blowfish

송민호

유튜브 : https://youtu.be/xXvMs87E8NU

한성대학교 HANSUNG UNIVERSITY

CryptoCraft LAB

blowfish

- 1993년 브루스 슈나이어(Bruce Schneier)가 설계한 키 방식의 대칭형 블록암호
  - DES 대안으로 개발한 **대칭키 알고리즘**

- **퍼블릭 도메인**
  - 슈나이어가 누구든 자유로이 사용할 수 있다고 선언
  - Blowfish가 공개되었을 당시에 다른 알고리즘들은 기밀사항이나 특허였음

- 소프트웨어에서 양호한 암호화 속도를 제공

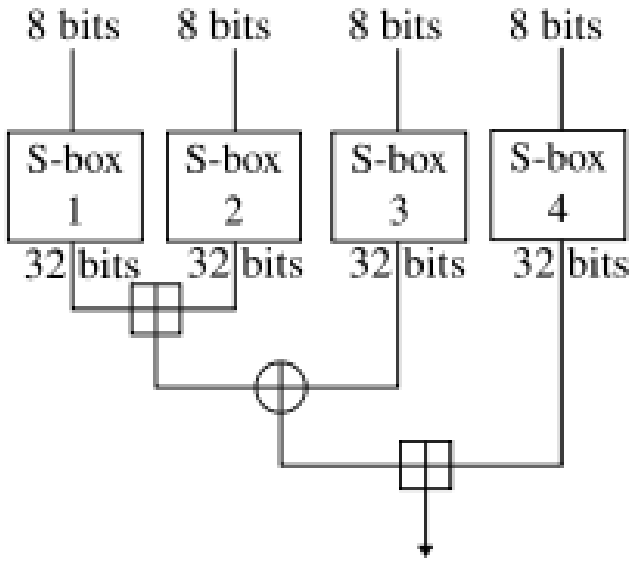
- 주요기능 : 키 의존 Sbox, 더 복잡한 키 스케줄

blowfish

- 64비트 블록 크기, 32비트 ~ 448비트에 이르는 가변 키 길이 사용

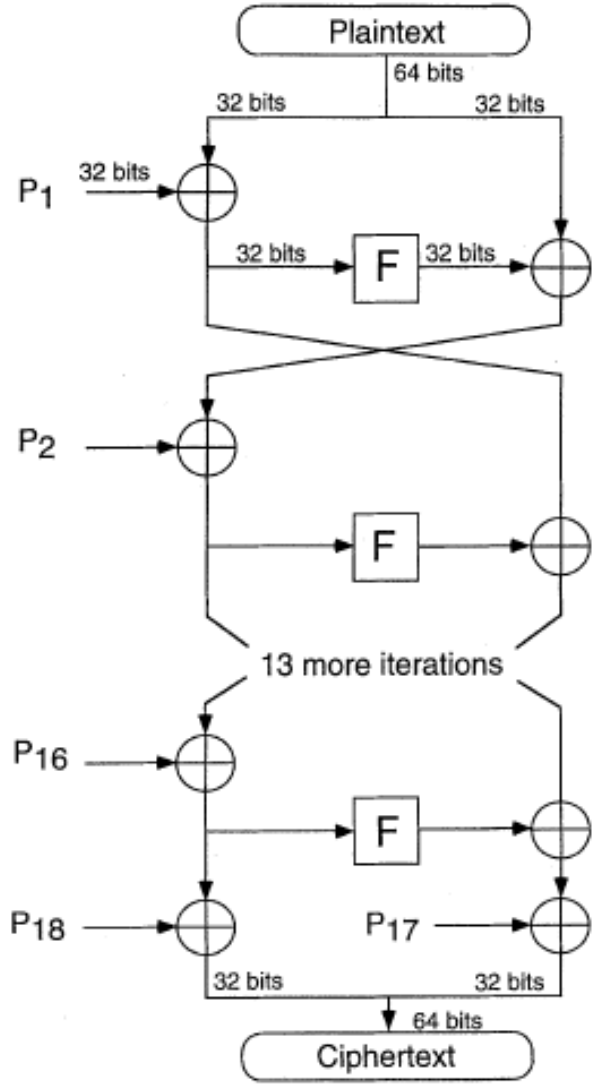
- 16라운드 **파이스텔 구조** 암호
  - 파이스텔 구조 : 데이터를 두 부분으로 나누어 좌, 우 두 부분에 교대로 비선형 변환을 적용시키는 구조

  - 치환(Substitution), 순열(Permutation)을 번갈아 수행하는 구조

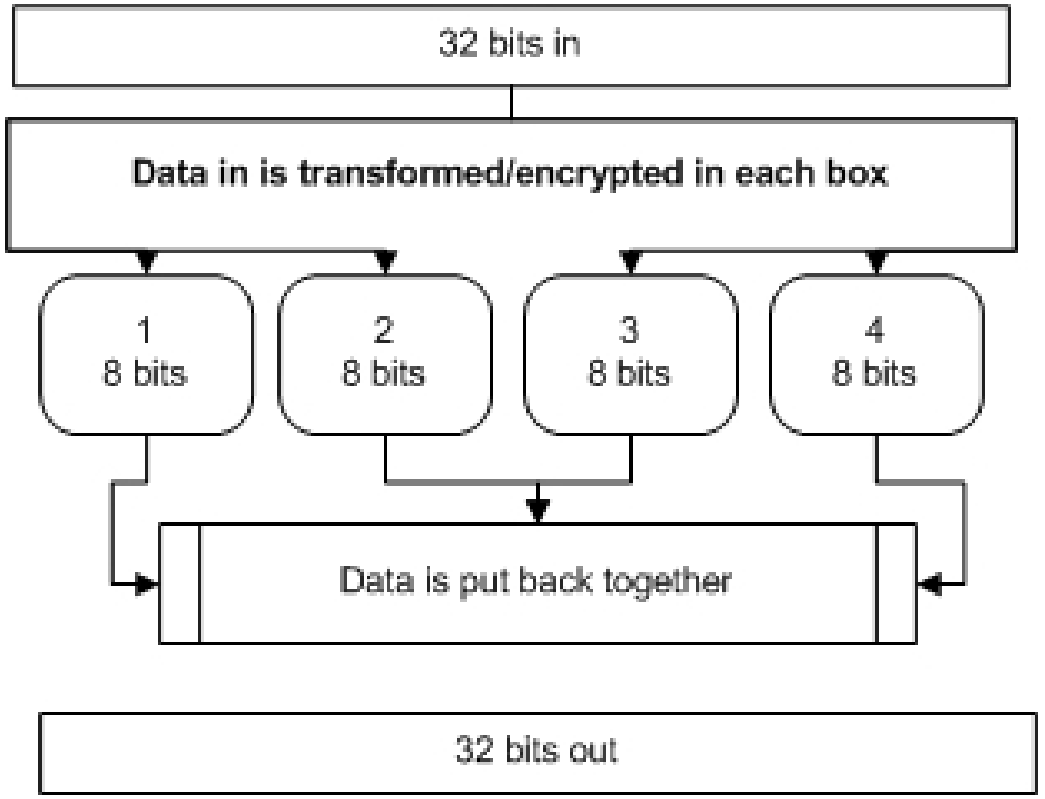


Blowfish의 파이스텔 암호 함수

blowfish 구조



Blowfish 전체 구조



Blowfish 32 bits 연산

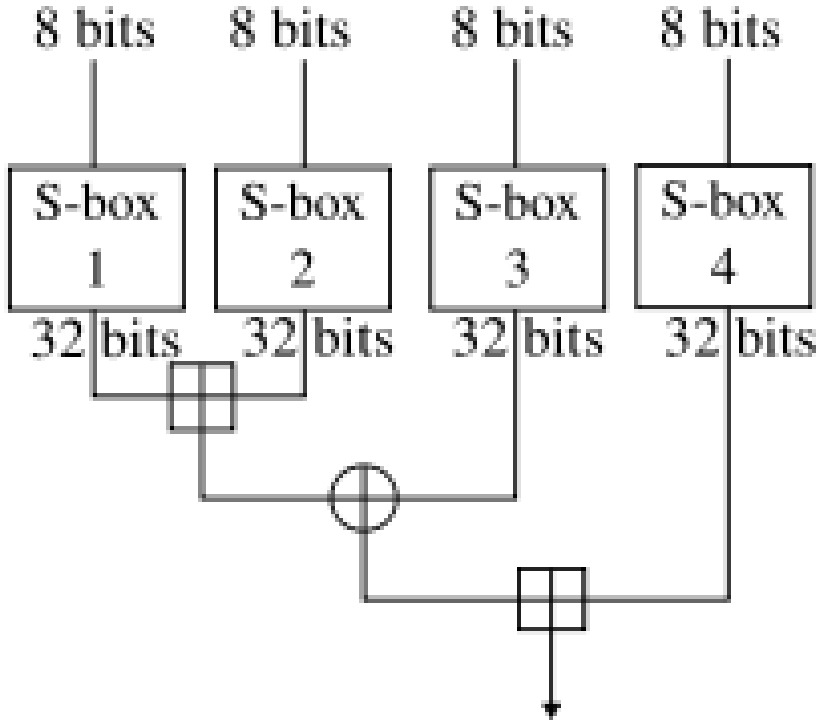
blowfish 장점

- **빠른 속도**
  - 32비트 마이크로 프로세서에서 1 바이트당 18클럭 사이클의 속도
  - RC5, DES, IDEA보다 빠름
- **간결성**
  - 5K 이내의 메모리에서 실행될 수 있음
- **단순성**
  - 간단한 구조는 구현이 쉽고 알고리즘의 강도 결정이 쉬움

- **기본 연산 2가지**
  - 덧셈 연산
  - 비트 XOR연산

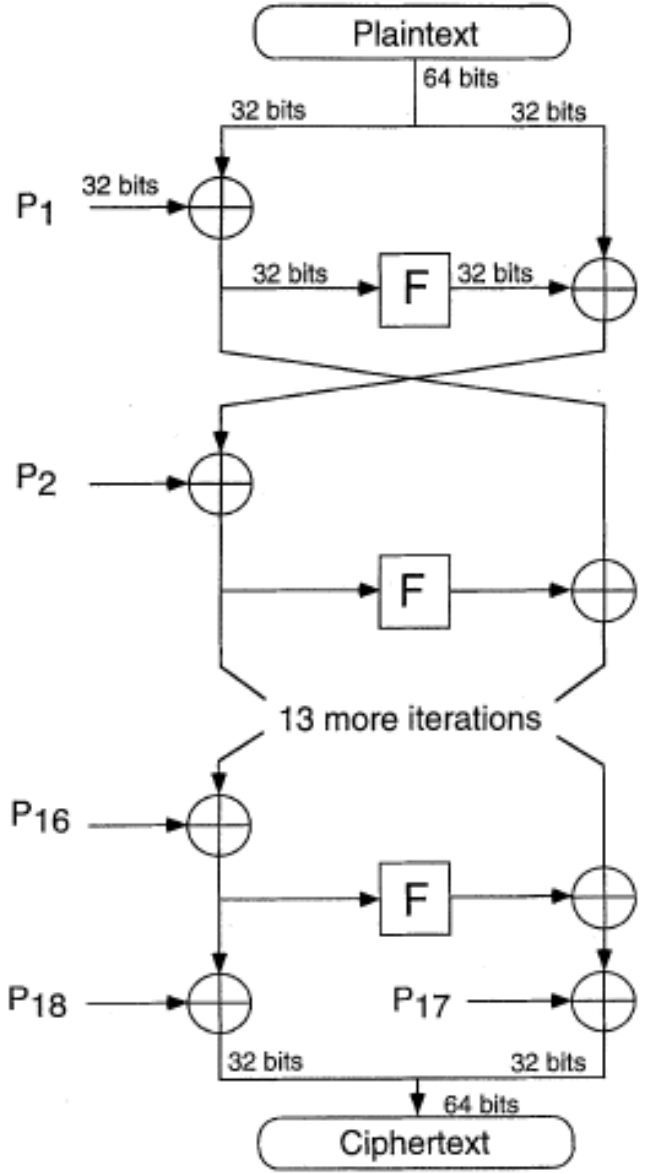
blowfish - Feistel

```
unsigned long F(unsigned long x)
{
    unsigned short a;
    unsigned short b;
    unsigned short c;
    unsigned short d;
    unsigned long  y;

    d = x & 0x00FF;
    x >>= 8;
    c = x & 0x00FF;
    x >>= 8;
    b = x & 0x00FF;
    x >>= 8;
    a = x & 0x00FF;
    //y = ((S[0][a] + S[1][b]) ^ S[2][c]) + S[3][d];
    y = S[0][a] + S[1][b];
    y = y ^ S[2][c];
    y = y + S[3][d];

    return y;
}
```



blowfish - Encryption

```
void Blowfish_encipher(unsigned long *xl, unsigned long *xr)
{
    unsigned long  Xl;
    unsigned long  Xr;
    unsigned long  temp;
    short          i;

    Xl = *xl;
    Xr = *xr;

    for (i = 0; i < N; ++i) {
        Xl = Xl ^ P[i];
        Xr = F(Xl) ^ Xr;

        temp = Xl;
        Xl = Xr;
        Xr = temp;
    }

    temp = Xl;
    Xl = Xr;
    Xr = temp;

    Xr = Xr ^ P[N];
    Xl = Xl ^ P[N + 1];

    *xl = Xl;
    *xr = Xr;
}
```



blowfish -Keyschedule

```
 j = 0;
 for (i = 0; i < N + 2; ++i) {
data = 0x00000000;
for (k = 0; k < 4; ++k) {
    data = (data << 8) | key[j];
    j = j + 1;
    if (j >= keybytes) {
        j = 0;
    }
}
P[i] = P[i] ^ data;
 }
```

```
datal = 0x00000000;
  datar = 0x00000000;

 for (i = 0; i < N + 2; i += 2) {
Blowfish_encipher(&datal, &datar);

P[i] = datal;
P[i + 1] = datar;
 }

 for (i = 0; i < 4; ++i) {
for (j = 0; j < 256; j += 2) {

   Blowfish_encipher(&datal, &datar);

   S[i][j] = datal;
   S[i][j + 1] = datar;
}
 }
```

Q & A