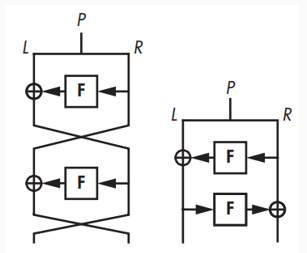
**라운드 구축 방법**

블록 암호는 라운드 반복 알고리즘으로 구성한다. 라운드자체는 보안이 약하나 여러 번 반복하면 강한 암호화를 만들 수 있다. SPN은 AES 암호화에 사용하는 구축 기법이고 파이스텔은 DES에 사용하는 구축 기법이다. 한 번 문자를 바꾸고(혼돈) 순서를 섞으면(확산) SPN 1round이다. SPN을 반복해서 구성하는 알고리즘은 보통 특정한 크기의 데이터 즉 블록을 처리한다. 블록의 크기는 64비트, 128비트, 192비트 등이 있다. 알고리즘에 데이터와 키를 넣어 SPN을 여러 번 반복할수록 강력한 암호문이 만들어진다. 블록 암호는 암호화해야할 데이터를 암호화에 사용할 알고리즘이 처리하는 데이터 크기만큼 자르고, 자른 부분마다 알고리즘을 적용해 그 결과물을 합친다.이처럼 알고리즘이 임의의 크기를 지닌 데이터를 처리하도록 구성하는 방식을 운영모드라 한다. 암호화 알고리즘으로 운영모드를 만든다. 운영모드는 암호화 알고리즘을 특정 방식으로 동작해 하나의 단위 암호 시스템을 만든다. 단위 암호 시스템 여러 개가 모여 전체 암호 시스템을 구성한다. 운영 모드는 ECB, CBC, CFB, OFB, CTR 등이 있으며 전체 암호 시스템은 AES, DES 등이 있다.

**파일스텔 기법**

1970년 IBM공학자 호르스트 파이스텔이 설계하였다.

1. 64bit 블록을 절반으로 나누어 32bit 블록 L, R을 만든다.
2. L을 L F(R)로 정한다. F 대입-치환 라운드
3. L, R의 값 교환
4. 2 ~ 3 단계 15회 반복
5. L, R 연결해 64 비트 블록 생성