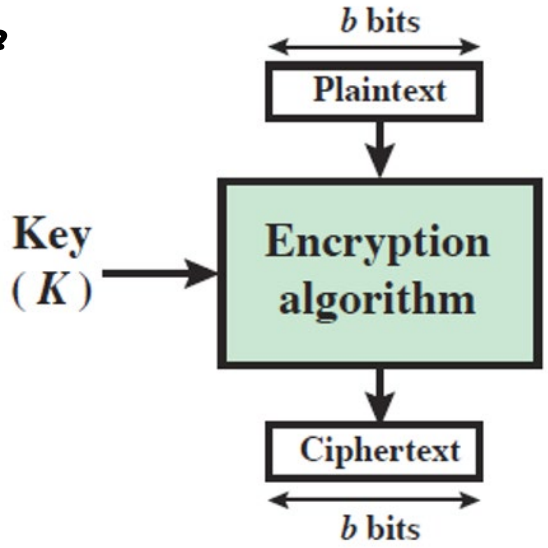
Chapter 3
Block Ciphers and the Data Encryption Standard

Abridged version

Block Ciphers

- Block ciphers process messages in blocks, each of which is then en/decrypted.
- Many current ciphers are block ciphers.
  - Better analysis
  - Broader range of applications

메시지를 block단위로 나눔



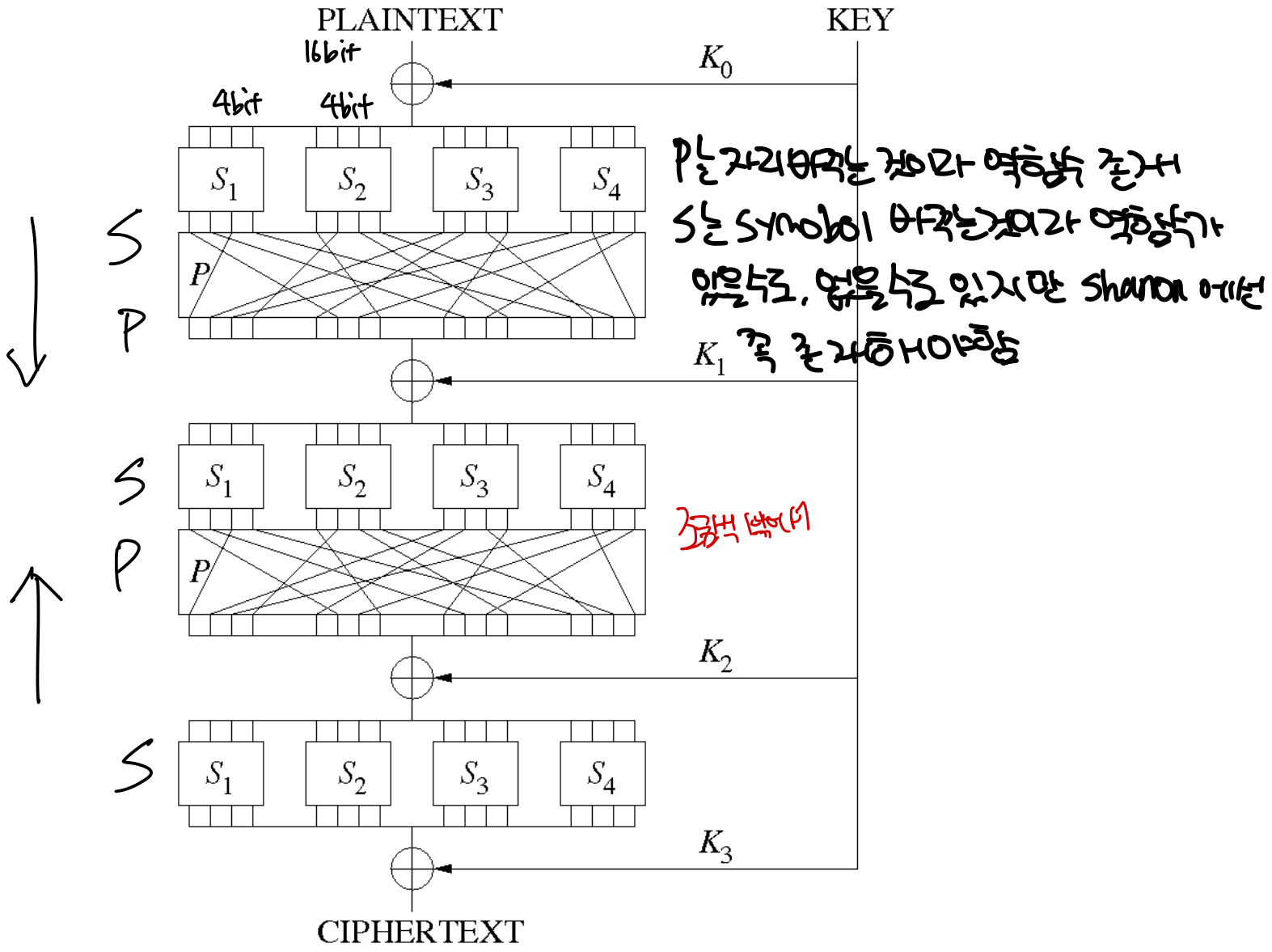
Shannon: Substitution-Permutation Ciphers

S-P

- Claude Shannon introduced the idea of substitution-permutation (S-P) networks in 1949 paper.
- S-P networks form basis of modern block ciphers.
- S-P networks are based on the two primitive cryptographic operations seen before:
  - Substitution (S-box)
  - Permutation (P-box)

S.P 연산이 있으면 섞어버자.

A 3-round Substitution-Permutation Network



Feistel Cipher Structure

- In Shannon's S-P networks, the S-boxes must be invertible.
- The Feistel network eliminates the requirement of that S-boxes be invertible.
- A Feistel network is thus a way of constructing an invertible function from non-invertible components.

Shannon은 invertible, reversible 하여야함. 역함수 찾을 필요 X

Feistel은 이것을 없애줌

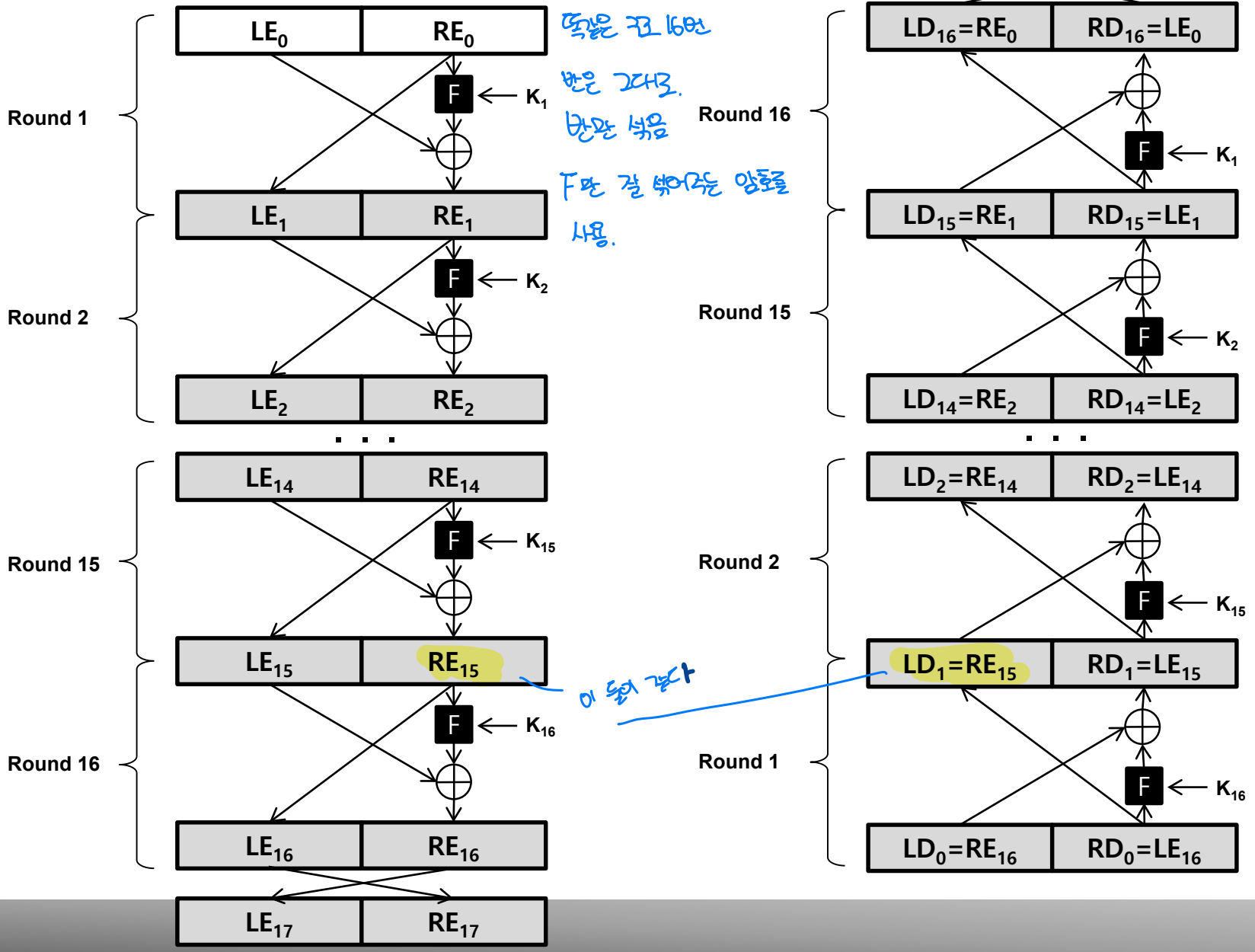
① 반반자르고, RE_0을 LE_1에 그대로 갖고옴.

② RE_0를 key에 집어 넣고, 나온 OUTPUT이랑 LE_0이랑 XOR해줌

③ 위과정을 16번 반복

결국 찾아야할것은 'F' function

Feistel Cipher Structure



Note

- XOR 성질 같은것이 들어오면 0
  - ✓ $A \oplus 0 = A$
  - ✓ $A \oplus A = 0$
  - ✓ If $A \oplus B = C$, then $A = B \oplus C$

B XOR 양변

- Encryption: $RE_{16} = LE_{15} \oplus F(RE_{15}, K_{16})$ 그대로 가져왔으니까 $LD_1 = RE_{15} = LE_{16} = RD_0$
- Decryption: $RD_1 = RE_{16} \oplus F(LE_{16}, K_{16})$
- $RE_{15} = LE_{16}$ 둘이 같음

대입

- $RD_1 = RE_{16} \oplus F(LE_{16}, K_{16})$
  $= LE_{15} \oplus F(RE_{15}, K_{16}) \oplus F(LE_{16}, K_{16})$
  $= LE_{15}$
  $\therefore RD_1 = LE_{15}$ 증명

↳ $LE_{15} \oplus F(LE_{16}, K_{16}) \oplus F(LE_{16}, K_{16})$
$= LE_{15} = RD_1$

Data Encryption Standard (DES)

- DES was adopted in 1977 by NBS (now NIST) as FIPS PUB 46
  - 64-bit data block with 56-bit key

key는 56bit. data block 64bit

- History

64-비트 2배증가가 아닌 2^64 증가

IBM에서 만든

  - In the late 1960s, IBM set up a research project led by Horst Feistel.
  - The project concluded in 1971 with the development of the Lucifer cipher.
  - Lucifer is a Feistel block cipher with 64-bit data block and 128-bit key.
    - redeveloped as a commercial cipher with input from NSA and others.
  - In 1973 NBS issued request for proposals for a national cipher standard.
  - IBM submitted their revised Lucifer which was accepted as the DES.
- Controversy over design

미국정보에서 DES 56 bit로 바꿈

  - DES 56-bit key vs. Lucifer 128-bit key.

이때서 정부인가들은 너무큼

  - Design criteria were classified (e.g., S-box).

이런걸 바꾸고. 공개. 이유는 비공개

Lucifer 식을 Revised (약간 줄이고정) 하고 56으로줄임.

DES Encryption Overview

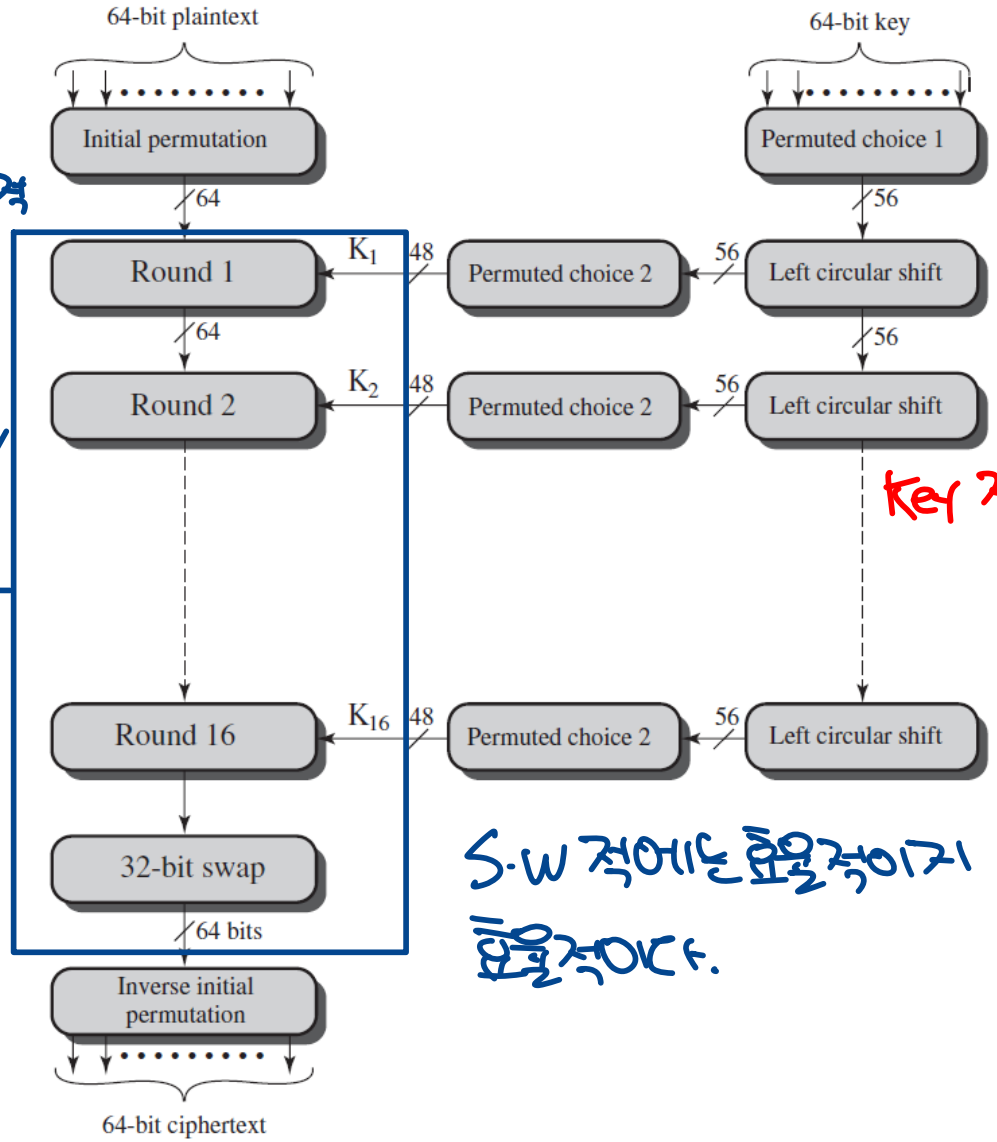


Figure 3.5 General Depiction of DES Encryption Algorithm

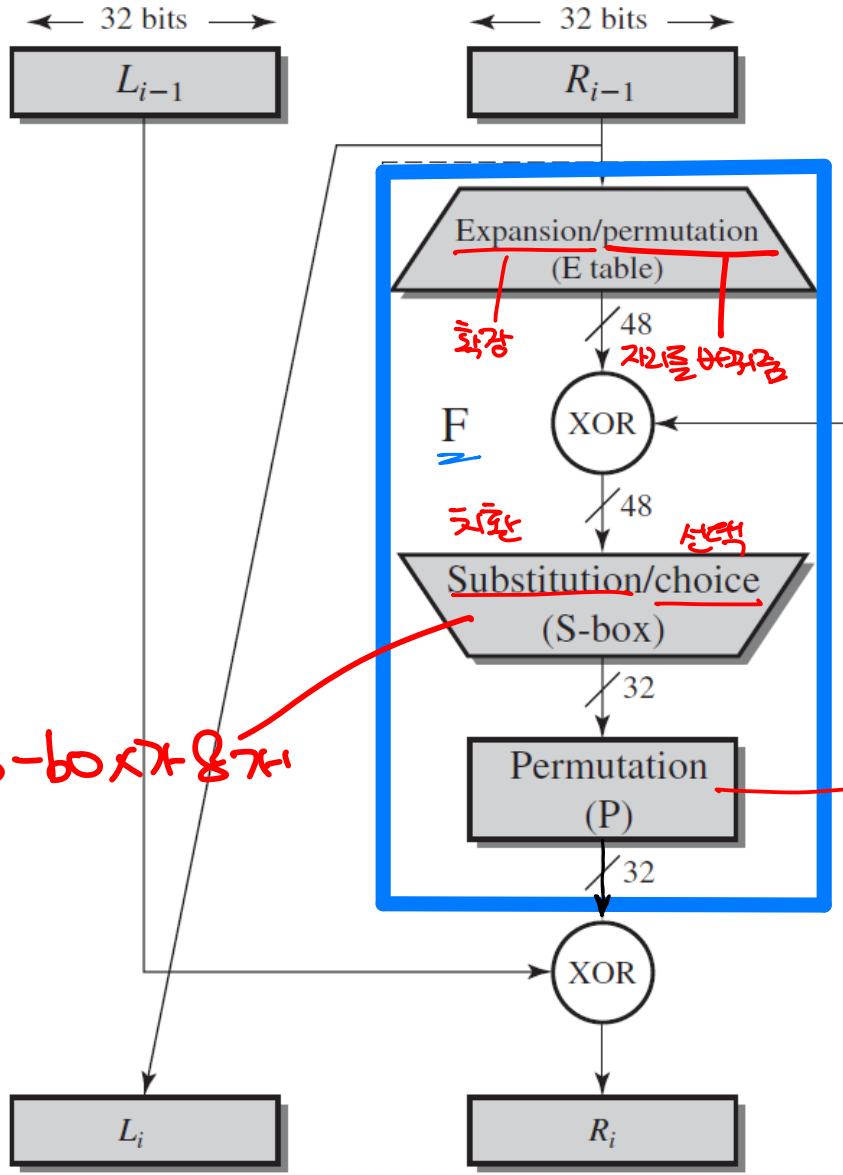
DES Round Structure

- DES uses two 32-bit L & R halves.
- As for any Feistel cipher, DES can be described as:
  - $L_i = R_{i-1}$
  - $R_i = L_{i-1} \oplus \mathrm{F}(R_{i-1}, K_i)$

DES. Fiestel 구조를 설명하는 식

- F takes 32-bit R half and 48-bit subkey:
  - expands R to 48-bits using expansion permutation E
  - adds to subkey using XOR
  - passes through 8 S-boxes to get 32-bit result
  - finally permutes using 32-bit permutation P

Single Round of DES



- F function

비트수가 같아야 XOR 할수있으므로 key와 message 비트수가 다름, message를 48 bit로 늘림.

S-box 1개당 6개의 입력, 4개의 출력
ex) 11011 빨간색은 row, 파란색은 column설정

Brute-Force Attack

- Brute-force attack 무식하게 힘으로 깨는 공격
  - For any cipher, the most basic method of attack is brute force—trying every possible key in turn. The length of the key determines the number of possible keys, and hence the feasibility of this approach.

  2^{56} 번

- EFF's DES-cracker 더이상 DES는 안전하지 않다
  - In 1998, a custom DES-cracker was built by the Electronic Frontier Foundation (EFF), a cyberspace civil rights group, at the cost of approximately US$250,000.
  - The machine brute-forced a key in a little more than 2 days' worth of searching.

    2일정도면 풂

    EFF - 개인의 권리를 지켜주는 민간단체

Brute-Force Attack

- Brute-force attack
  - For any cipher, the most basic method of attack is brute force—trying every possible key in turn. The length of the key determines the number of possible keys, and hence the feasibility of this approach.

- EFF's DES-cracker
  - In 1998, a custom DES-cracker was built by the Electronic Frontier Foundation (EFF), a cyberspace civil rights group, at the cost of approximately US$250,000.
  - The machine brute-forced a key in a little more than 2 days' worth of searching.

Brute-Force Attack

- Brute-force attack
  - For any cipher, the most basic method of attack is brute force—trying every possible key in turn. The length of the key determines the number of possible keys, and hence the feasibility of this approach.

- EFF's DES-cracker
  - In 1998, a custom DES-cracker was built by the Electronic Frontier Foundation (EFF), a cyberspace civil rights group, at the cost of approximately US$250,000.
  - The machine brute-forced a key in a little more than 2 days' worth of searching.