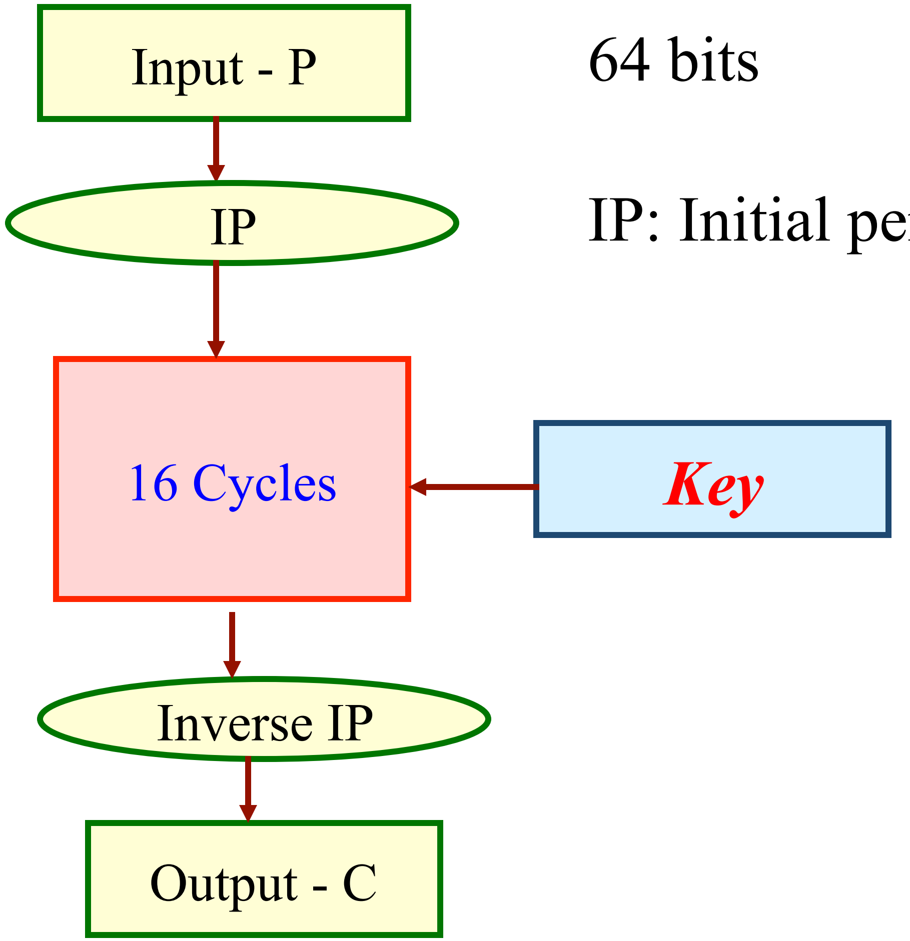
Background Knowledge of DES

Data Encryption Standard

- Combination of substitution and transposition
  - Repeated for 16 cycles
  - Provides confusion and diffusion
- *Product cipher*
  - Two weak but complementary ciphers can be made more secure by being applied together
- Symmetric-key block cipher (block size of 64bits)

A High Level Description of DES



64 bits

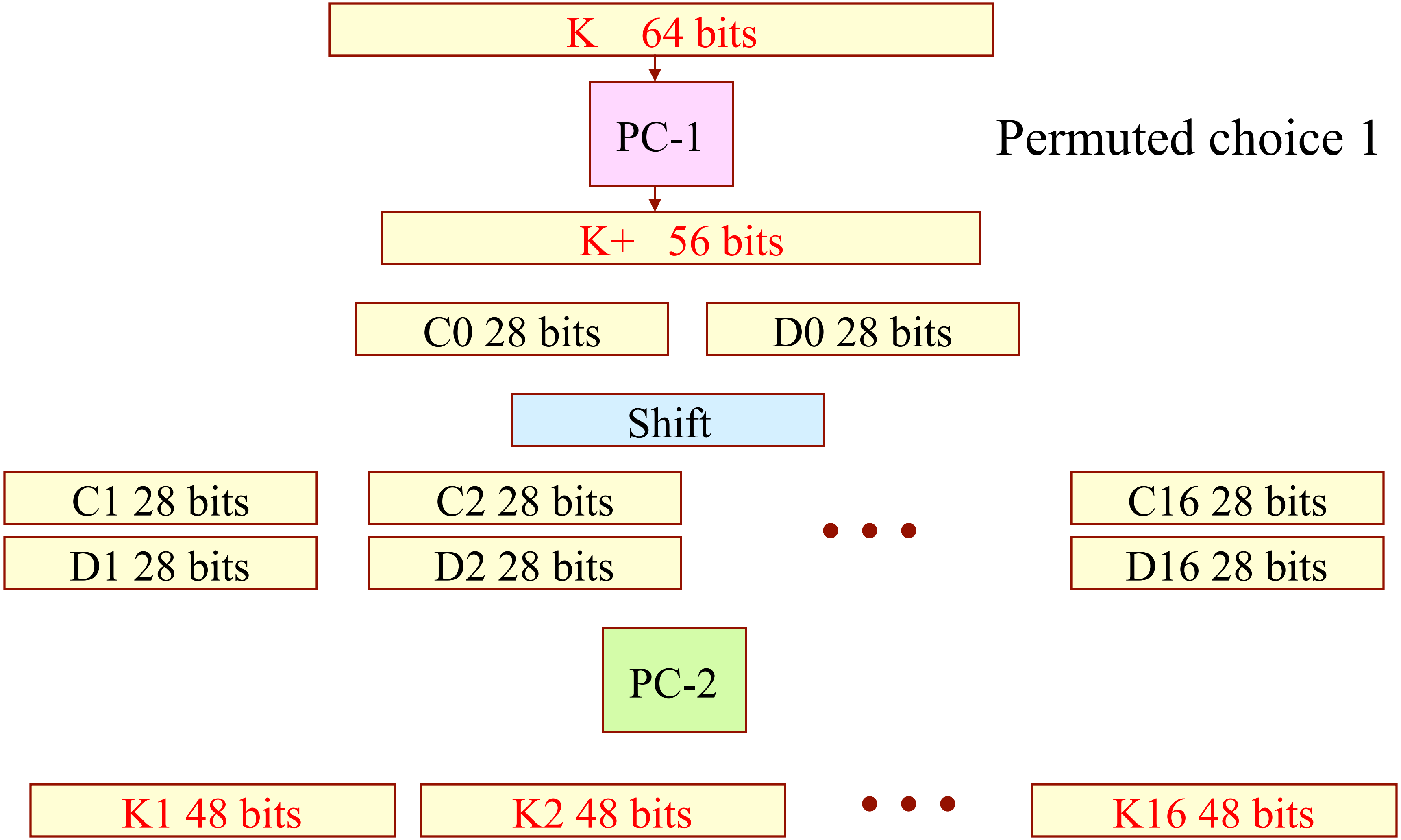
IP: Initial permutation

56 bits

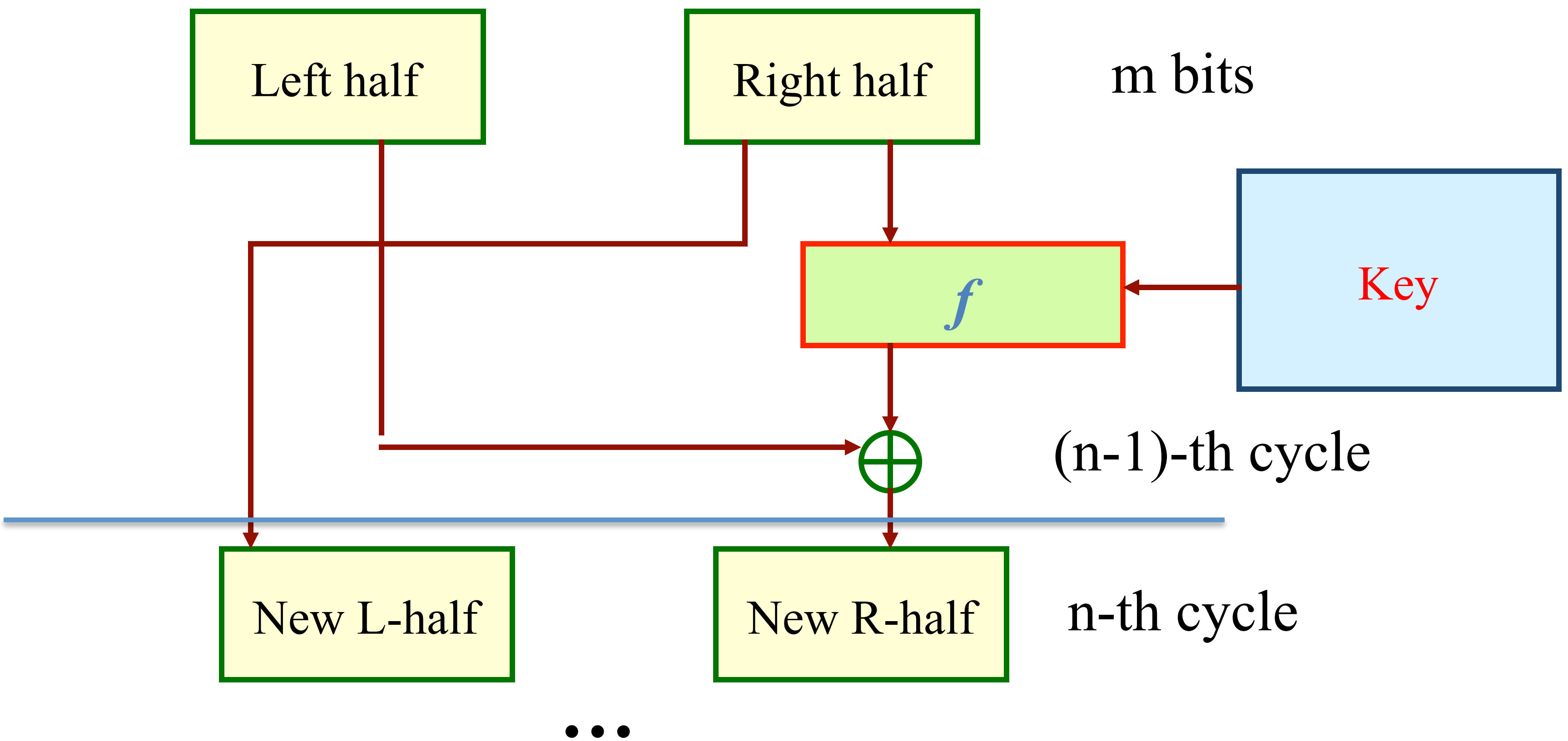
Key Schedule

- The process of deriving keys
- PC1 reduces 64bits -> 56 bits
- C16(enc) = C0(dec), D16(enc) = D0(dec)
- Modern ciphers have much more complex key schedule

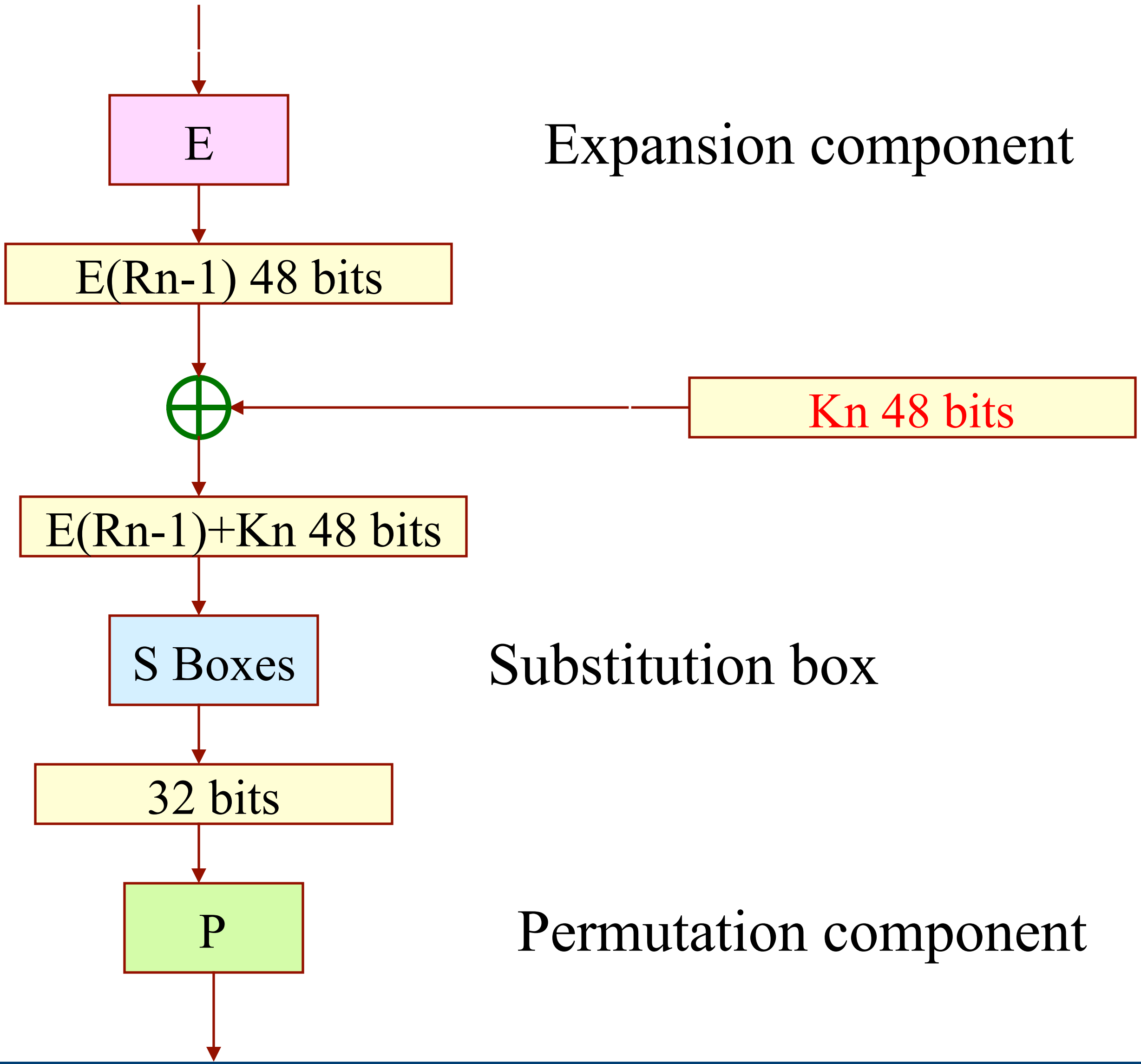
Key Summary


K 64 bits
PC-1
Permuted choice 1
K+ 56 bits
C0 28 bits
D0 28 bits
Shift
C1 28 bits
D1 28 bits
C2 28 bits
D2 28 bits
C16 28 bits
D16 28 bits
PC-2
K1 48 bits
K2 48 bits
K16 48 bits

A Cycle in DES



Summary of *f*



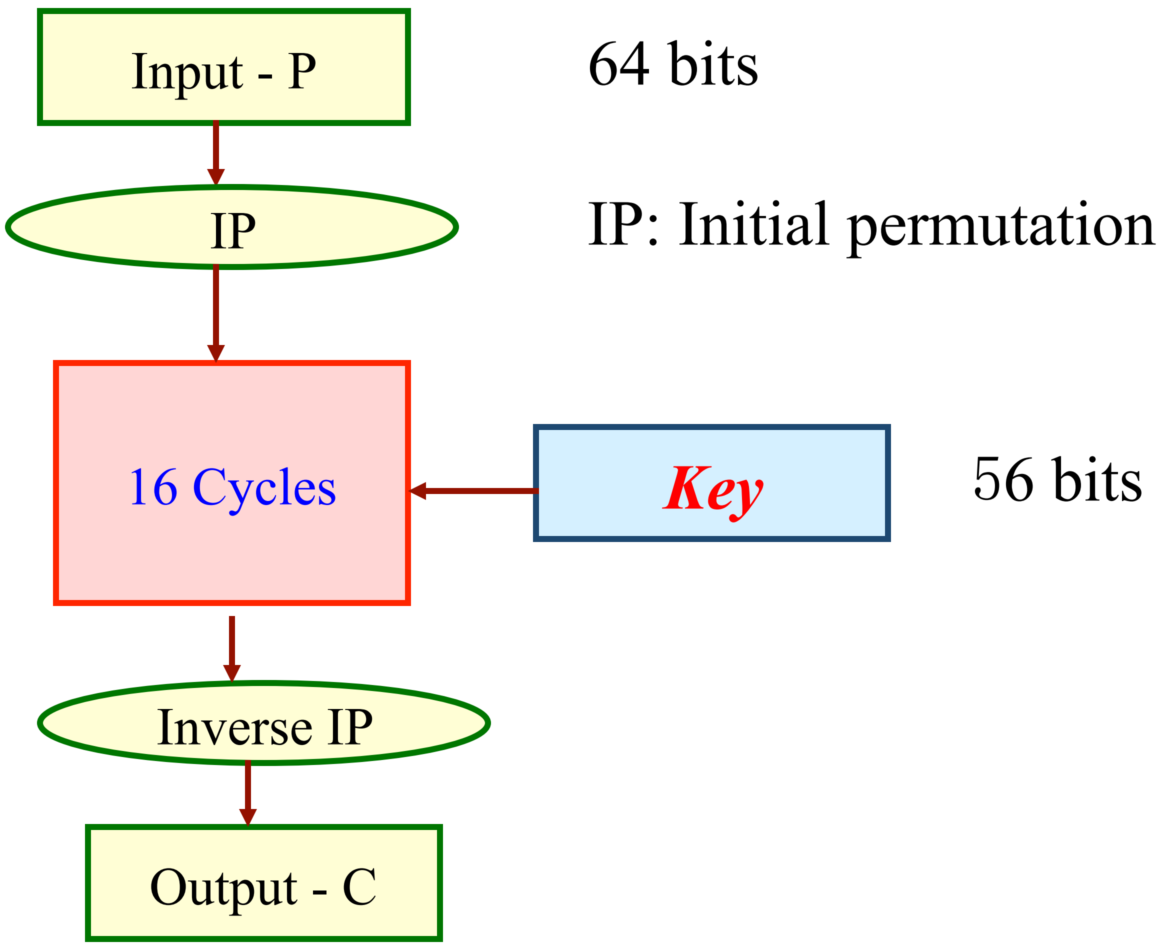
E
Expansion component
E(Rn-1) 48 bits
Kn 48 bits
E(Rn-1)+Kn 48 bits
S Boxes
Substitution box
32 bits
P
Permutation component

Decryption of DES

- The decryption process of DES is essentially the same as the encryption process
  - use the ciphertext as the input for decryption
  - use the subkey K_i in reverse order, i.e., use K_n in the first round, K_{n-1} in the second round…

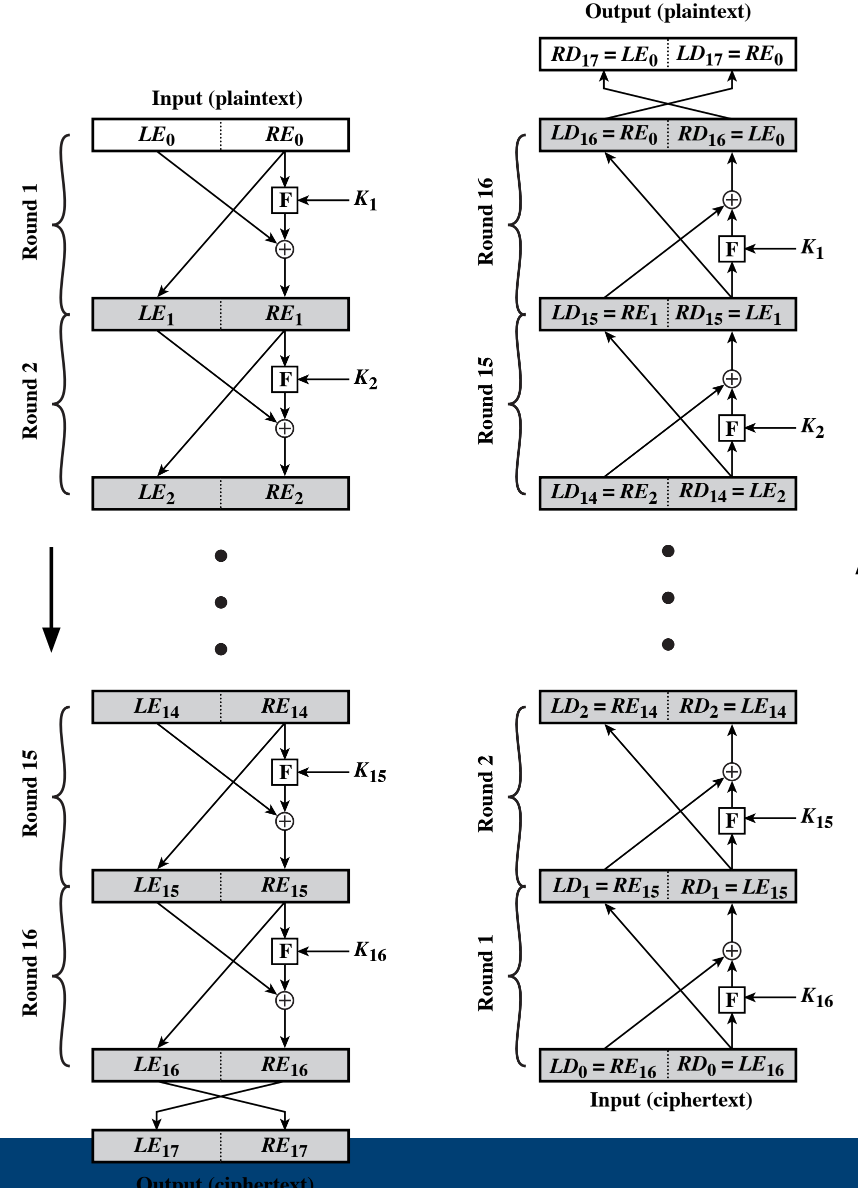
- Good property of this nice feature
  - don't need to implement two different algorithms

A High Level Description of DES



Prove the Correctness of Decryption

- If we can prove $LD_i = RE_{16-i}$ and $RD_i = LE_{16-i}$, then the decryption is correct



Background Knowledge of DES

- Developed in the early 1970s IBM; for the protection of sensitive, unclassified electronic government data
- The publication resulted in its quick international adoption and widespread academic scrutiny
- Proved by National Security Agency (NSA) and published in 1977

Background Knowledge of DES

- The heart of DES is the 16 cycles and f function
  - Expansion component (P)
  - S-boxes (S)
  - Permutation component (P)

Background Knowledge of DES

- Proposed the use of a cipher that alternates substitutions and permutations

Substitutions

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

Permutation

- No elements are added or deleted or replaced in the sequence, rather the order in which the elements appear in the sequence is changed

Avalanche Effect

- Avalanche effect means a small change in the plaintext (or key) should create a significant change in the ciphertext.
- Avalanche effect is the prime design criteria for any block cipher—why?
  - If the change of one bit from the input leads to the change of only one bit of the output, then it is easy to guess to find the input
  - E(1011)=1110; E(1001)=?

Background Knowledge of DES

- An example of avalanche effect

Plaintext: 0000000000000000 Key: 22234512987ABB23
Ciphertext: 4789FD476E82A5F1

Plaintext: 000000000000000<u>1</u> Key: 22234512987ABB23
Ciphertext: 0A4ED5C15A63FEA3

Background Knowledge of DES

- Objective of concatenating permutation and substitution in each cycle
  - Achieve avalanche effect

Background Knowledge of DES

- The number of cycles/rounds (why 16?)
  - A fact: only after eight rounds (on average, in DES), each ciphertext is a function of every plaintext bit and every key bit;

Rounds	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Bit differences	1	6	20	29	30	33	32	29	32	39	33	28	30	31	30	29

an example

Background Knowledge of DES

- The number of cycles/rounds (why 16?)
  - A fact: only after eight rounds (on average, in DES), each ciphertext is a function of every plaintext bit and every key bit;
  - However, DES with less than sixteen rounds are vulnerable to **known-plaintext** attacks
    - Known plaintext attack
    - Chosen plaintext attack

Background Knowledge of DES

- The objective of IP and inverse IP
  - Has no cryptographic significance in DES
  - The reason they are included in DES is not clear and has not been revealed by the DES designer
  - One guess is that DES was designed to be implemented in hardware, and these permutations may thwart a software simulation of the mechanism

Security of DES

- Cracking the DES
  - In 1980s, Diffie-Hellman outlined a "brute-force" attack on DES
    - By "brute-force" is meant that you try as many of the **256** (why?) possible keys to decrypt the ciphertext into a meaningful plaintext message
  - They estimated that it would cost $20m to build such device

Security of DES

- 2 types of attack
  - Analytical attacks
    - In 1975, people tried to crack DES.
    - In 1999, it was cracked by Eli Biham & Adi Shamir.
    - The attack was called Differential Cryptanalysis.
      - Requires 2^47 (x,y) pairs
      - Although better than brute-force, doesn't work in practice
    - The second attack was Linear Cryptanalysis.
      - Requires 2^43 (x,y) pairs
      - Still too high

Security of DES

- 2 types of attack
  - Brute-force attack
    - Given (X0, Y0) Check if $DES^{-1}_{Ki}(Y0) = X0$ where $i=0..2^{56}-1$

Security of DES

- 2 types of attack
  - Brute-force attack
    - In 1998, DeepCrack special-purpose DES hardware cracker was built
      - Could break DES in 4.5 days
      - Cost $220K
      - Used 27 boards each containing 64 chips
      - Was capable of testing 90 billion keys a second
      - On July 17, 1998, they announced they had cracked a 56-bit key in 56 hours
      - Official death of DES ☺

Security of DES

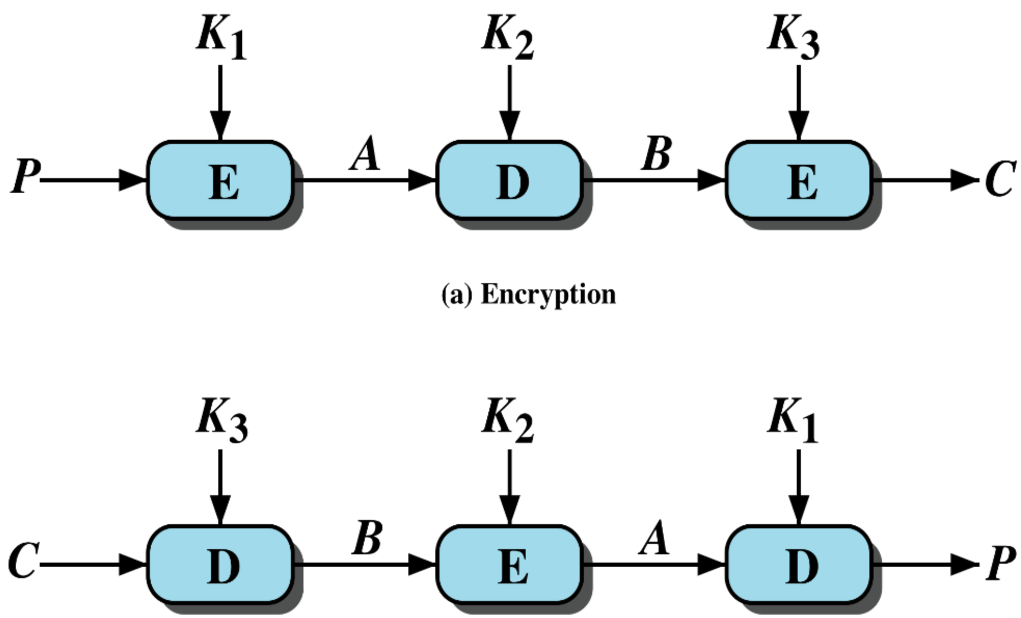
- 2 types of attack
  - Brute-force attack
    - In early 1999, Distributed. Net used the DES Cracker and a worldwide network of nearly 100K PCs to break DES in 22 hours
      - they were testing 245 billion keys per second
    - It has been shown that a dedicated hardware device with a cost of $1M (is much less in 2010) can search all possible DES keys in about 3.5 hours
    - This just serves to illustrate that any organization with moderate resources can break through DES with very little effort these days

Security of DES

- 2 types of attack
  - Brute-force attack
    - In 2007, Copacobana
      - Could break DES in 1.5 days
      - Cost $10K

Triple DES

- Triple-DES uses three keys and three executions of DES algorithm



(a) Encryption

(b) Decryption

Triple DES

- Keying options
  - Option 1: all three keys (K1, K2, K3) are independent: the strongest, with 3∗56=168 independent key bits
  - Option 2: K1 and K2 are independent, and K3=K1: provides less security with 2∗56=112 key bits, but stronger than pure DES
  - Option 3: all three keys are identical—equivalent of DES (why?)

Triple DES

- Attractions:
  - 168-bit (or 112-bit) key length overcomes the vulnerability to brute-force attack of DES
  - underlying encryption algorithm is the same as in DES
- Drawbacks:
  - algorithm is sluggish in software
  - uses a 64-bit block size

Data Encryption Standard (DES)

- DES is the most studied cipher in the world
- DES is unsecure today (key too short)
- 3DES is used in electronic passports
- 3DES is very secure

Alternatives to DES

- AES – defacto world standard
- 3DES – still very secure
- There are more than 200 block ciphers
- Requires time to be adopted
- AES finalists (5 algorithms)

AES

- Advanced encryption standard
  - 128, 192, 256 bit keys
  - similar level of computation complexity with DES
  - idea is similar to DES
  - widely used nowadays