블록암호 운용모드

유튜브 주소 : https://youtu.be/hfMFD_hEsSU

운용모드 개요

ECB, CBC 모드

OFB, CFB, CTR 모드

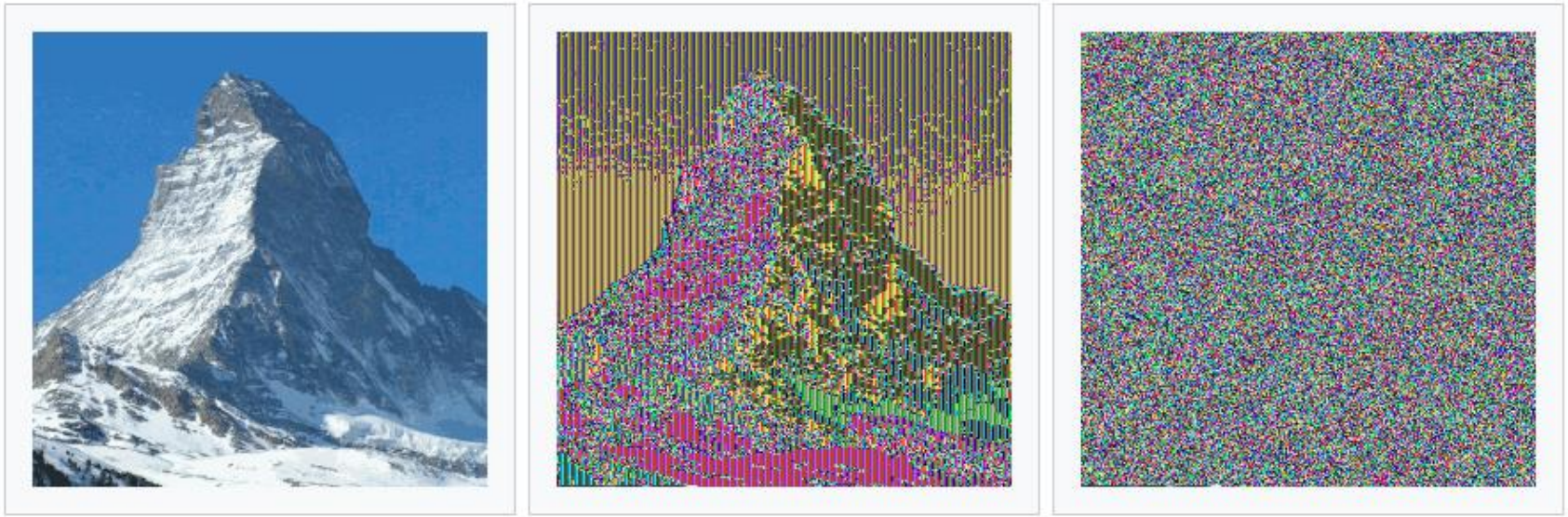
블록암호 운용모드

- 블록 암호를 블록 단위로 암,복호화되는 과정을 운용하는 절차
  - 평문의 암,복호화를 어떻게 반복하느냐에 따라 보안성이 달라짐
  - 암호화와 인증을 목적으로 정의
  - 공개키 암호에도 적용 가능하나 일반적이진 않음

- NIST에서는 5가지 운용 모드를 정의함
  - ECB모드 - Electronic Code Blok mode (전자 부호표 모드)
  - CBC모드 - Cipher Block Chaining mode (암호 블록 연쇄 모드)
  - CFB모드 - Cipher-FeedBack mode (암호 피드백 모드)
  - OFB모드 - Output-FeedBack mode (출력 피드백 모드)
  - CTR모드 - CounTer mode (카운터 모드)

ECB 모드

- 가장 간단하며 기밀성이 낮은 모드
- 평문 블록을 암호화한 것이 그대로 암호문 블록이 됨
  - 평문 블록과 암호 블록이 1:1 관계를 가짐



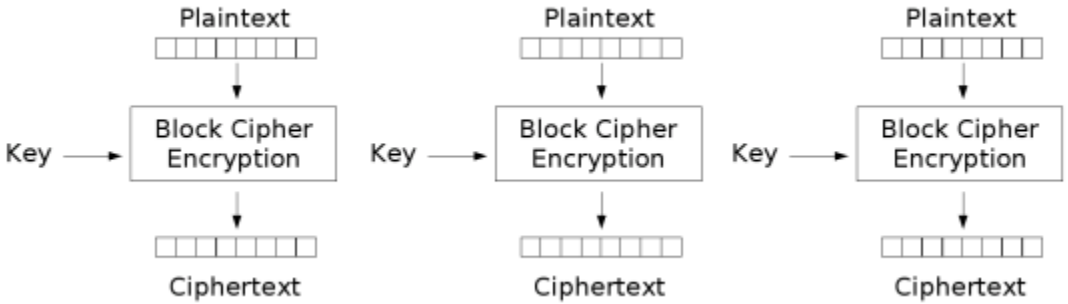
Original picture

With ECB Block Mode

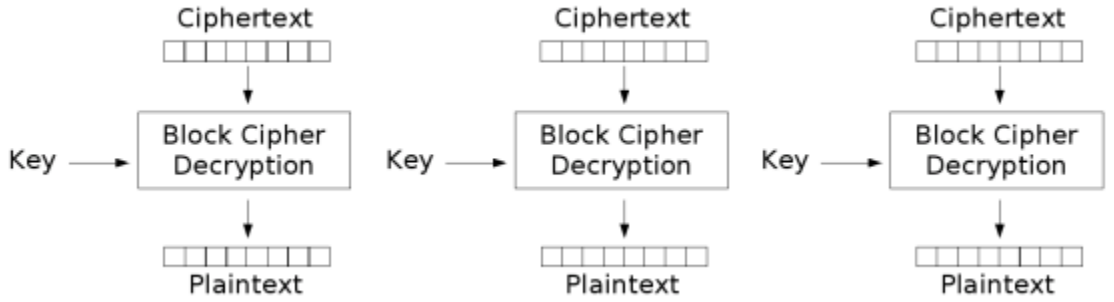
With any other Block Mode

ECB 모드

- 각 블록마다 대응되는 암호문 블록으로 암호화 됨
  - 평문과 암호문 블록이 1:1 대응
- 각 블록은 독립적으로 처리됨
  - 에러가 발생해도 다른 블록에는 영향 안줌
- 모든 블록이 같은 암호화 키를 사용
  - 한 개의 블록이 해독되면 나머지 블록도 해독됨
- 패딩 사용



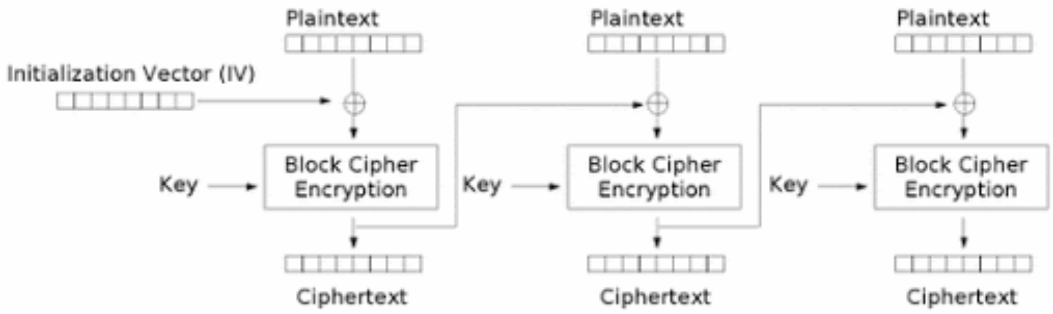
ECB 암호화



ECB 복호화

CBC 모드

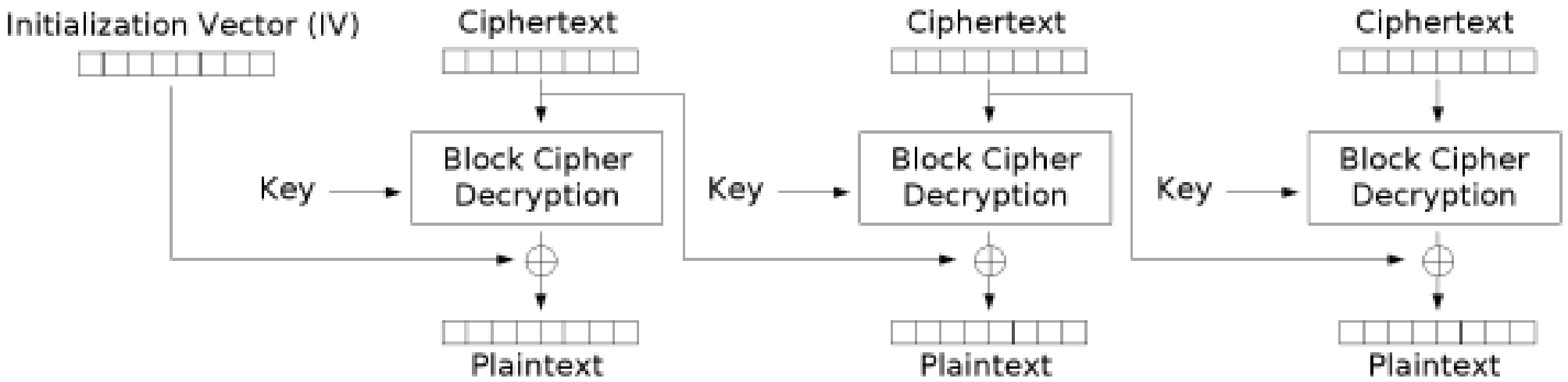
- 각 평문 블록이 이전 암호문 블록과 XOR
  - 첫 블록을 암호화 할 땐 초기 벡터 필요
  - 초기 벡터는 nonce여야 함
  - 초기 벡터가 비밀값일 필요 X
- CBC 방식은 확률적
  - 새로운 초기 벡터를 적용할 때 마다 완전히 다른 암호문 블록들이 생성
- 평문과 암호문이 1:1 대응 관계가 아님 -> ECB 모드의 단점 없음
- 운용모드 중 보안성이 가장 높은 방식으로 가장 많이 사용



CBC 암호화

CBC 모드

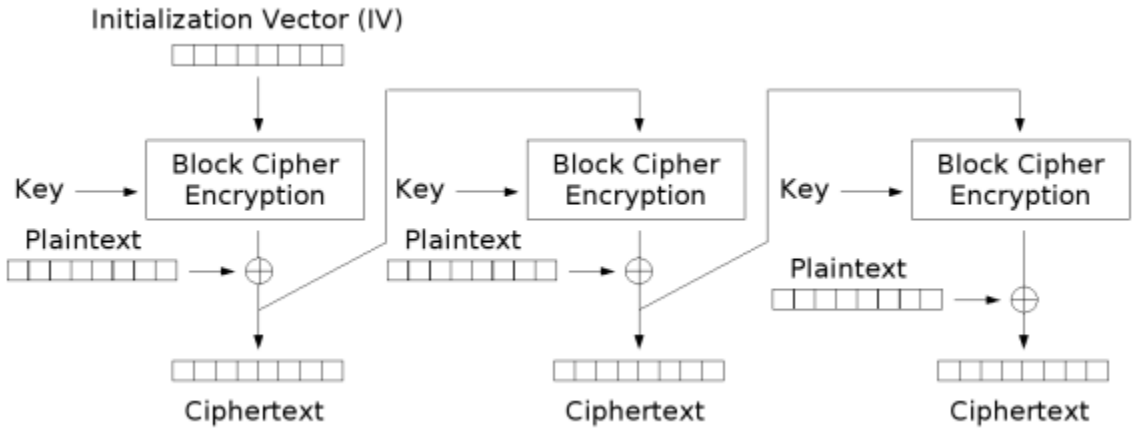
- CBC 모드 복호화
- 암호화 시 에러가 발생해 비트 누락 시 한 비트씩 앞으로 밀림
  - 이후 블록은 어긋나서 복호화 불가



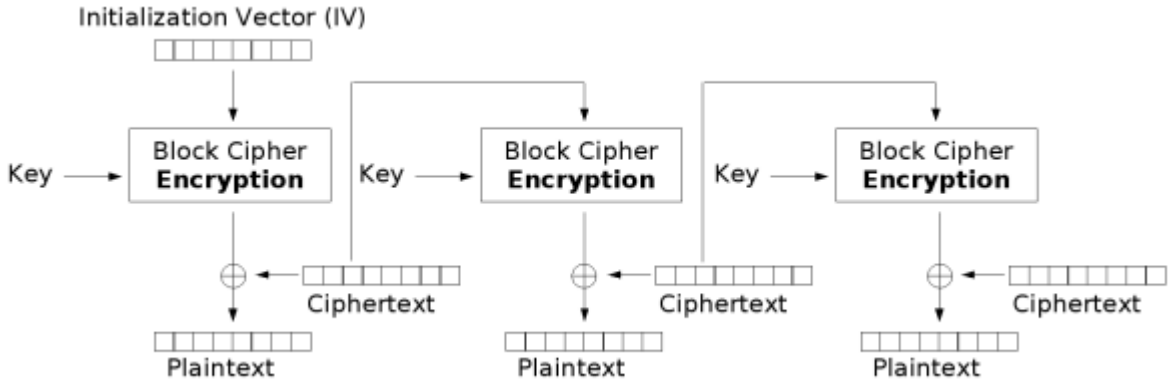
CBC 복호화

CFB 모드

- CBC의 변형된 방식
  - 블록암호를 스트림 암호로 변환
- 어떠한 값과 평문을 XOR한 결과값이 암호문이 됨
  - 스트림 암호의 형태를 지님
  - 키 스트림이 암호문에 의존하는 비동기식 스트림 암호
- 문자가 암호화 되는 즉시 전송 가능
- 블록 암호의 복호화 과정 없이 평문 복호화 가능



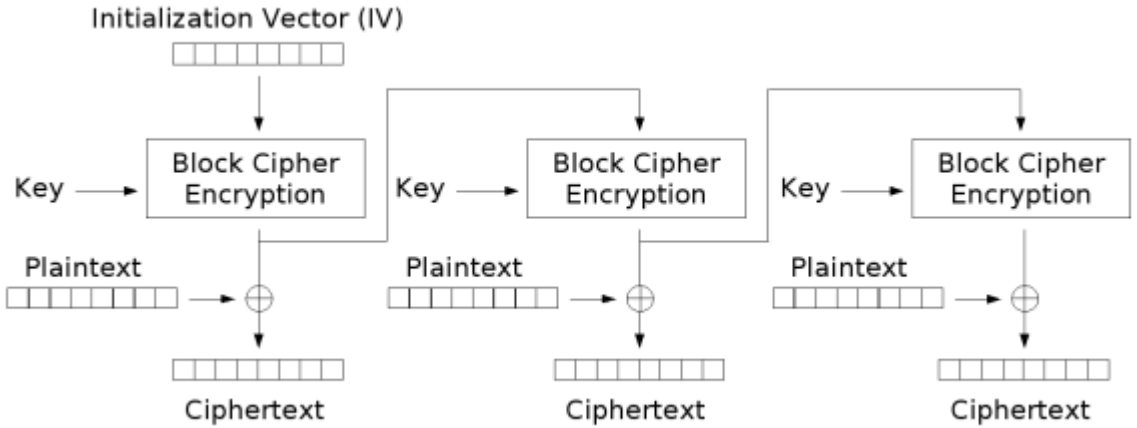
CFB 암호화



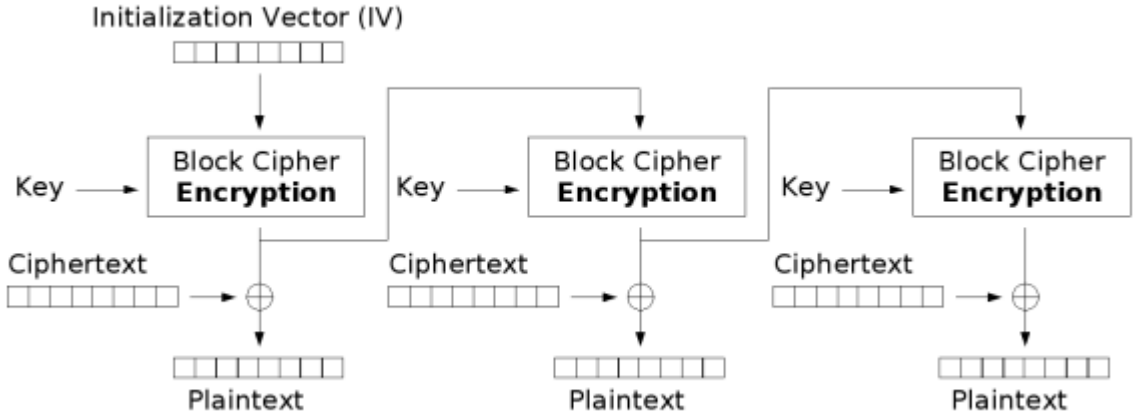
CFB 복호화

OFB 모드

- 블록 암호를 스트림 암호로 변환
- Output FeedBack mode
  - 암호 알고리즘의 Output값을 다음 암호 알고리즘에 사용
  - CFB와 차이점 지님
  - CFB는 초기벡터와 XOR한 암호문을 다음 암호 알고리즘에 사용
- ECB, CBC, CFB 모드를 개선한 운용 모드



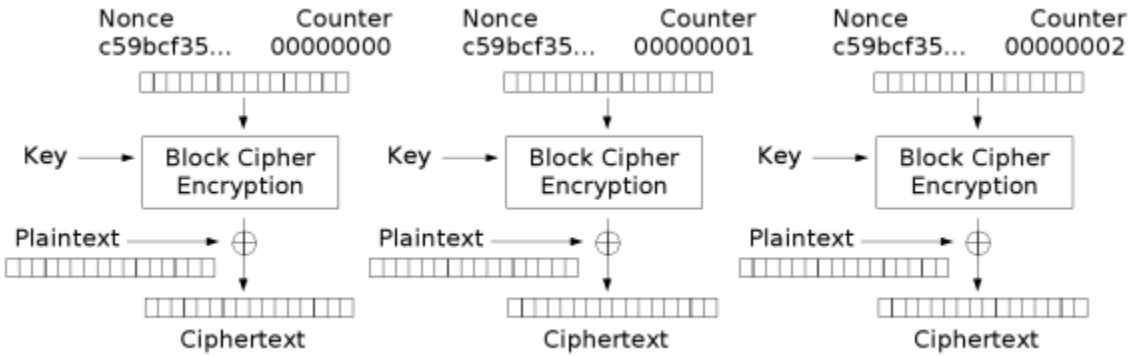
OFB 암호화



OFB 복호화

CTR 모드

- 스트림 암호의 구조를 가짐
- 암호화 시 마다 Nonce를 구함
- 암호화 할 때 마다 1씩 증가하는 counter를 Nonce와 결합해 사용
- 이전 블록의 어떠한 값도 다음 블록에 영향을 주지 않음
  - 오류 전파가 없음
- 원하는 부분만 복호화 할 수 있음



CTR모드 암호화

Q & A