split
DES Rounds
Join
Post Permutation
Ciphertext

DES - Input

- DES requires blocks of 64 bits to work on

DES - Initial Permutation



DES - Initial Permutation

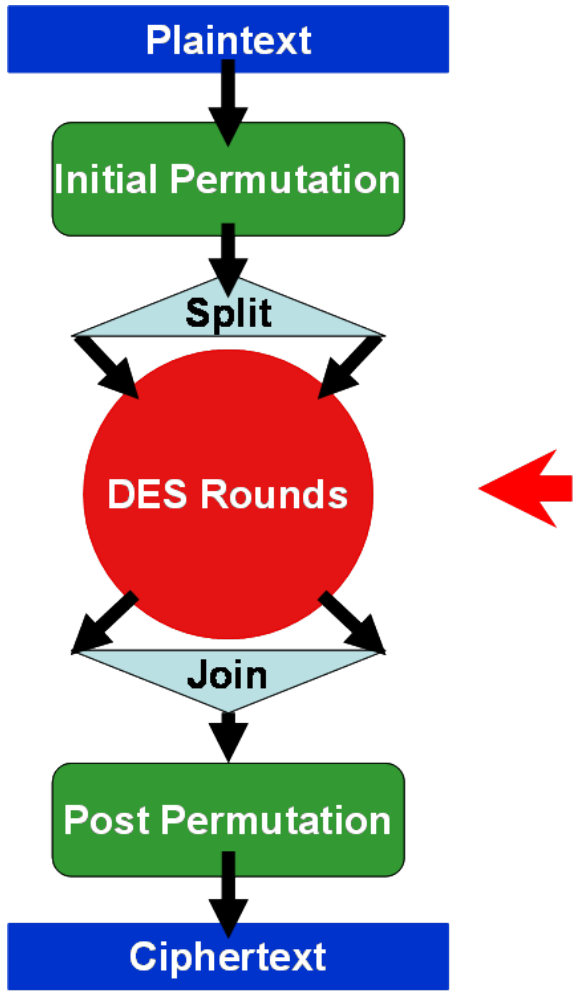
- Initial Permutation is a straight permutation of plaintext
- Does not affect security of DES
- Probably designed to allow easier loading of plaintext /ciphertext into a DES processor
- After initial permutation, the data is broken into two blocks (left half and right half, each 32 bits)

DES - Initial Permutation

Table: 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

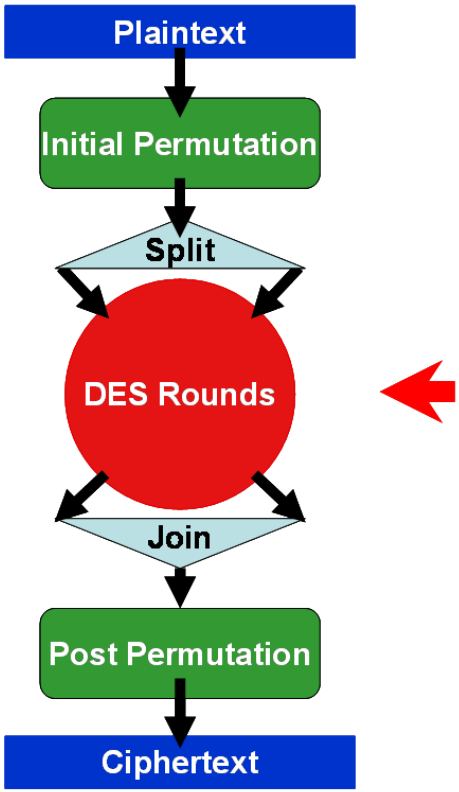
DES - Rounds

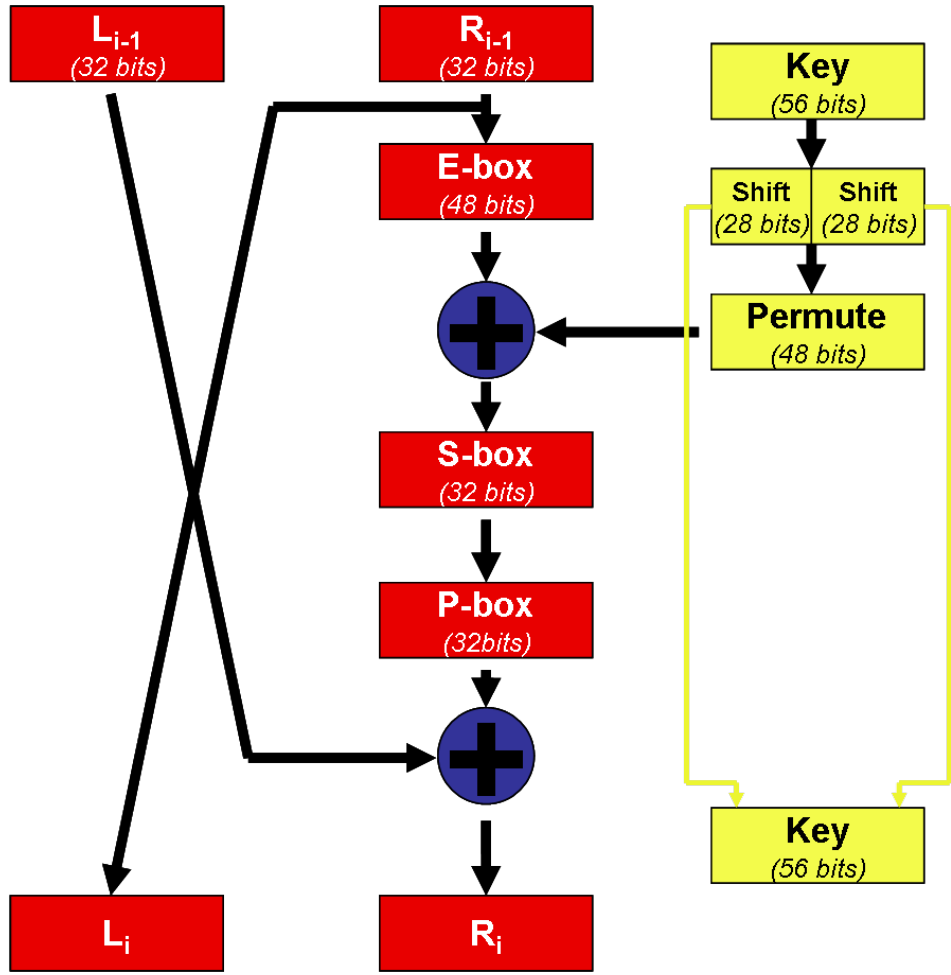

Plaintext
Initial Permutation
Split
DES Rounds
Join
Post Permutation
Ciphertext

DES - Rounds

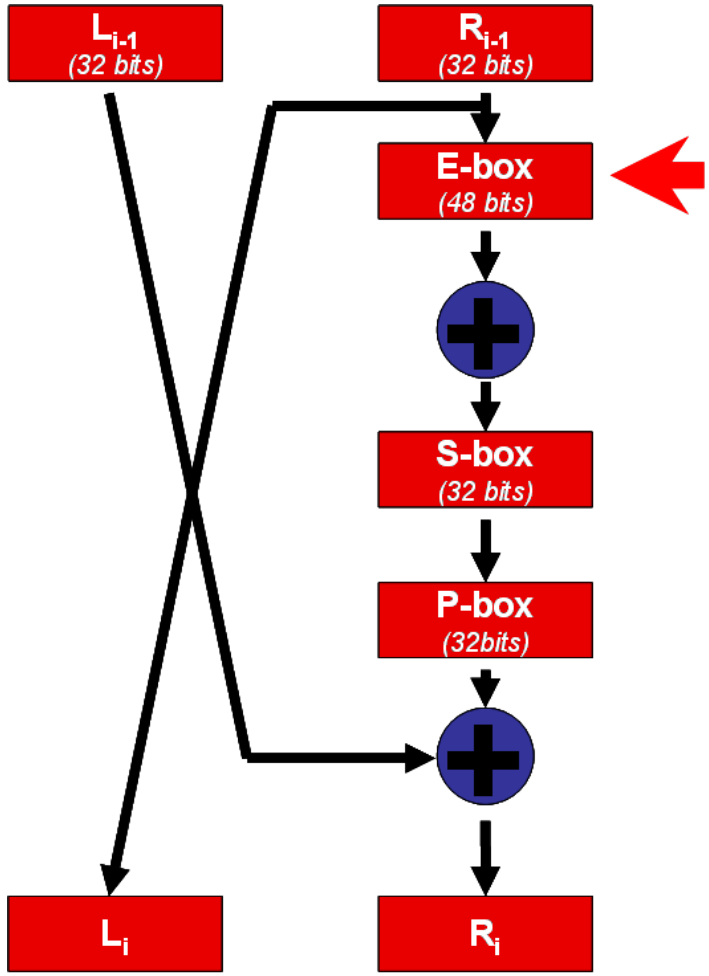
- DES has 16 rounds
- Each round consists of a permutation (E-Box), substitution (S-Box) and a permutation (P-box)
- Each round uses a sub-key of 48 bits

DES - One Round





DES - E-Box Expansion



DES - E-Box Expansion

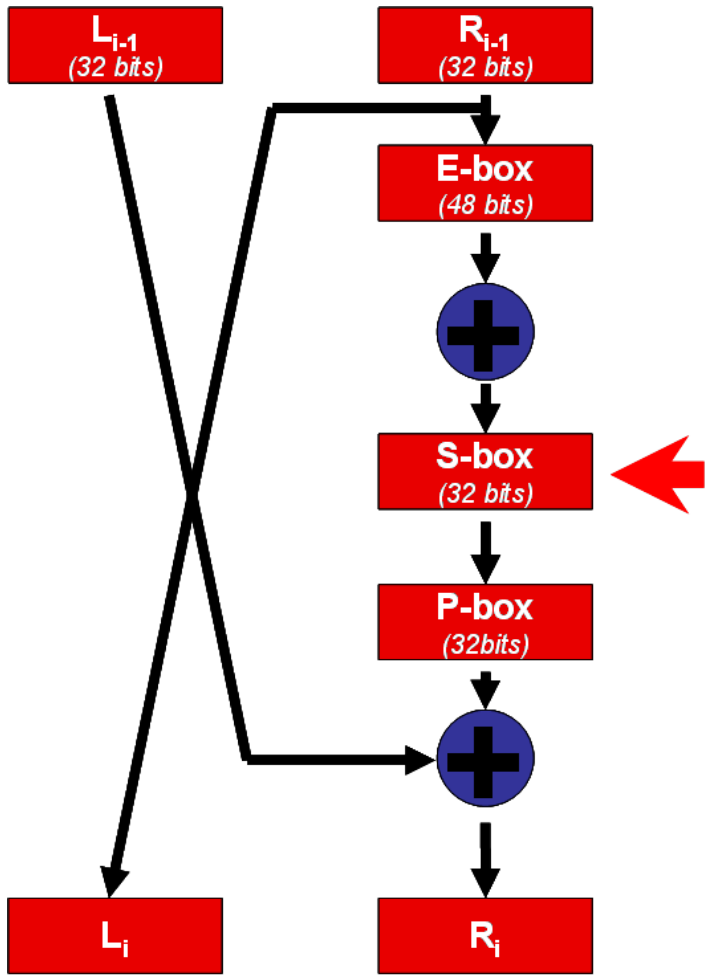
- Expands right hand side to 48 bits by duplicating certain bits
- Output same length as subkey $\rightarrow$ XOR
- Avalanche effect: dependence of all output bits on each input bit
- Expands and permutes $\rightarrow$ diffusion

DES - E-Box Expansion

Table: E-box expansion

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

DES - S-Box Substitution



DES - S-Box Substitution

- Performs substitution and compression $\rightarrow$ output 32 bits
- Introduces confusion
- 8 different S-Boxes
- Each S-Box has 6 inputs and 4 outputs
  - Each 48 bit input divided into 8 blocks of 6 bits
  - first and last bits determine row
  - middle bits determine column

DES - S-Box Substitution

Table: S-Box 1

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

DES - S-Box Substitution

Table: S-Box 2

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

DES - S-Box Substitution

Table: S-Box 3

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

DES - S-Box Substitution

Table: S-Box 4

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

DES - S-Box Substitution

Table: S-Box 5

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

DES - S-Box Substitution

Table: S-Box 6

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

DES - S-Box Substitution

Table: S-Box 7

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

DES - S-Box Substitution

Table: S-Box 8

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

DES - S-Box Substitution

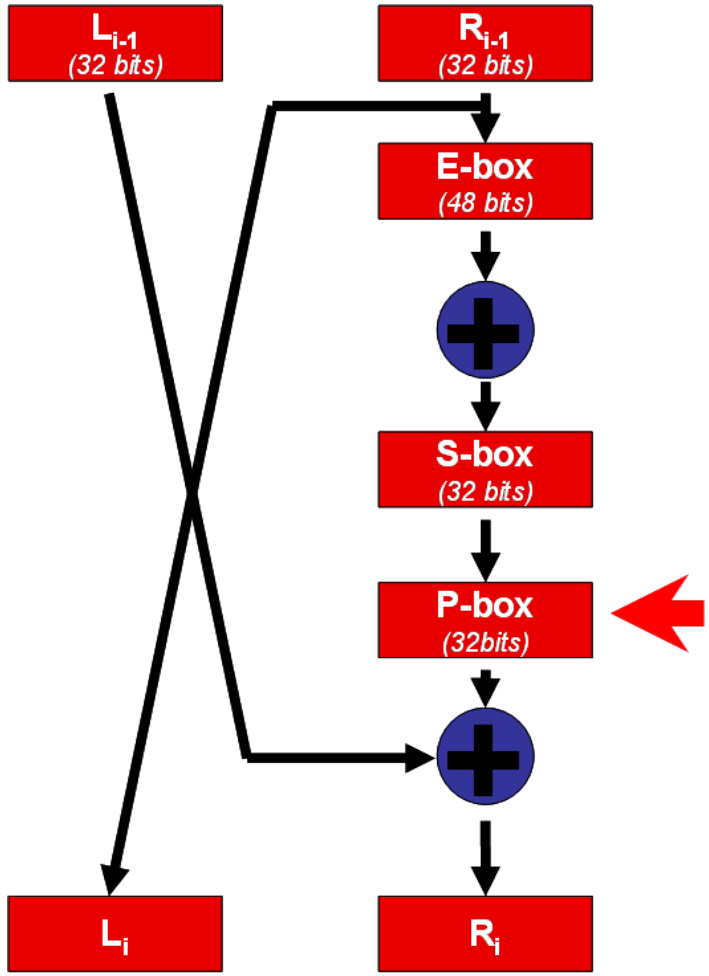
Example:

First input block - 100111_2 (using S-Box 1)

$$\begin{array}{lcll} \text{Row} & = & \text{bit 1, bit 6} & = & 11_2 \text{ (row 3)} \\ \text{Column} & = & \text{bits 2-5} & = & 0011_2 \text{ (col 3)} \\ & = & 2_{10} & & \\ & = & 0010_2 & & \end{array}$$

NB: rows and columns are zero indexed

DES - P-Box Permutation



DES - P-Box Permutation

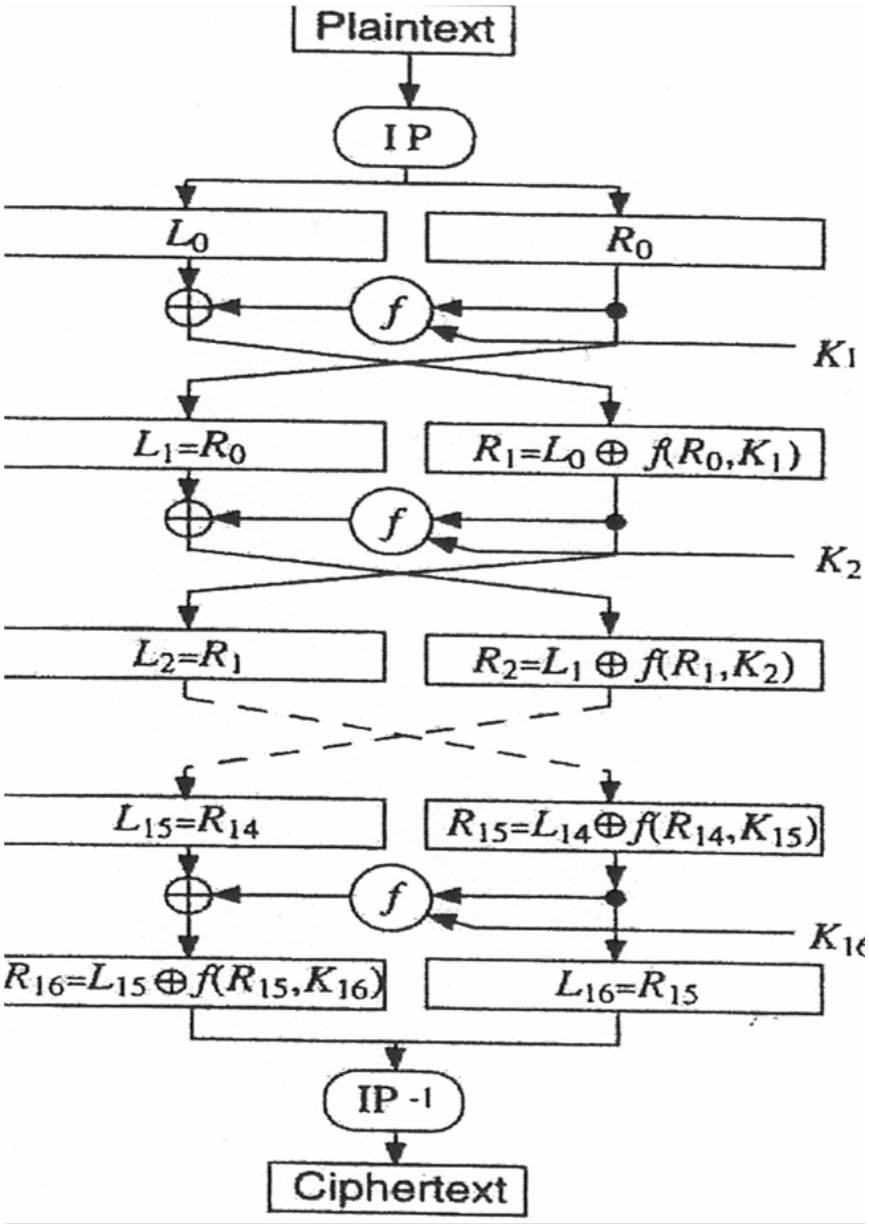
- Performs 1-1 bit mapping permutation

DES - P-Box Permutation

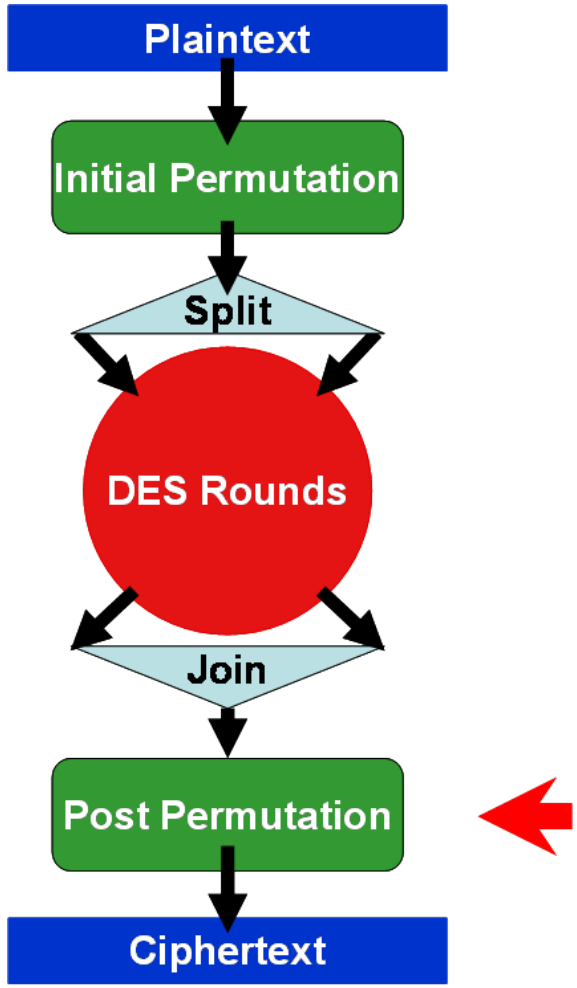
Table: P-Box Permutation

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

DES - Complete set of rounds



DES - Final Permutation



DES - Final Permutation

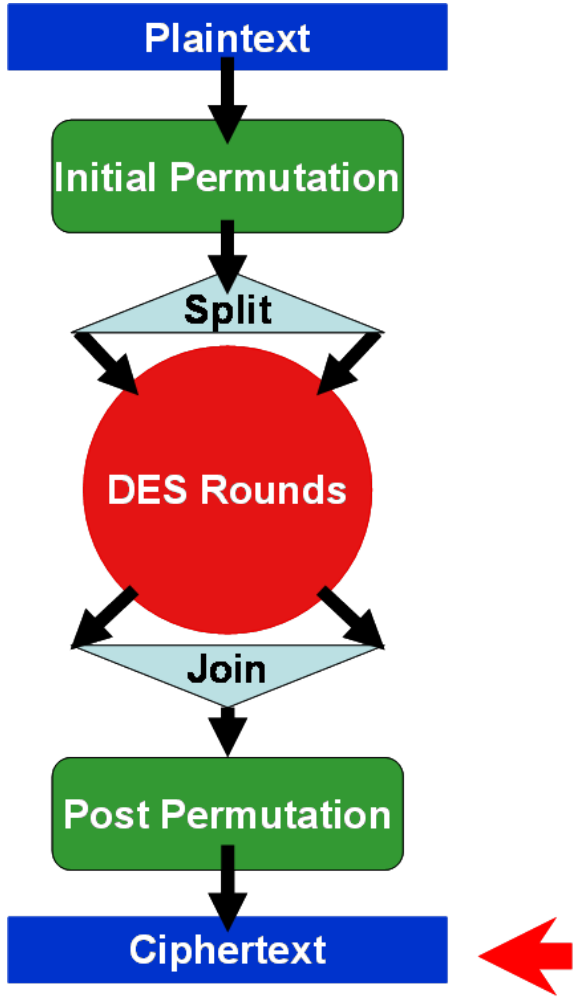
- Streams are rejoined before final permutation (64 bit output)
- Inverse of initial permutation

DES - Final Permutation

Table: Final 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

DES - Output


Plaintext
Initial Permutation
Split
DES Rounds
Join
Post Permutation
Ciphertext

DES - Output

- 64 bit ciphertext block results

DES - Decryption

Use exactly same algorithm

Reverse order of keys

DES - Analysis

- Number of rounds
  - 5 rounds ensure every ciphertext bit is a function of every plaintext and key bit
  - 8 rounds ensure ciphertext is random function of key and plaintext
  - Less than 16 rounds, plaintext attack more efficient than brute force
- Particular S-box design $\rightarrow$ non-linear, stand up to differential cryptanalysis
- Biggest criticism - small key space

DES Weak Keys

- 4 Weak keys
- 6 Semi-weak pairs
- 48 possibly weak keys

What is the key space of DES?

DES Weak Keys

56-bit key split in two halves, each half is shifted independently.

All ones or all zeros, or half ones and half zeros

Produce only 1 subkey for all rounds (minimises randomness)

0	0	0	0	0	0	0		0	0	0	0	0	0	0
0	0	0	0	0	0	0		F	F	F	F	F	F	F
F	F	F	F	F	F	F		0	0	0	0	0	0	0
F	F	F	F	F	F	F		F	F	F	F	F	F	F

DES Semi-weak key pairs

Produces only two subkeys

Come in pairs $\rightarrow$ both encrypt the same plaintext to same ciphertext

One key can decrypt messages made with the other key in the pair

DES possibly weak keys

Produces only four subkeys