Network Security and Cryptography
Symmetric-key cryptography

Lecture 2: Data Encryption Standard (DES)

Mark Ryan

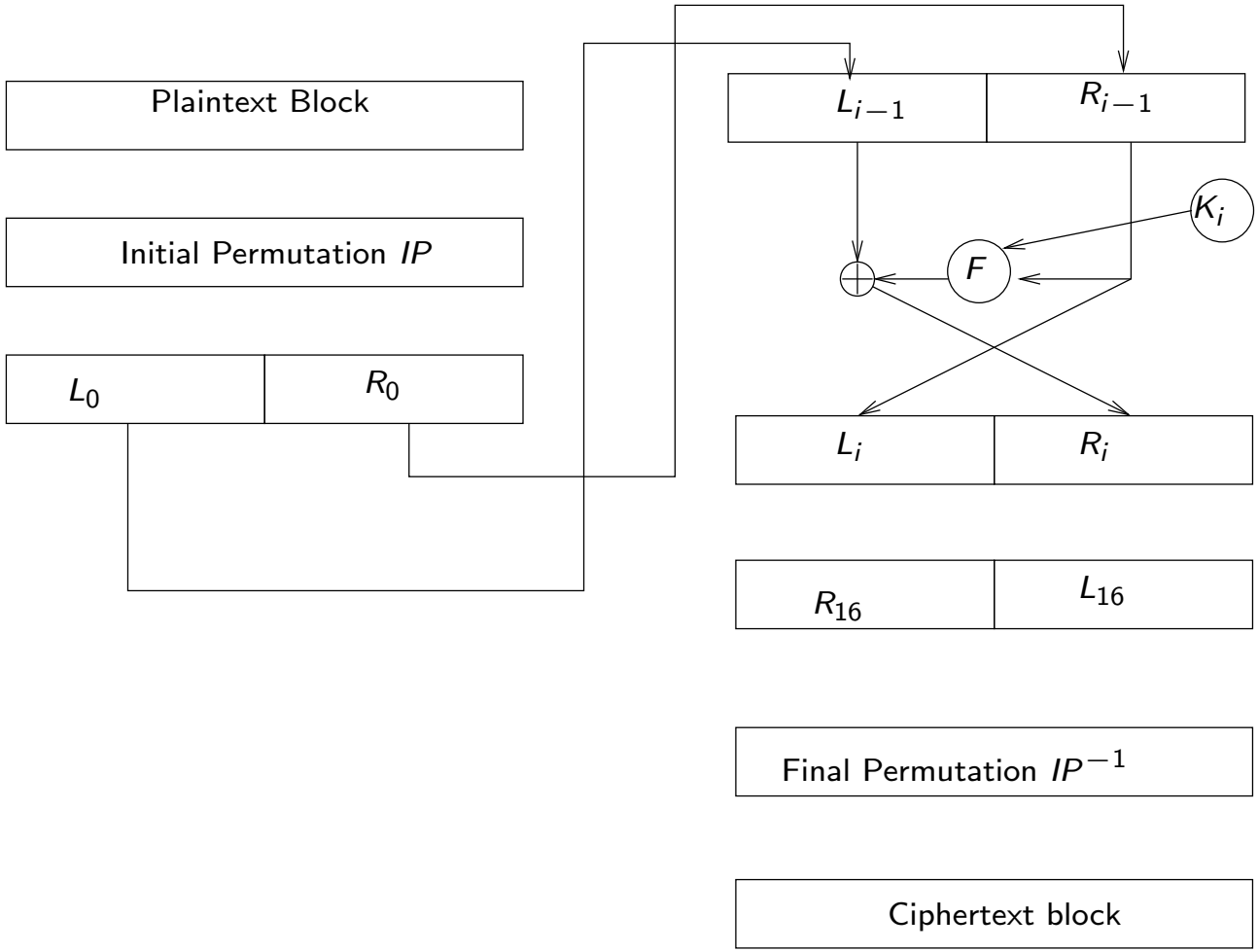
Data Encryption Standard (DES), adopted in 1976

Design parameters

- Block length is 64 bits
- Key length is is 56 bits
  - Actually, the key length is often said to be 64 bits. But 8 of those bits are parity bits. So the effective key length is 56 bits.
- DES consists of 16 "rounds". Each round uses a roundkey, also called a subkey, derived from the main key.

  Subkey length is 48 bits for each subkey $K_1, \ldots, K_{16}$. Subkeys are derived from the 56 bit key via the "key schedule".

Overview of DES



Notation for DES operations

Have three special operations:

- Cyclic shifts on bitstring blocks: Will denote by $b <<< n$ the move of the bits of block b by n to the left. Bits that would have fallen out are added at the right side of the b.
  $b >>> n$ is defined similarly
- Permutations on the position of bits: Written down as output order of the input bits.
  Example: the permutation $\boxed{4\ 1\ 2\ 3}$ means that
  - the fourth input bit becomes the first output bit,
  - the first input bit becomes the second output bit,
  - the second input bit becomes the third output bit, and
  - the third input bit becomes the fourth output bit.

  Sometimes, we use the word "permutation" for bit re-arrangements that include duplication or dropping of bits, even though that is not a proper permutation.

Key schedule

Have different keys for each round, computed by so-called *Key schedule*

64-bit key is actually 56-bit key plus 8 parity bits

- First apply a permutation PC-1 which removes the parity bits. This results in 56 bits.
- Split result into half to obtain (C_0, D_0)
- For each round $i = 1, ..., 16$, we compute

$$\begin{aligned} C_i &= C_{i-1} <<< p_i \\ D_i &= D_{i-1} <<< p_i \end{aligned}$$

where

$$p_i = \begin{cases} 1 & \text{if } i = 1, 2, 9, 16 \\ 2 & \text{otherwise} \end{cases}$$

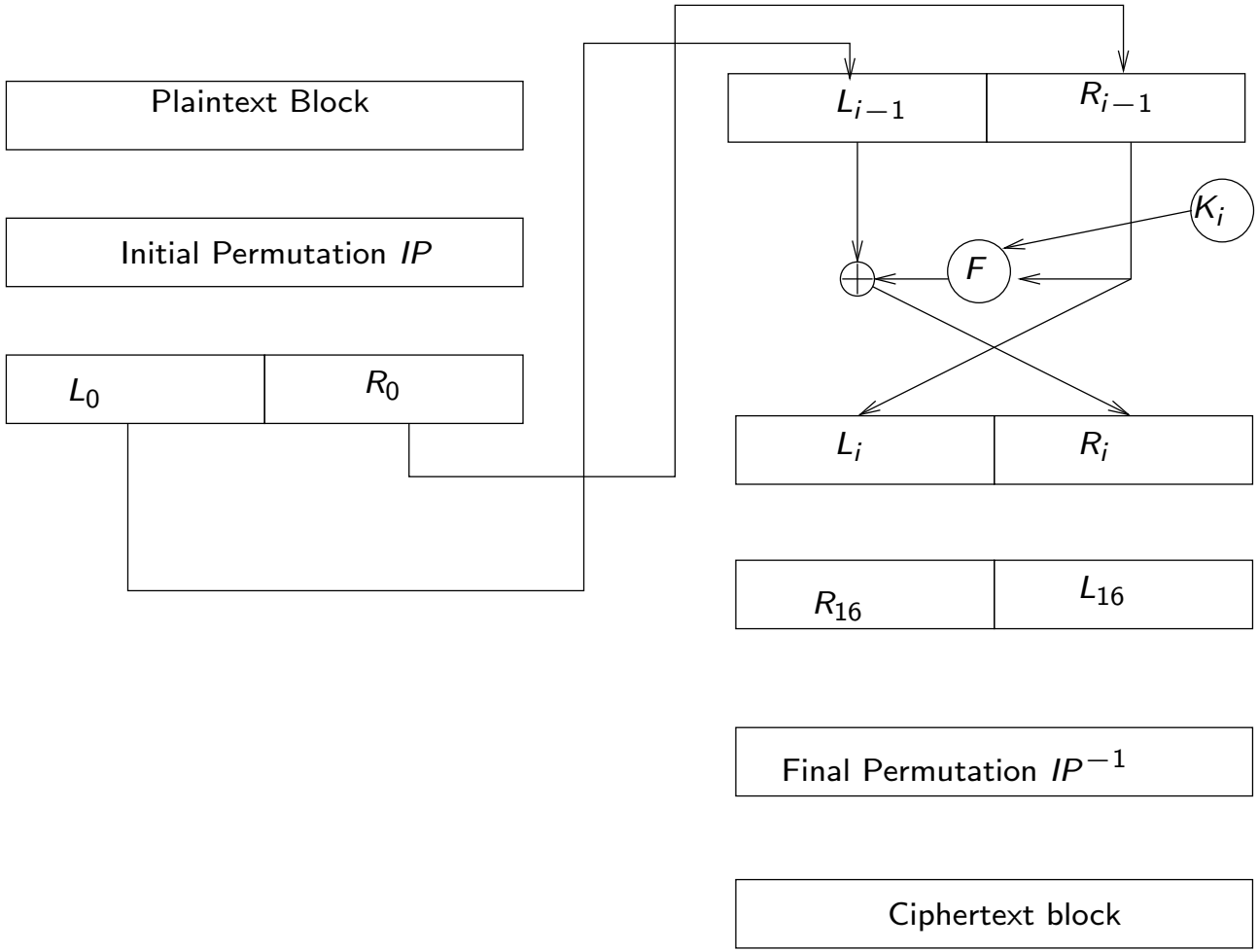
- Now we join C_i and D_i together, and apply a permutation PC-2 which produces a 48-bit output, to obtain K_i.

Feistel cipher: a way of doing block ciphers

Invented in 1971 at IBM
Important class of ciphers (eg Blowfish, DES, 3DES)
Same encryption scheme applied iteratively for several rounds
Important step: Derive next message state from previous message state via special function called *Feistel function*
Encryption is organised as a series of "rounds".
Each round works as follows:

- Split input in half
- Apply Feistel function to the right half
- Compute xor of result with old left half to be new left half
- Swap old right and new left half, unless we are in the last round

Overview of DES



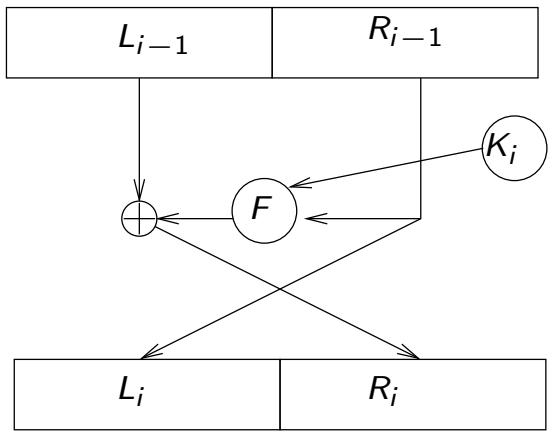
DES Feistel Cipher, continued

Formal definition:

- Split plaintext block in two equal pieces $M = (L_0, R_0)$
- For each round $i = 1, 2, \ldots, 16$ compute

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

- The ciphertext is $C = (R_{16}, L_{16})$



Decryption

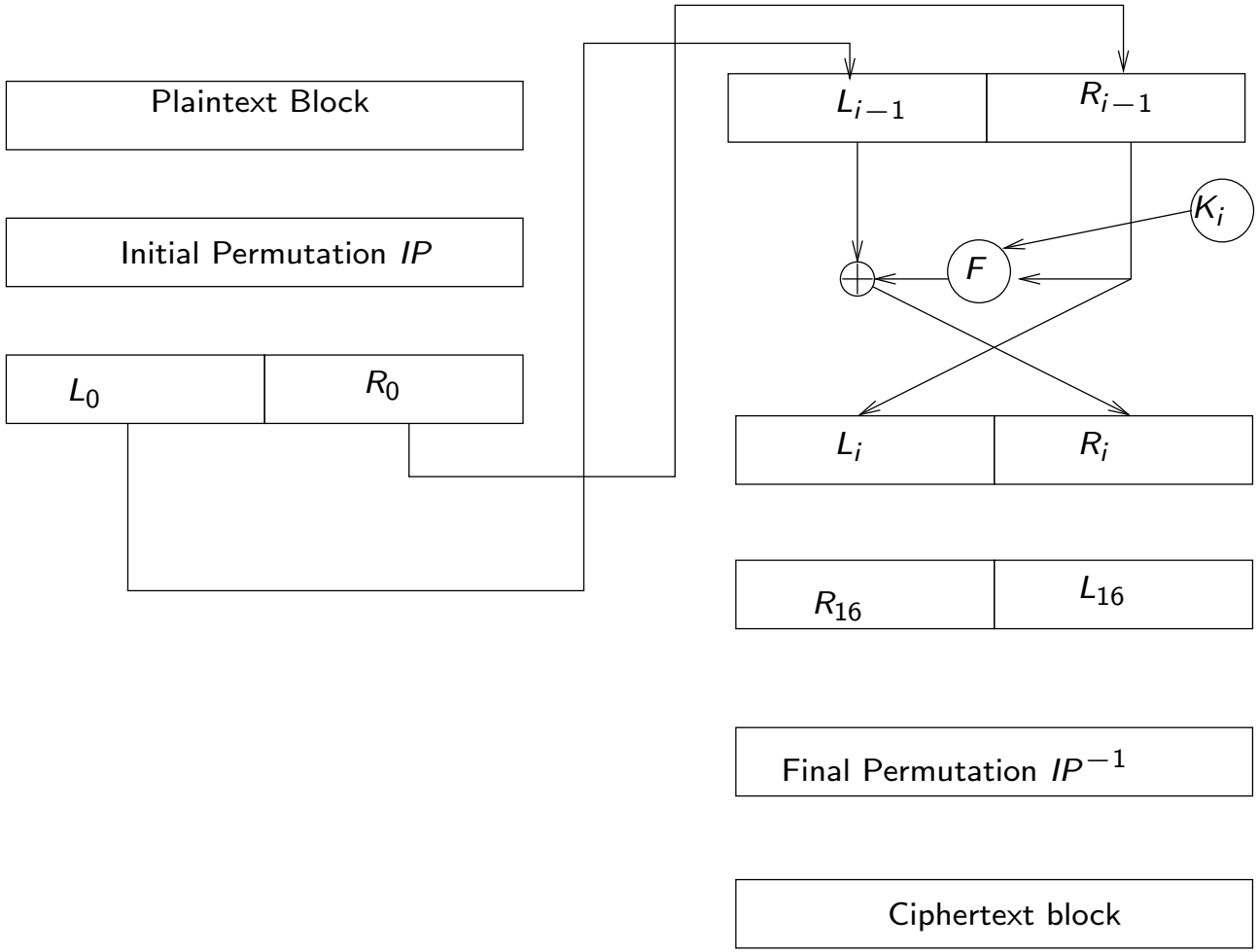
Works as encryption, but with a reversed order of keys

- Split ciphertext block in two equal pieces $C = (R_{16}, L_{16})$
- For each round $i = 16, 15, \ldots, 1$ compute

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

- Plaintext is $M = (L_0, R_0)$

Overview of DES

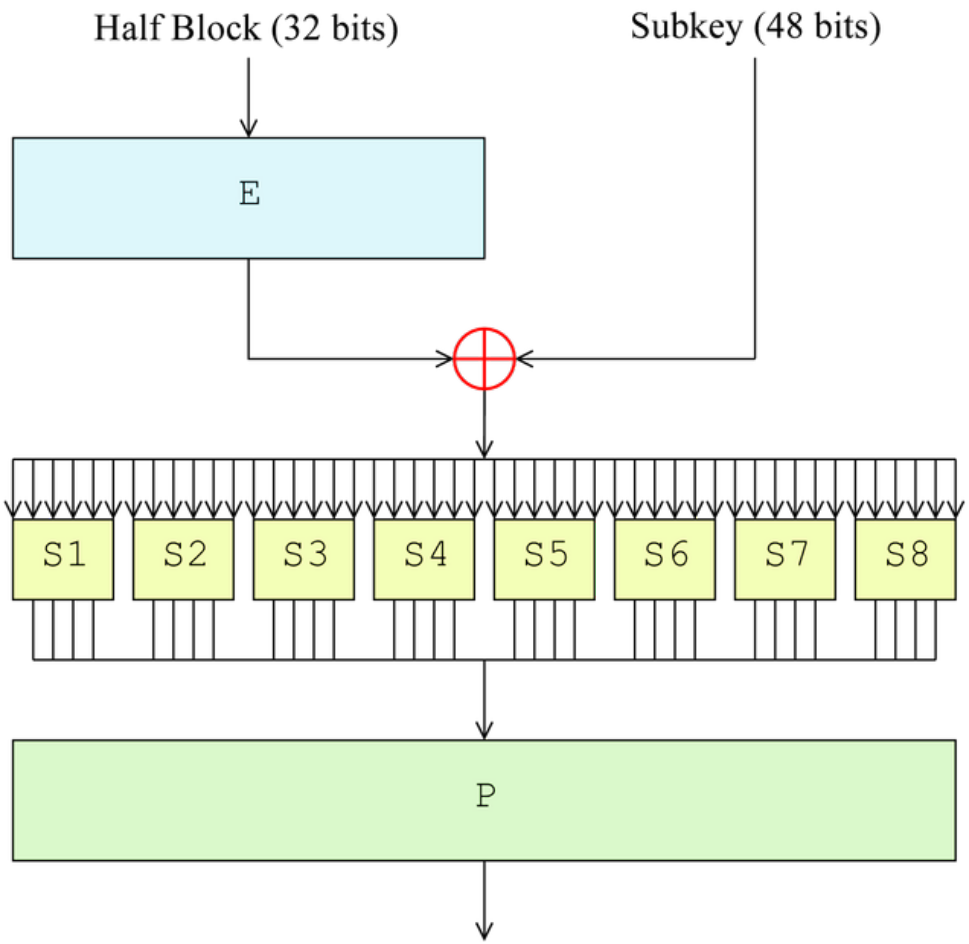


DES Feistel function

Four stage procedure:

- Expansion permutation: Expand 32-bit message half block to 48 bit block by doubling 16 bits and permuting them
- Round key addition: Compute xor of this 48 bit block with round key K_i
- S-Box: Split 48 bit into eight 6-bit blocks. Each of them is given as input to eight substitution boxes, which substitute 6-bit block by 4-bit block.
- P-Box: Combine these eight 4-bit blocks to 32-bit block and apply another permutation.

DES Feistel function, continued



Source: Wikipedia

S-boxes

- S-boxes: An S-box substitution is a table lookup. Input is 6 bit, output is 4 bit. Works as follows:
  - Strip out outer bits of input and join them. This two-bit number is the row index.
  - Four inner bits indicate column number.
  - Output is corresponding entry in table

Confusion and diffusion

The design of DES aims to provide confusion and diffusion.

- Confusion means that each bit of the ciphertext should depend on several parts of the key, obscuring the connections between the two.
- Diffusion means that if we change a single bit of the plaintext, then (statistically) half of the bits in the ciphertext should change.

A related property is "non-linearity". If a cipher has this property, it means that the ciphertext is not a "linear" combination of the key and the plaintext. (That would be weak. More precisely, it would be vulnerable to differential cryptanalysis.)

Permutations and XOR are linear operations. So some non-linear operations need to be used as well. The S-box of DES is a non-linear operation.

Choice of S-boxes

Because of their non-linearity, the S-boxes are the core of DES in terms of cryptographic strength.

Motivation for the choice of the particular S-boxes not known until 1990s. It includes the following constraints:

- No single output bit should be too close to a linear combination of the input bits.
- If two inputs to an S-box differ in exactly one bit, their outputs must differ in at least two bits.
- If two inputs to an S-box differ in the two middle bits, their outputs must differ in at least two bits.
- If two inputs to an S-box differ in their first two bits and are identical in their last two bits, the two outputs must be different.

Reminder: overview of DES