AEAD

https://youtu.be/1OqbjiVaAqA

AEAD

- Authenticated Encryption with Associated Data
- 관련 데이터와 인증된 암호화
- AE + AD

AE

- 인증된 암호 방식 (Authenticated Encryption, AE)
- MAC을 이용하여 무결성 및 인증 제공

AE - 문제점

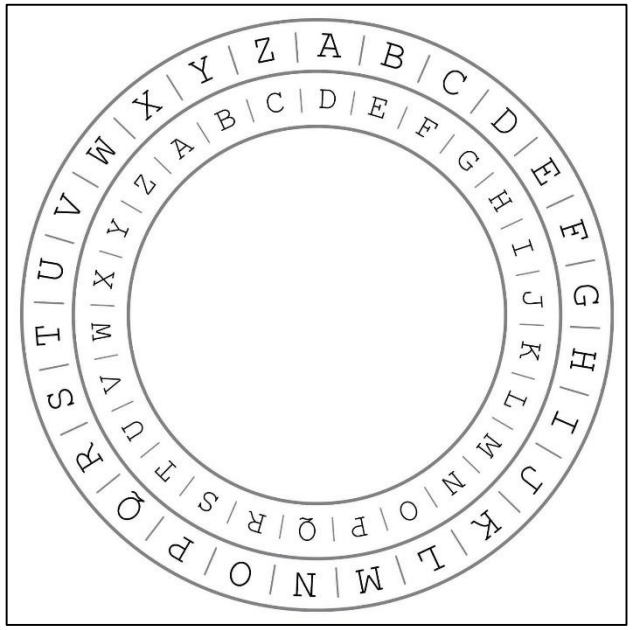
- Encryption data와 MAC의 안전한 결합은 쉽지 않음
- 클라이언트의 Encryption data 수정에 대한 예방 불가

AE - 문제점

- 원본 데이터 : { “User”: “Oren”, “Admin”: “N” }
- 암호화 데이터 : { “Xvhu”: “Ruhq”, “Dgplq”: “Q” }

- 어드민 확인 코드 : isAdmin = GetSessionCookieData().Admin != ‘N’

- 클라이언트에서 데이터 { “Xvhu”: “Ruhq”, “Dgplq”: “R” } 로 변경



예시 카이사르 암호 치환 테이블

AE - 문제점

- 암/복호화가 잘 작동하여도 값에 대한 온전한 보존 보장 불가

- 혼동된 대리인 문제 (Confused Deputy Problem)

혼동된 대리인 문제

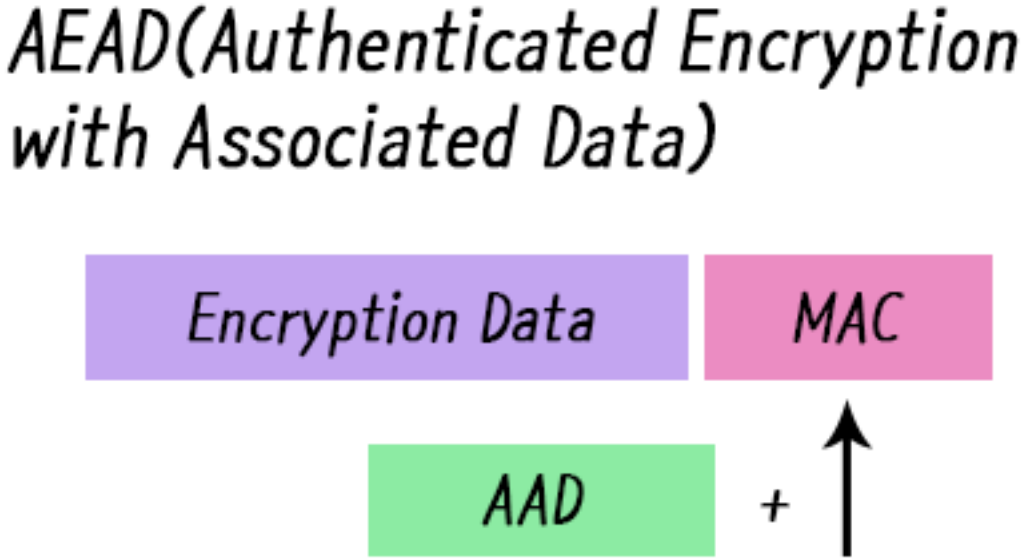
- 공격자는 특정 공격 방식을 이용하여 대리인의 권한 수정
- 프로그램은 공격자가 속였다는 사실을 인지하지 못함 (= 혼동된 대리인)
- 공격자는 대리인을 이용해 다른 사용자에 권한 행사 혹은 데이터에 접근

CSRF 공격

- 사이트간 요청 위조 (Cross-Site Request Forgery)
- 사용자로 하여금 자신도 모르게 공격자가 의도한 행위를 요청하게 함
- 사이트에서 어드민 페이지의 경로가 /admin_setup 이고 GET 파라미터를 통해 값을 요청할 때
- 공격자가 게시글에 <img src="/admin_setup?user=john&passwd=1234"> 태그를 추가
- 어드민이 그 게시글을 클릭하면 자신의 권한에 의해 해당 명령 실행

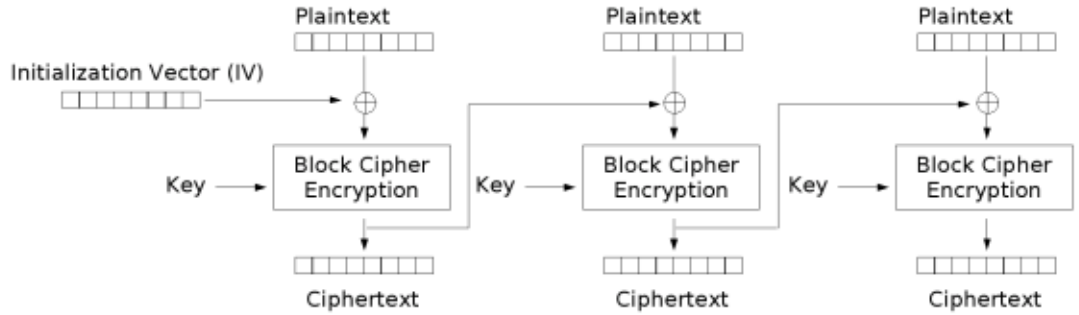
AD

- 관련 데이터 (Associated Data 혹은 Additional Associated Data (AAD))
- AD를 MAC에 추가하여 인증 강화
- MAC의 부인방지 불가에 대해 보완

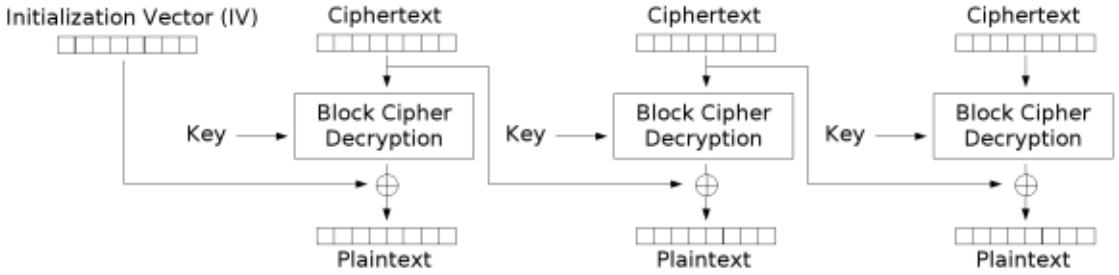


CBC 모드

- Cipher-Block Chaining
- 평문과 IV를 XOR 연산한 값을 입력값으로 설정
- 출력된 암호문을 다시 평문과 XOR 및 입력
- 오라클 패딩 공격에 취약



Cipher Block Chaining (CBC) mode encryption



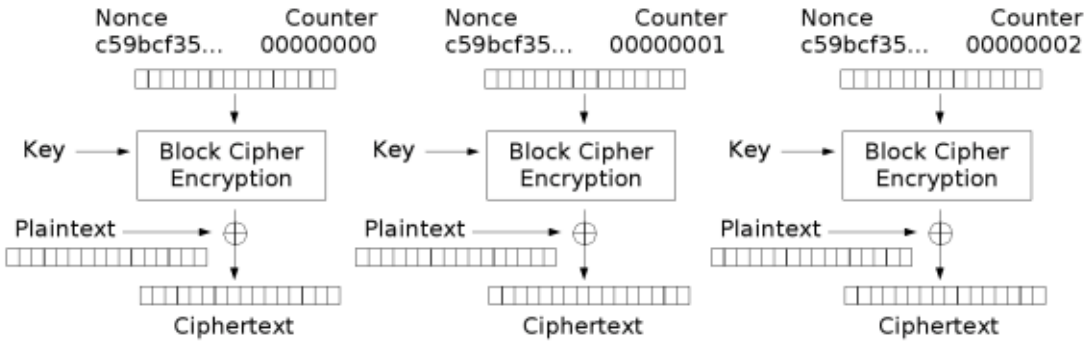
Cipher Block Chaining (CBC) mode decryption

오라클 패딩 공격

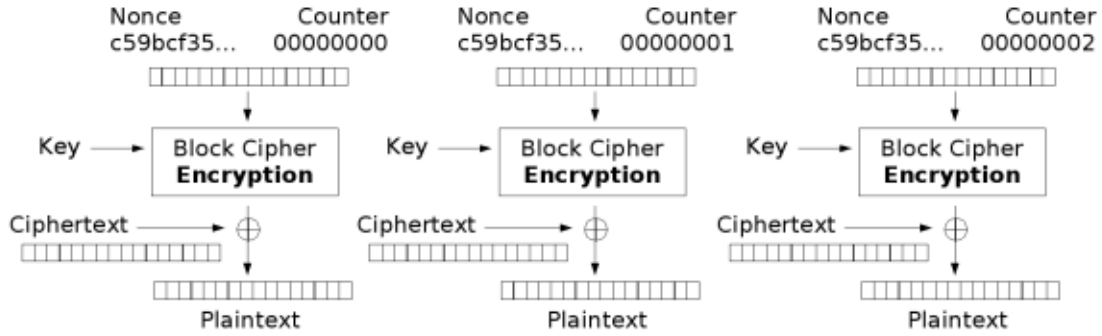
- 블록암호는 데이터를 블록 사이즈에 맞춰 패딩
- 서버에 잘못된 암호문을 넣었을 때의 패딩의 올바름 유무에 관한 응답을 통해 평문 유추
- 조작한 값을 서버로 보내서 공격

CTR 모드

- Counter
- 암호화 함수에 nonce, counter, key를 넣음
- 출력된 결과값과 평문을 XOR 연산
- 패딩 없음
- 병렬 연산 가능



Counter (CTR) mode encryption



Counter (CTR) mode decryption

CTR 모드

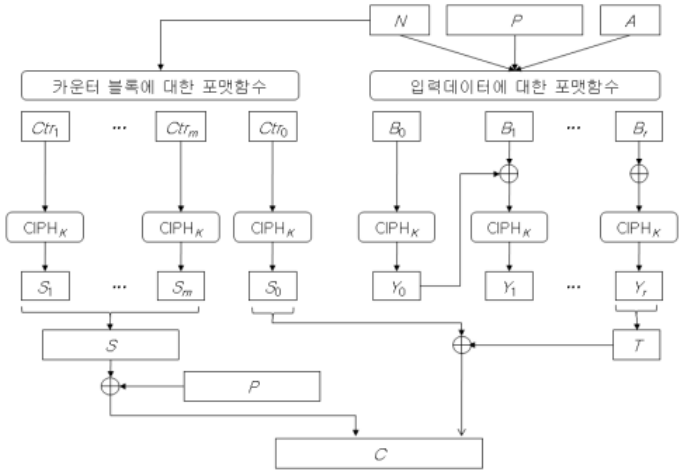
- CCM (Counter with CBC-MAC)

- GCM (Galois/Counter Mode)

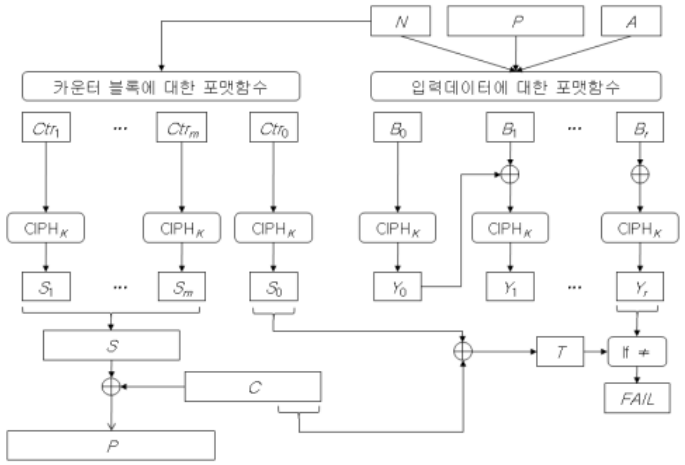
CCM

- CTR + CBC-MAC
- CBC-MAC을 통해 MAC 생성
- N: Nonce, P: Payload, A: AD
- Nonce로 CTR 블록 생성
- MAC 계산에 N, P, A 모두 사용

(그림 1) CCM 모드 암호화

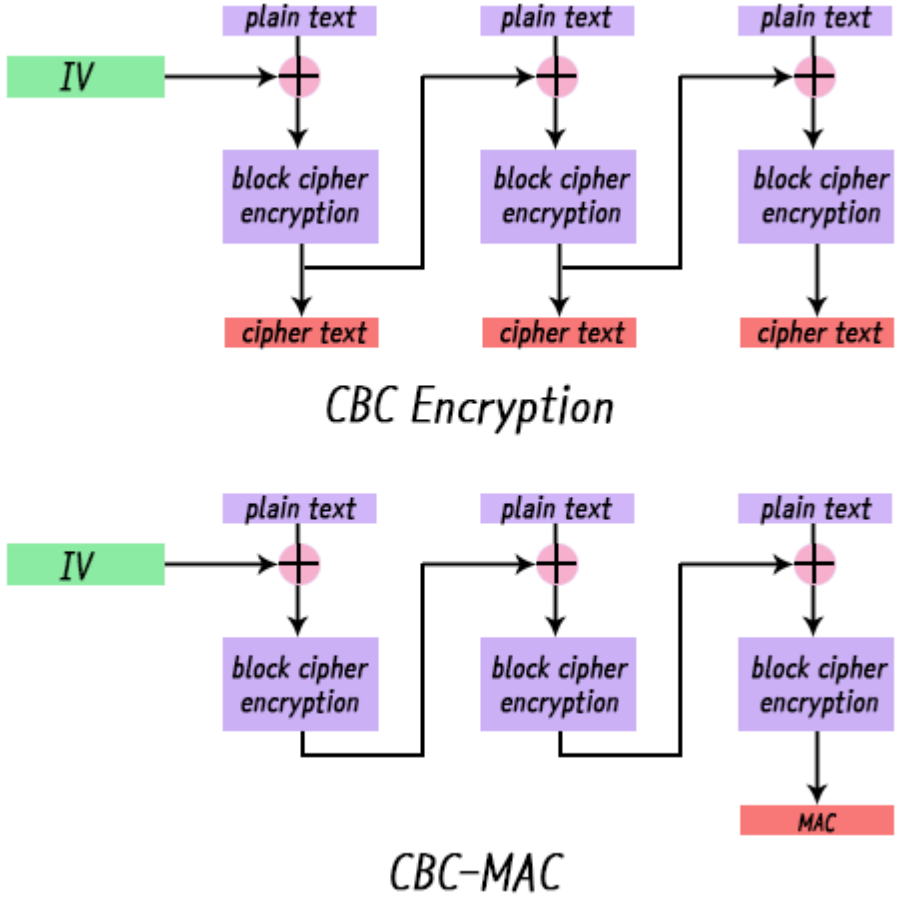


(그림 2) CCM 모드 복호화



CBC-MAC

- CBC 원리를 이용하여 MAC 계산



GCM

- MAC 계산에 GMAC (Galois-MAC) 사용
- GHASH 함수를 이용하여 인증 보장
- nonce에 따라 CTR_0 블록 다르게 생성
- 데이터 값의 HASH가 암호문에 포함되어 있어 복호화 시 검증
- GMAC을 먼저 복호화 가능하여, 값 미리 검증 가능

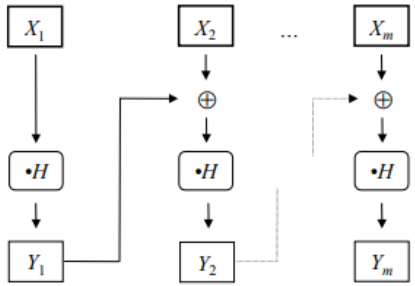
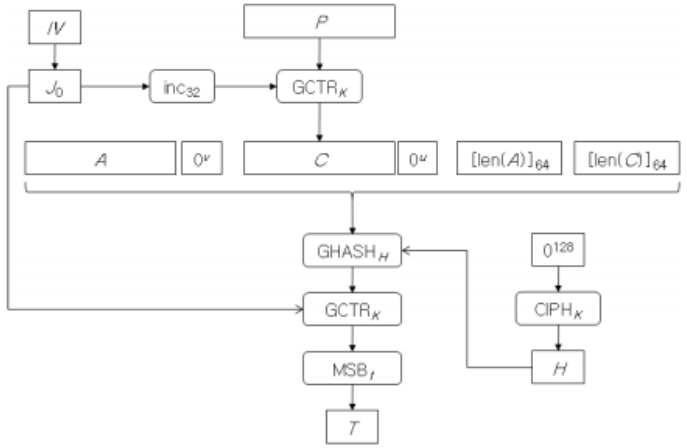


Figure 1: $\mathrm{GHASH}_H(X_1 \| X_2 \| \ldots \| X_m) = Y_m$.

GHASH 함수

(그림 5) GCM 모드 암호화



Q & A