

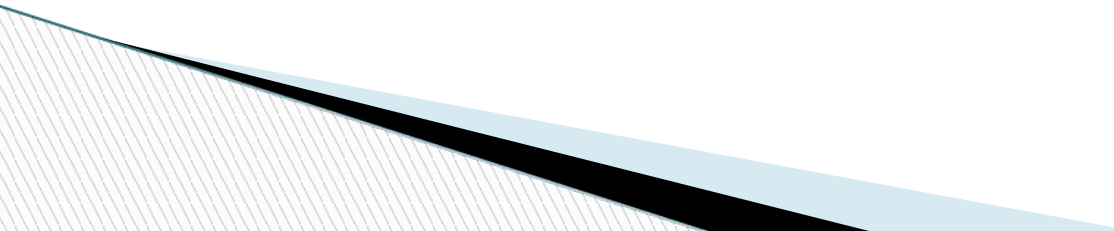
Module 2

Symmetric ciphers

Dept. of Telecommunication
DSCE



Modern Block Ciphers

- One of the most widely used types of cryptographic algorithms
 - Provide secrecy /authentication services
 - Focus on DES (Data Encryption Standard)
 - To illustrate block cipher design principles
- 

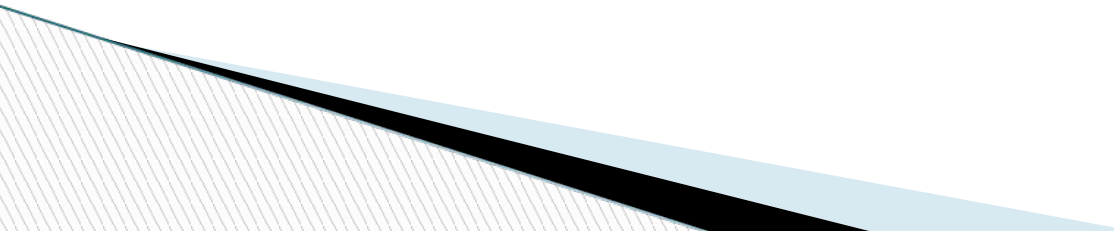
Block vs Stream Ciphers

- ❑ Block ciphers process messages in blocks, each of which is then en/decrypted
- ❑ Like a substitution on very big characters
 - 64-bits or more
- ❑ Stream ciphers process messages a bit or byte at a time when en/decrypting
- ❑ Many current ciphers are block ciphers
- ❑ Broader range of applications

Claude Shannon and Substitution-Permutation Ciphers

- Claude Shannon introduced idea of substitution-permutation (S-P) networks form basis of modern block ciphers
- S-P nets are based on the two primitive cryptographic operations seen before:
 - *substitution* (S-box)
 - *permutation* (P-box)
- Provide *confusion* & *diffusion* of message & key

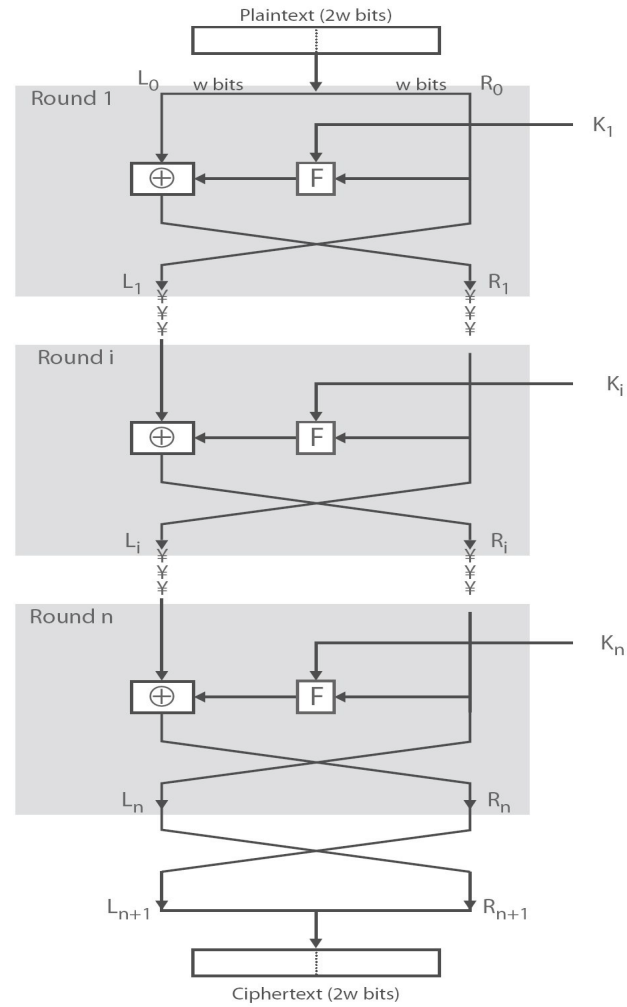
Confusion and Diffusion

- ❑ Cipher needs to completely obscure statistical properties of original message
 - ❑ A one-time pad does this
 - ❑ More practically Shannon suggested combining S & P elements to obtain:
 - ❑ **Diffusion** – dissipates statistical structure of plaintext over bulk of cipher text
 - ❑ **Confusion** – makes relationship between cipher text and key as complex as possible
- 

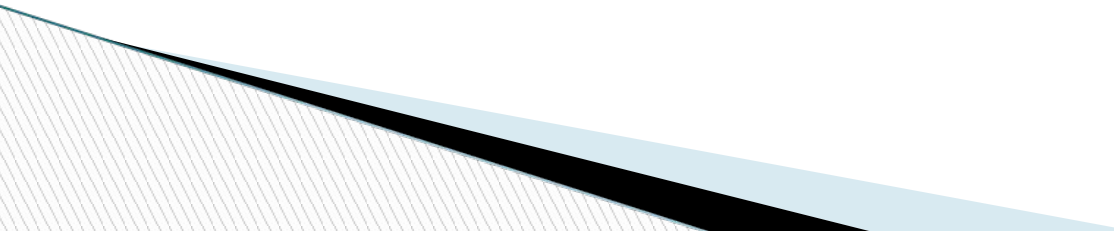
Feistel Cipher Structure

- Horst Feistel devised the **feistel cipher**
- Partitions input block into two halves
 - Process through multiple rounds which
 - Perform a substitution on left data half
 - Based on round function of right half & subkey
 - Then have permutation swapping halves
- Implements Shannon's S-P net concept

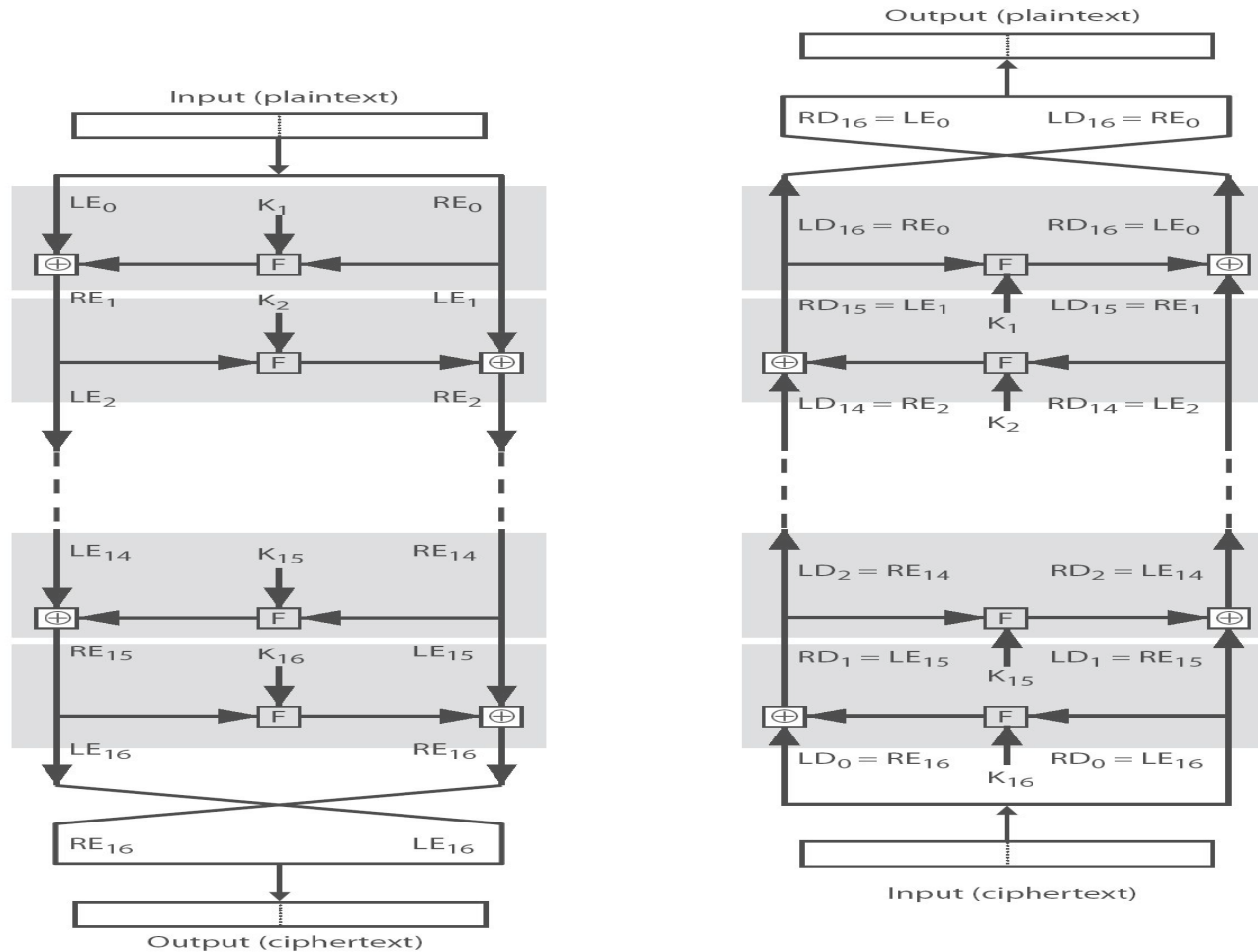
Feistel Cipher Structure



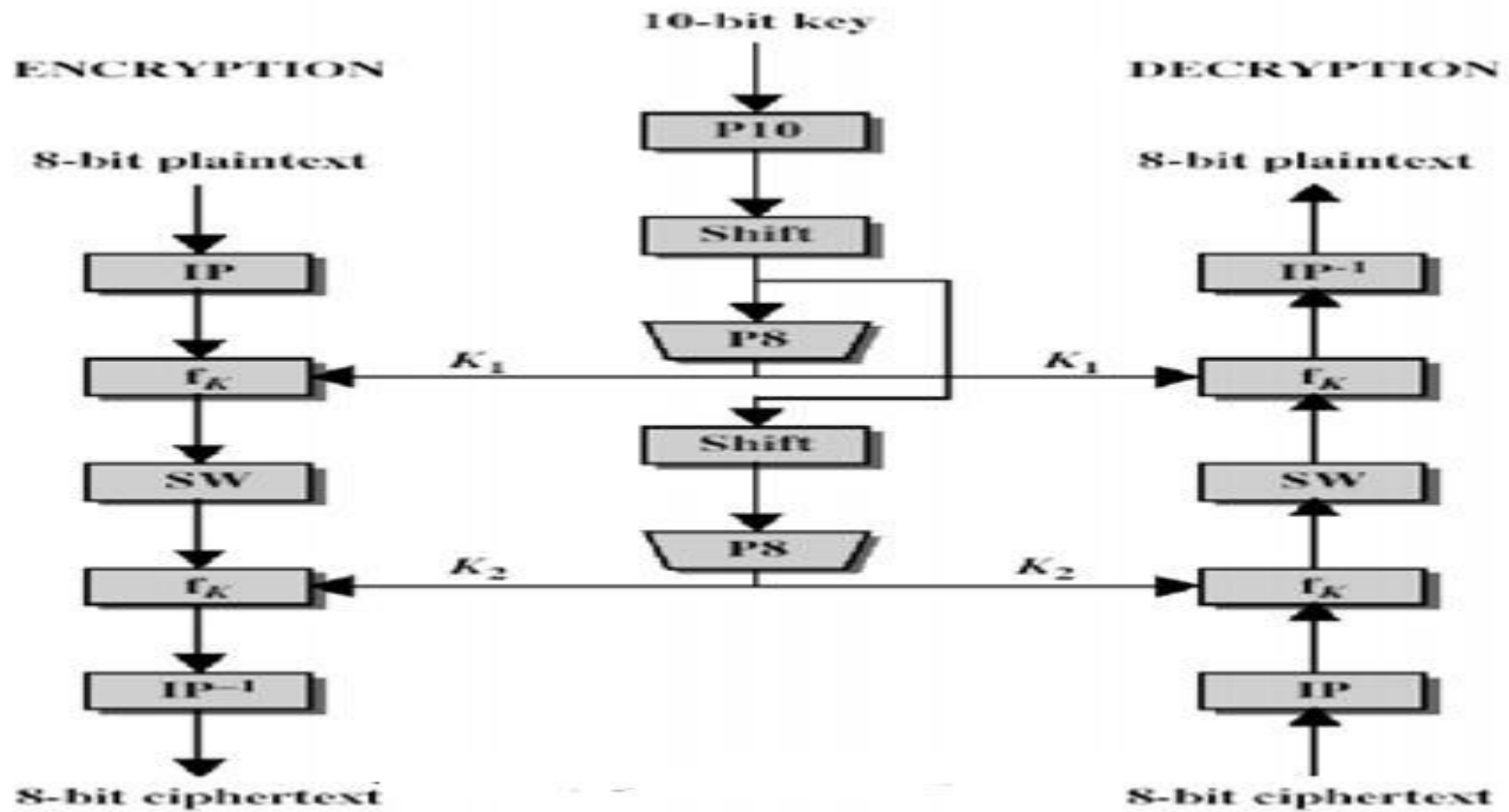
Feistel Cipher Design Elements

- Block size
 - Key size
 - Number of rounds
 - Sub key generation algorithm
 - Round function
- 

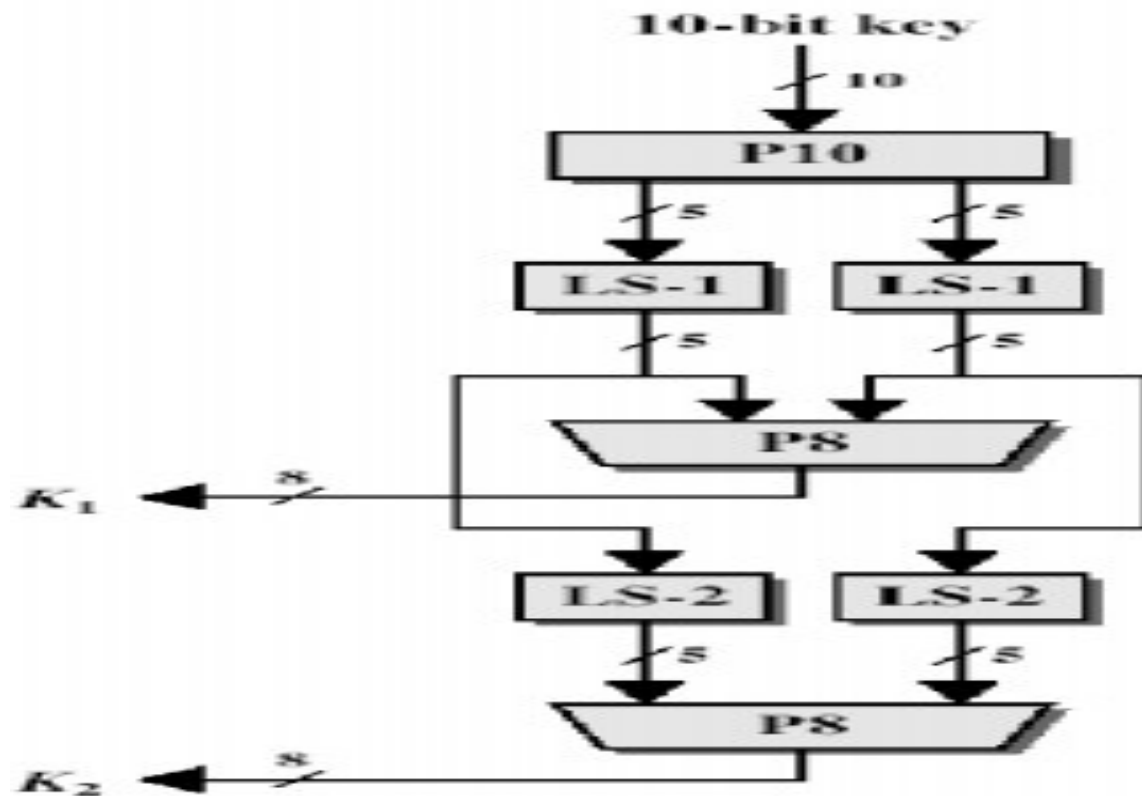
Feistel Cipher Decryption



S-DES



KEY GENERATION



S-DES ENCRYPTION

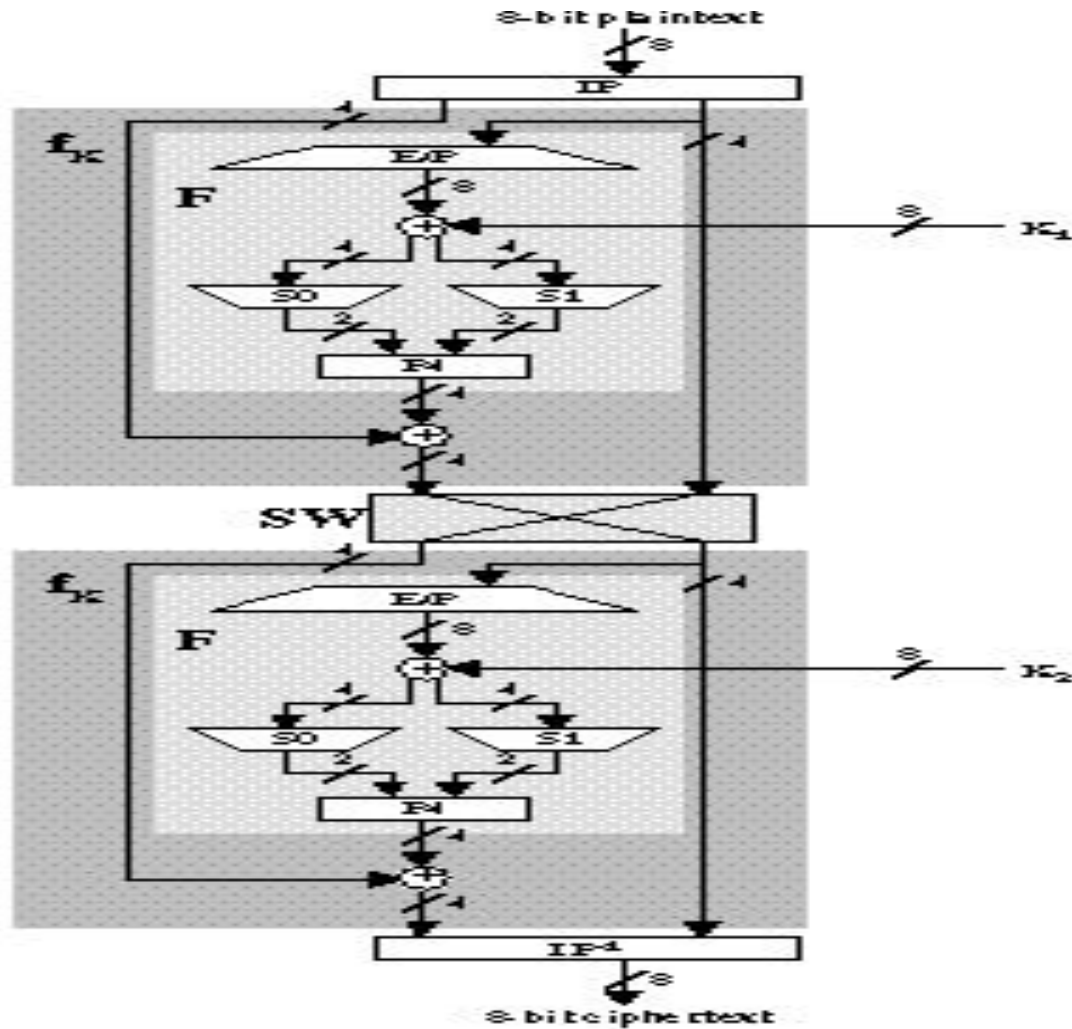
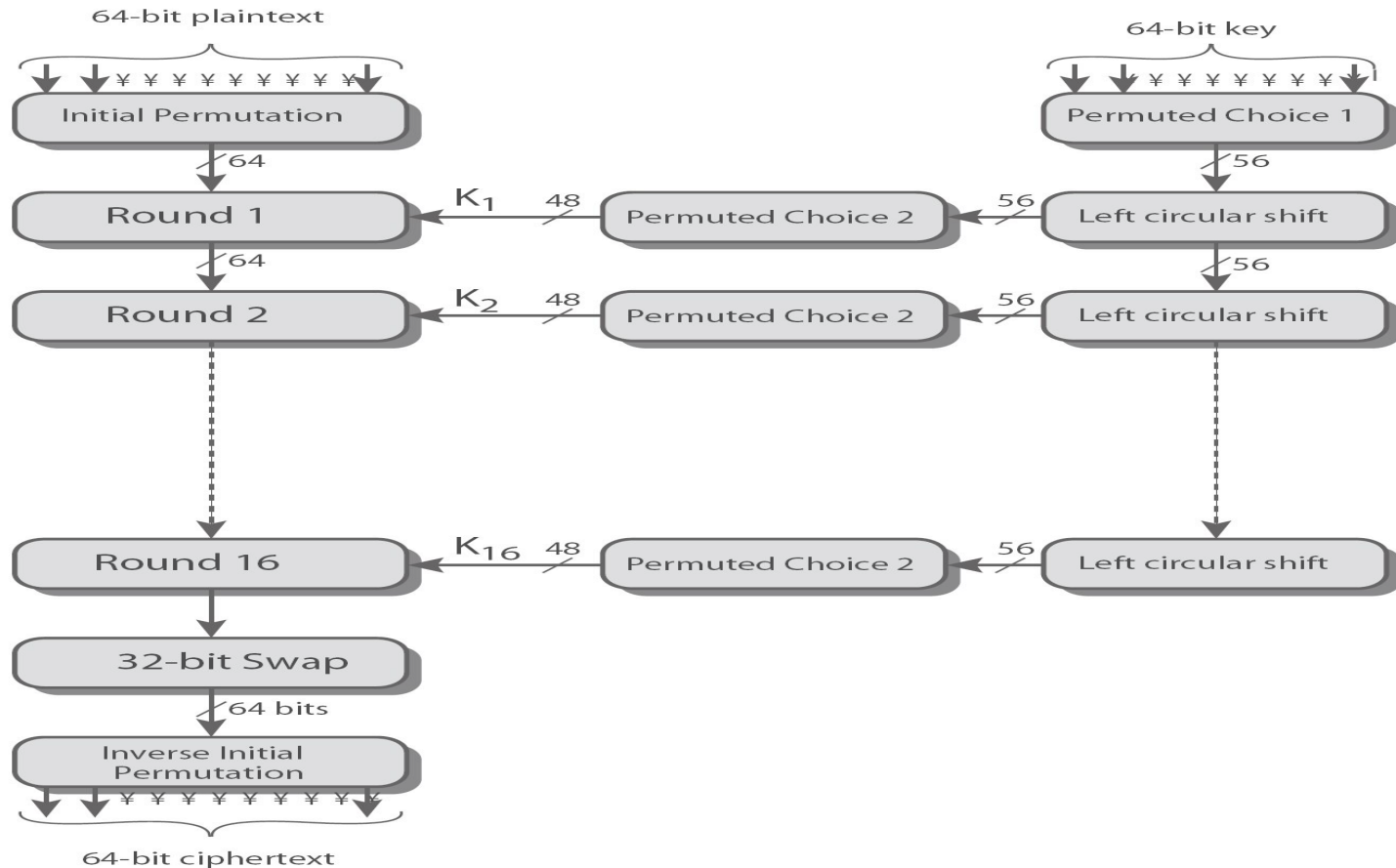


Figure 3.3 Simplified DES Encryption Detail

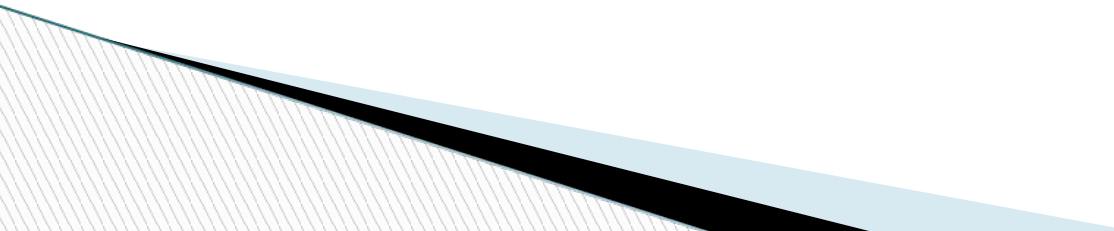
Data Encryption Standard (DES)

- ❑ Most widely used block cipher in world
- ❑ Adopted in 1977 by NBS (now NIST)
 - As FIPS PUB 46
- ❑ Encrypts 64-bit data using 56-bit key
- ❑ Has widespread use
- ❑ Has been considerable controversy over its security

DES Encryption Overview



Initial Permutation IP

- First step of the data computation
 - IP reorders the input data bits
 - Even bits to LH half, odd bits to RH half
 - Quite regular in structure (easy in h/w)
- 

DES Round Structure

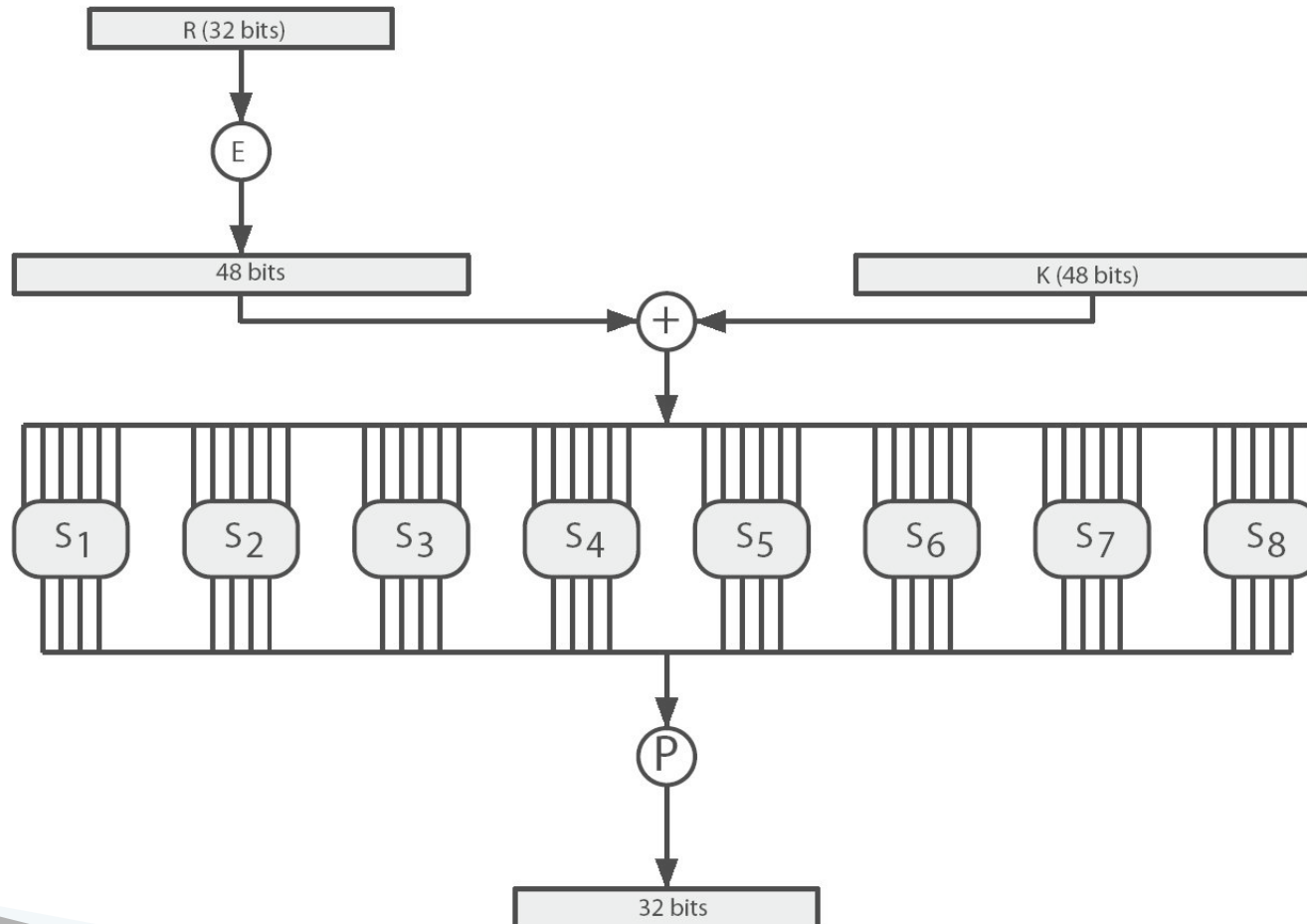
- Uses two 32-bit L & R halves
- As for any Feistel cipher can describe as:

$$L_i = R_{i-1}$$

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

- F takes 32-bit R half and 48-bit sub key:
 - Expands R to 48-bits using perm E
 - Adds to sub key using XOR
 - Passes through 8 S-boxes to get 32-bit result
 - Finally permutes using 32-bit perm P

DES Round Structure



Substitution Boxes S

- Have eight S-boxes which map 6 to 4 bits
- Each S-box is actually 4 little 4 bit boxes
 - outer bits 1 & 6 (**row** bits) select one row of 4
 - inner bits 2-5 (**col** bits) are substituted
 - result is 8 lots of 4 bits, or 32 bits
- Row selection depends on both data & key
 - feature known as autoclaving (autokeying)

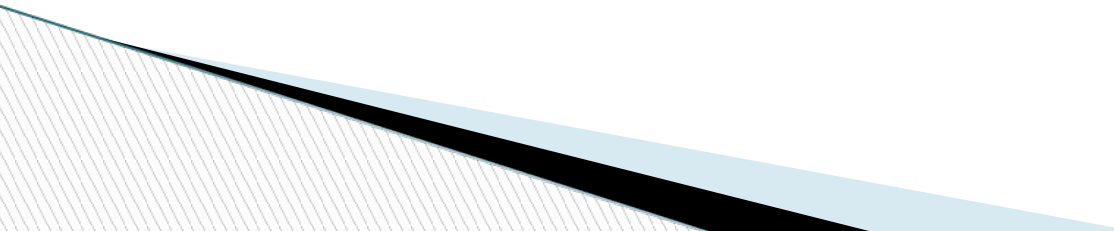
DES Key Schedule

- Forms subkeys used in each round
 - Initial permutation of the key (PC1) which selects 56-bits in two 28-bit halves
 - 16 stages consisting of:
 - rotating **each half** separately either 1 or 2 places depending on the **key rotation schedule K**
 - selecting 24-bits from each half & permuting them by PC2 for use in round function F

DES Decryption

- Decrypt must unwind steps of data computation
- With Feistel design, do encryption steps again using subkeys in reverse order (SK16 ... SK1)
 - IP undoes final FP step of encryption
 - 1st round with SK16 undoes 16th encrypt round
 - 16th round with SK1 undoes 1st encrypt round
 - Then final FP undoes initial encryption IP
 - Thus recovering original data value

Avalanche Effect

- Key desirable property of encryption algorithm
 - where a change of **one** input or key bit results in changing approx **half** output bits
 - DES exhibits strong avalanche
- 

Strength of DES – Key Size

- 56-bit keys have $2^{56} = 7.2 \times 10^{16}$ values
- brute force search looks hard
- recent advances have shown is possible
 - in 1997 on Internet in a few months
 - in 1998 on dedicated h/w (EFF) in a few days
 - in 1999 above combined in 22hrs!
- still must be able to recognize plaintext
- must now consider alternatives to DES

Strength of DES – Analytic Attacks

- Now have several analytic attacks on DES
- These utilise some deep structure of the cipher
 - by gathering information about encryptions
 - can eventually recover some/all of the sub-key bits
 - if necessary then exhaustively search for the rest
- Generally these are statistical attacks
- Include
 - differential cryptanalysis
 - linear cryptanalysis
 - related key attacks

Modes of Operation

- The way we use a block cipher is called its **Mode of operation** and five have been defined for the DES

▣ **Block Modes**

Splits messages in blocks

- 1) Electronic Codebook Book (ECB)
- 2) Cipher Block Chaining (CBC)

▣ **Stream Modes**

On bit stream messages

- 1) Cipher Block Chaining
- 2) Cipher Feedback Mode (CFB)
- 3) Counter Mode

AES

