19년 정보보호 전문가를 위한 암호 교육

최승주

19.2.24

Day 1

https://youtu.be/B-CNQB1MFWQ

암호 교육

19년 2월 18일(월) ~ 22일(금)

정보 보안에 관한 교육

1. 정보보안과 암호기술
2. 대칭키 및 공개키 암호
3. 정보보안 기술의 응용

1. 정보보안과 암호기술

보안의 3요소

- 기밀성(Confidentiality)
- 무결성(Integrity)
- 가용성(Availability)

공격 방식

- 수동적 공격

  공격자가 공격을 하고 있는지 알기 힘든 방식의 공격

  Ex) 도청, Traffic Analysis

- 능동적 공격

  공격자가 공격을 하고 있는지 알기 쉬운 방식의 공격

  Ex) Masquerade(위장), Replay(반복), Modification of Message(조작),
  Denial of Service(DoS)

공격 대처

Cryptography – 암호학

- 좁은 의미: 메시지를 다른 사람들이 못 알아보게 만들기
- 넓은 의미: 공격자의 영향을 극복해서 프로토콜이 정상적으로 돌아가게 하는 것

케르크호프스의 원리

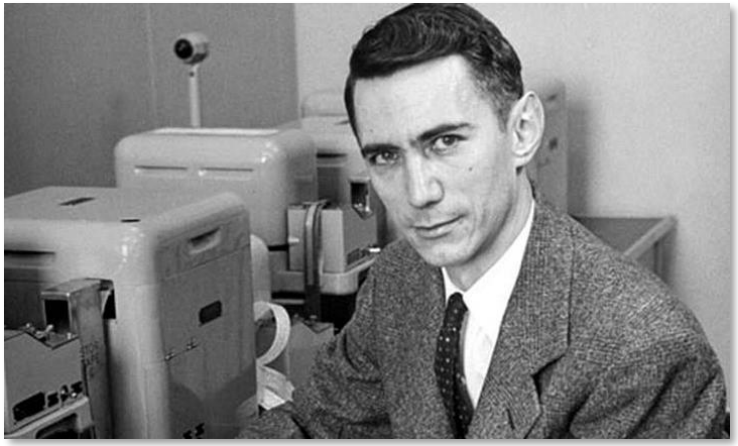
Kerchhoff – 19 세기

키를 제외한 시스템의 모든 내용이

알려지더라도 암호체계는 안전해야 한다.

알고리즘은 공개되어도 상관없어야 한다.

현대 암호학의 선구자

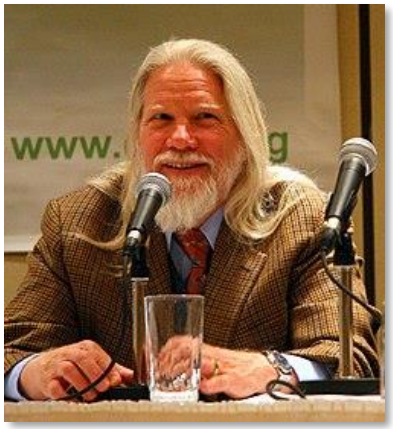


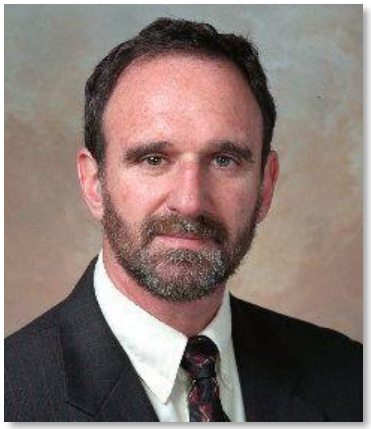
Claude Elwood Shannon

A Mathematical Theory of Communication

- 정보 이론의 시초
- 디지털 회로 이론 창시

현대 암호학의 선구자



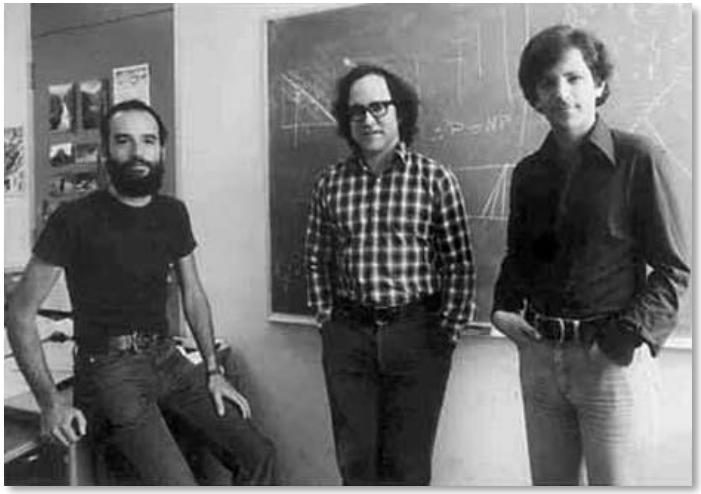


Whitefield Diffie & Martin Hellman

New Directions in Cryptography

- 공개열쇠암호 분야의 개척자
- 디피-헬만 키 교환

현대 암호학의 선구자



Rivest & Shamir & Adleman

A method for obtaining Digital Signatures and Public-Key Cryptosystems

- 공개키 암호 알고리즘 개발 (RSA)
- 전자서명이 가능한 최초의 알고리즘

고전 암호

- Caesar & Shift Cipher

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A

THIS IS A MESSAGE THAT HAS BEEN ENCODED WITH A VERY SIMPLE SHIFT CIPHER

UIJT JT B NFTTBHF UIBU IBT CFFO FODPEFE XJUI B WFSZ TJNQMF TIJGU DJQIFS

- Monoalphabetic Cipher

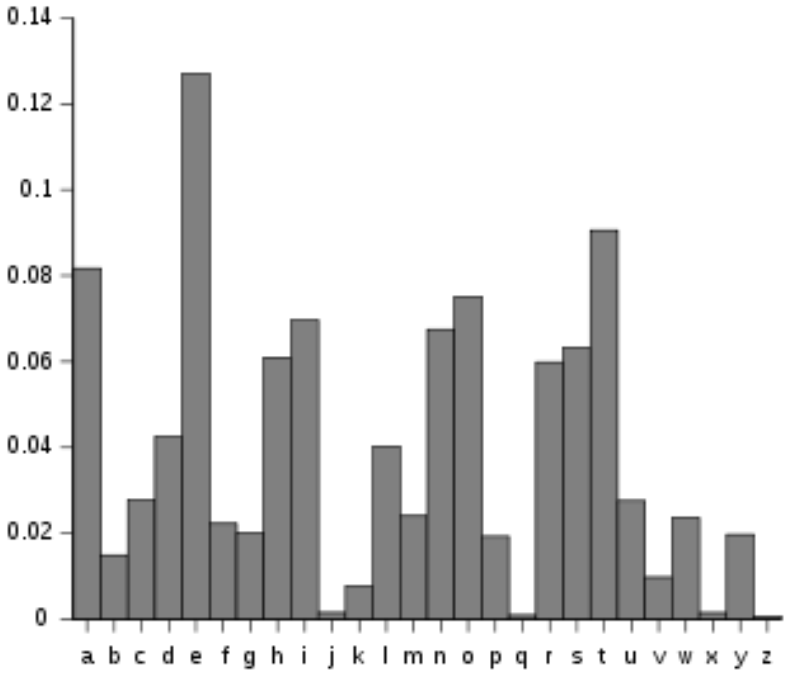
  A – 26 중 한 글자 선택

  B – 25 중 한 글자 선택 …

  총 26!

고전 암호

- Monoalphabetic Cipher
  - Frequency analysis



고전 암호

- Polyalphabetic Cipher

  순서가 없어 보이게 만드는 방식

  같은 E 여도 할당되는 알파벳이 다르게 만드는 등등

고전 암호

- One – Time Pad

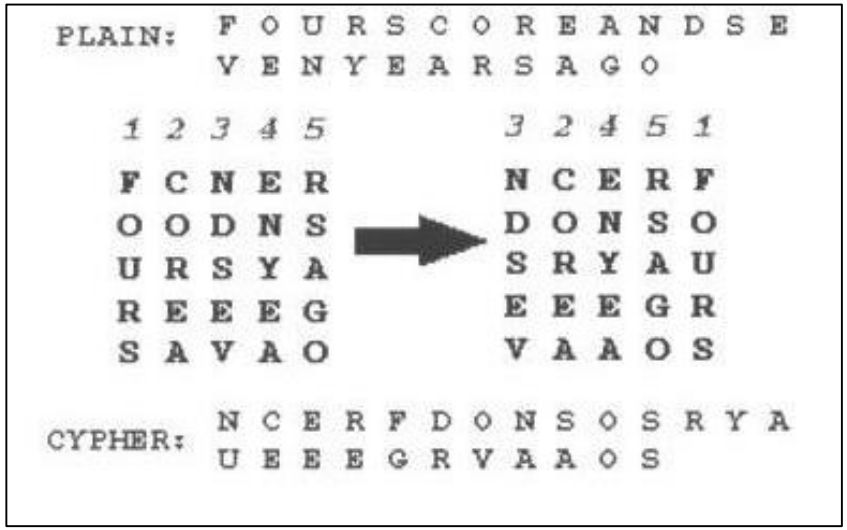
  메시지 만큼 키의 길이를 정한다.

  이론상으로는 완벽

  용량이 너무 커서 사용 불가

고전 암호

- Transposition Cipher



고전 암호

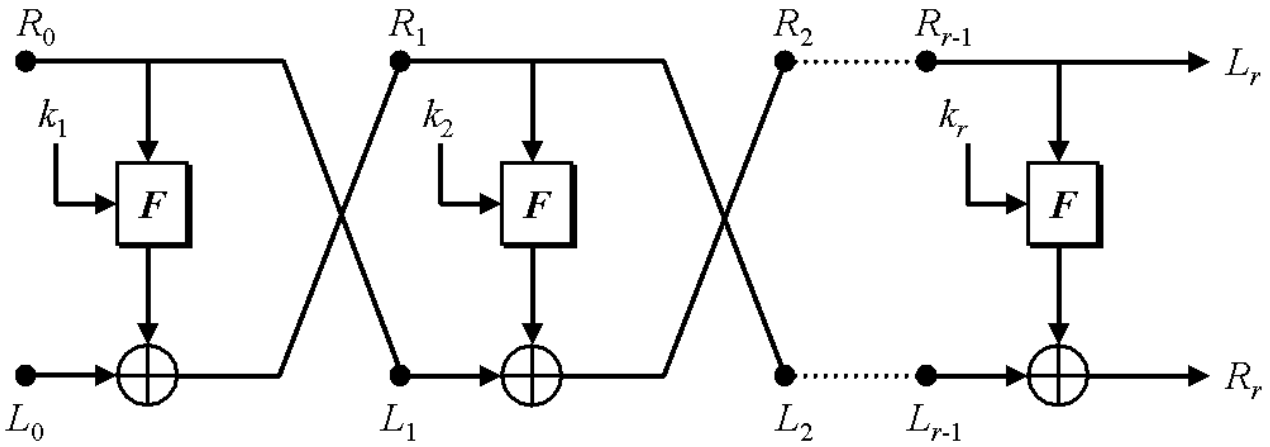
- Product Ciphers

  섞어주는 규칙을 여러 개 사용하자

  S-box & P-box

현대 암호

- Feistel(파이스텔)



현대 암호

- Feistel(파이스텔)

  한번에 다 섞지 않고 간단한 연산을 계속해서 반복해 주는 방식으로 진행

  요소: F, Round, Block Size

현대 암호

- DES

  정부에서 IBM의 루시퍼(128) 을 가져가 개조하여 DES(56) 제작

  Box들을 사용하여 Permutation 많이 함

  Avalanche Effect(산사태 효과)

  비트 하나만 바뀌어도 암호문의 절반 이상이 바뀌는 현상

현대 암호

- AES

  민간에서 공모전을 통해 뽑은 알고리즘 방식

  벨기에 암호학자 Daemen & Rijmen

  Rijndael에 기반

  Key 128, 192, 256

  안전도, 속도

외전

- Steganography

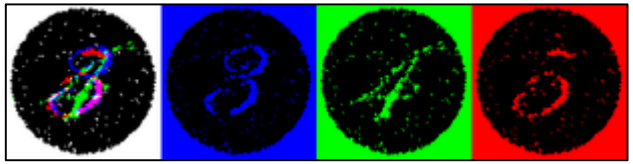
  데이터 은폐 기술 중 하나

  암호화 대안

  암호학: 메시지 존재를 숨기려고 하진 않는다.

  Steganography: 메시지 존재 자체를 숨기려고 한다.

  Ex) 음악 저주파에 메시지 숨겨 보내기



2. 대칭키 및 공개키 암호

암호

	대칭	비대칭
기밀	AES / DES	RSA - OAEP
무결성	MAC	RSA - PSS

암호

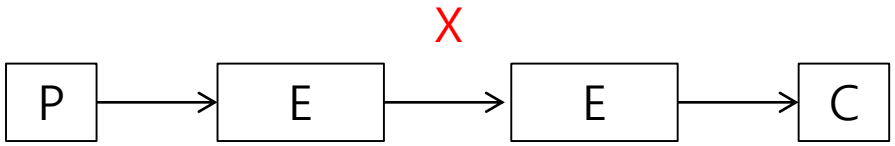
- 대칭: DES & AES
- 비대칭: RSA
- 기밀: 메시지를 숨기는 것이 목적
- 무결성: 위조를 못하게 하는 것이 목적

대칭 & 기밀

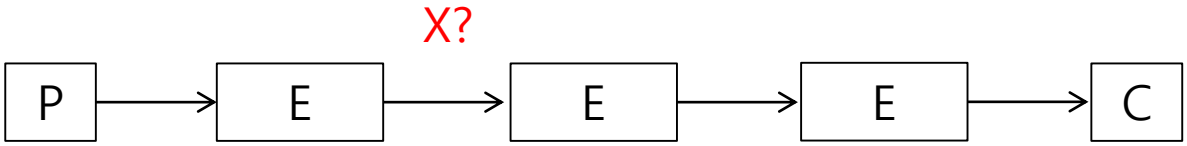
- DES & AES

Double DES

Meet in the middle attack



Triple DES



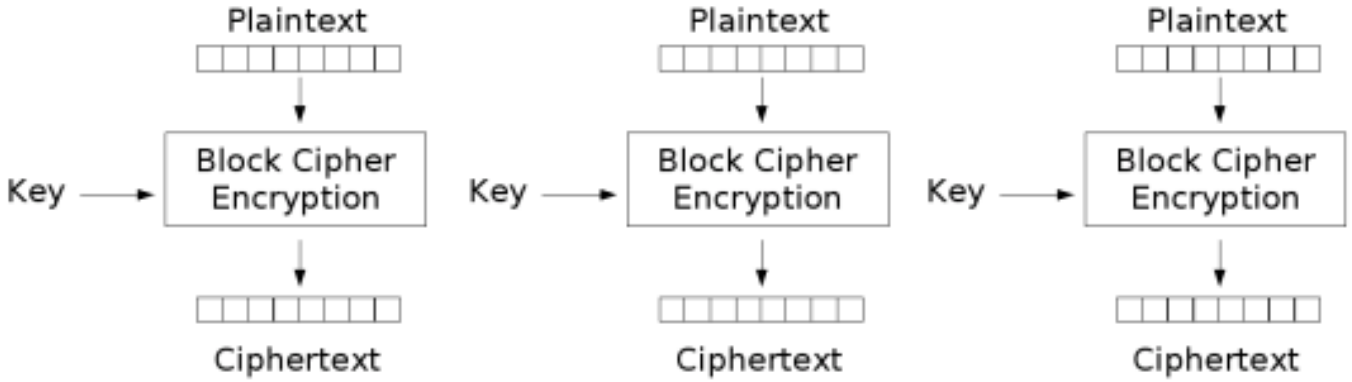
블록 암호 운용 방식

- 블록 암호를 반복적으로 안전하게 이용하는 절차

  블록 단위로 동작하는 알고리즘에서 블록들을 어떻게 끊어서 암호화 할지를 정하는 것

블록 암호 운용 방식

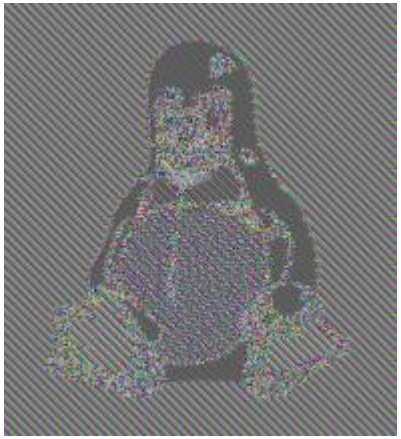
- 전자 코드북 (ECB)

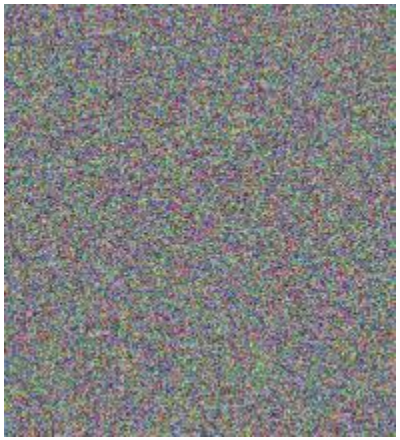


Electronic Codebook (ECB) mode encryption

블록 암호 운용 방식

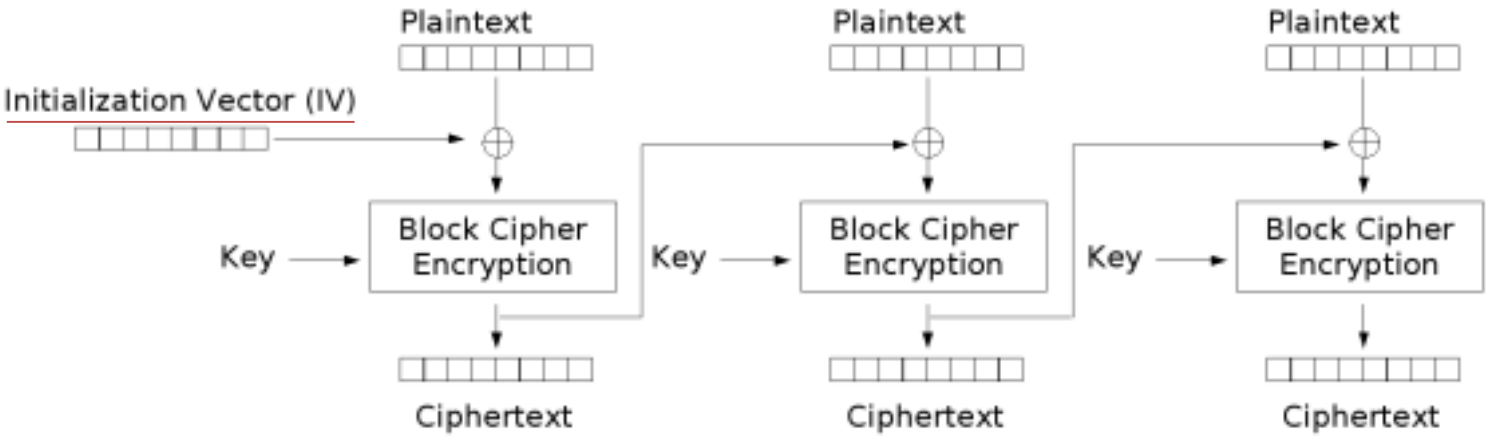
- 전자 코드북 (ECB)





블록 암호 운용 방식

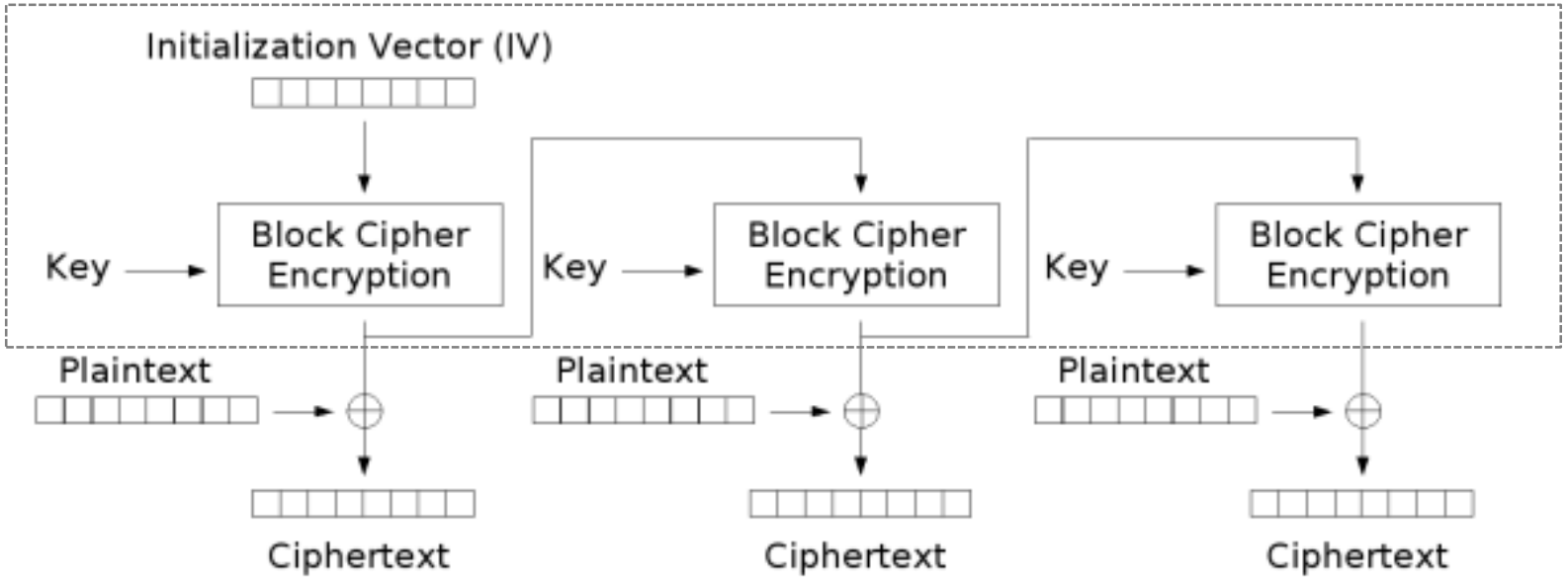
- 암호 블록 체인 방식 (CBC)



Cipher Block Chaining (CBC) mode encryption

블록 암호 운용 방식

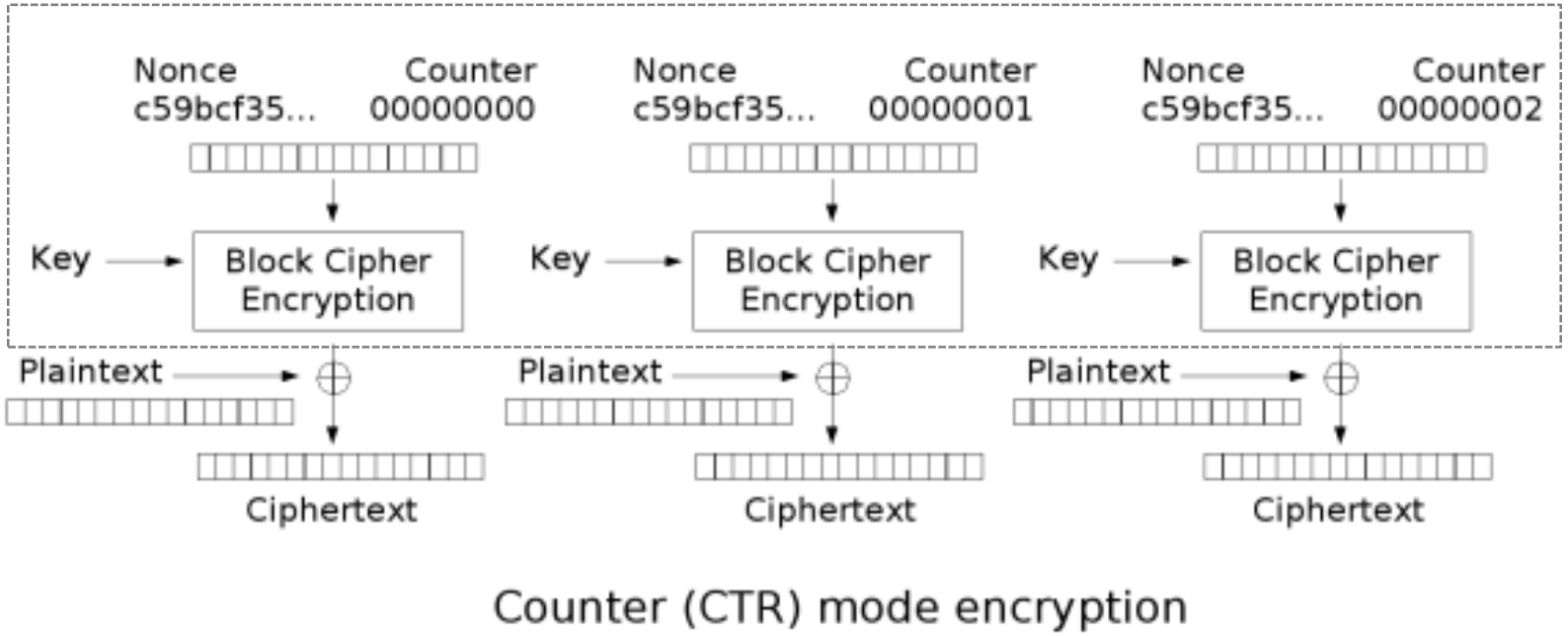
- 암호 블록 체인 방식 (OFB)



Output Feedback (OFB) mode encryption

블록 암호 운용 방식

- 카운터 (CTR)

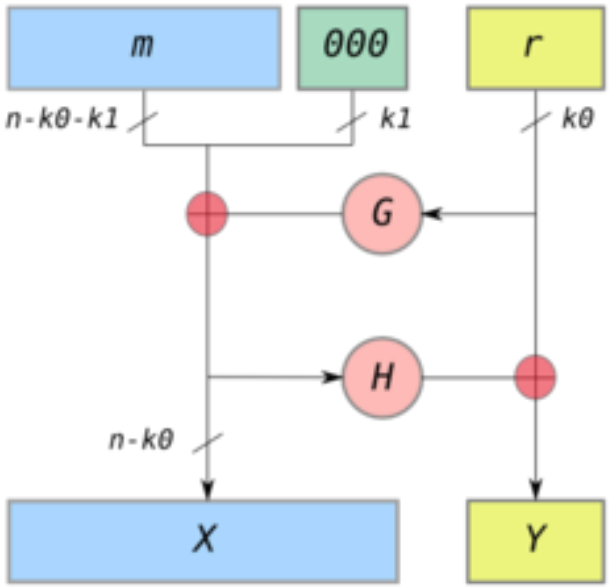


Counter (CTR) mode encryption

비대칭 & 기밀

- RSA – OAEP

  RSA: 같은 평문에 대해 동일한 암호문이 생긴다 – 난수 패딩



비대칭 & 기밀

- 비대칭키 관련 외전
  - 왜 AES나 DES를 사용하는가

    대칭키 속도 > 비대칭키 속도

  - 잠그는 사람과 푸는 사람이 같다면 비대칭키 쓸 이유가 없다

  - 주로 서로 모르는 사이간의 거래에서 사용

비대칭 & 기밀

- Hybrid Encryption
  - RSA는 Session 키 주고 받을 때만 사용
  - Session 형성되면 메시지는 AES로 주고 받기

무결성 & 비대칭

- RSA-PSS
  - 기밀이 목적이 아니라 무결성이 목적
  - 전자 서명
  - 메시지를 hash한 값을 전자 서명한다.
  - 내 메시지가 내 공개키로 풀어진다는 것은 내가 개인키로 서명을 했다는 의미

무결성 & 비대칭

- RSA-PSS

  Hash

  - 입력에 대한 고정된 크기의 출력이 생성
  - 해시 값으로부터 원래의 입력값과의 관계를 찾기 어려운 성질

무결성 & 비대칭

- Birthday Attack

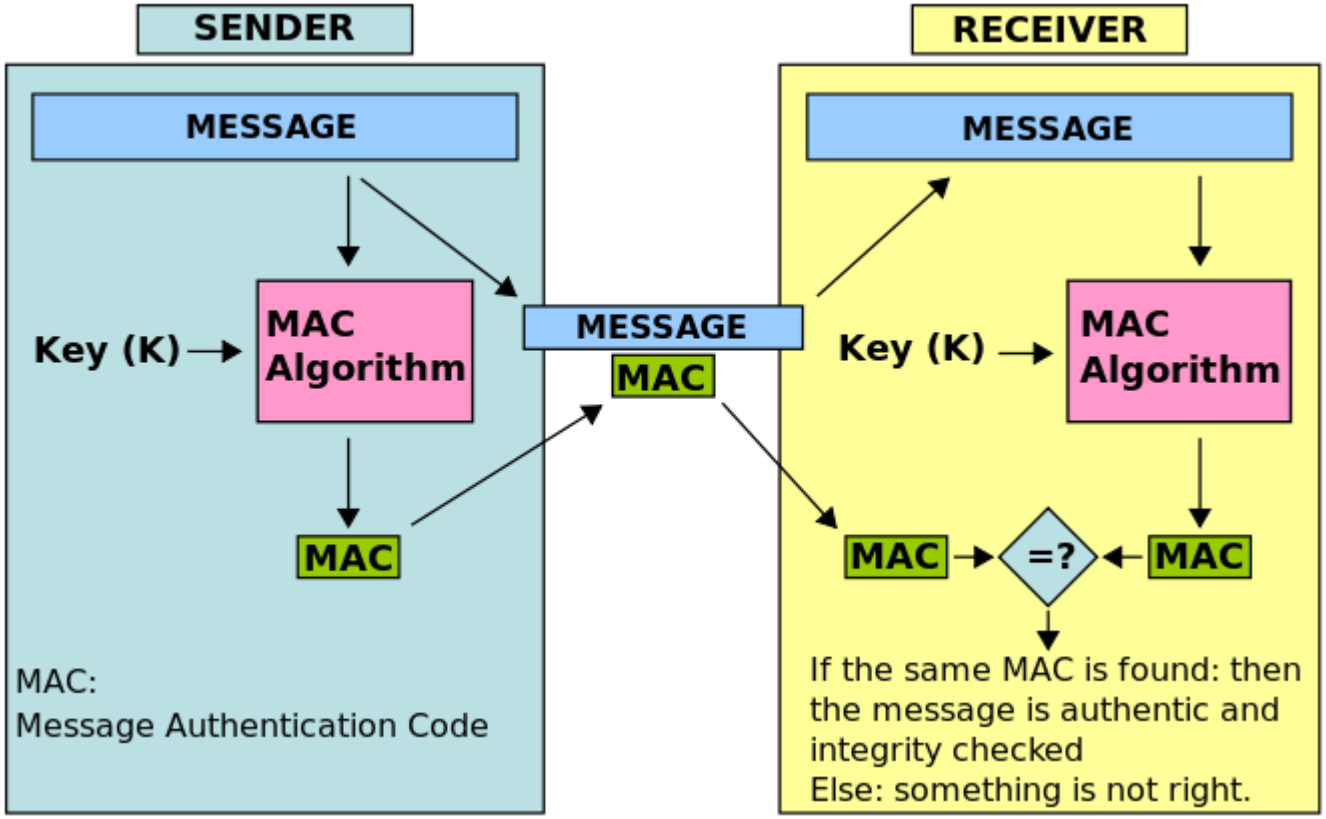
  암호학적 해시 함수의 해시 충돌을 찾아내는 암호 해독 공격

  - 한 방안에 생일이 겹치는 사람이 있기 위한 사람 수: 366
  - 실제 계산되어 나온 필요 사람 수: 23

  모든 값을 대입하지 않고도 해시 충돌을 찾아낼 확률이 크다

무결성 & 대칭

- MAC


SENDER
RECEIVER
MESSAGE
MESSAGE
Key (K)
MAC Algorithm
MESSAGE
MAC
Key (K)
MAC Algorithm
MAC
MAC
=?
MAC
MAC:
Message Authentication Code
If the same MAC is found: then the message is authentic and integrity checked
Else: something is not right.

3. 정보보안 기술의 응용

Authentication - 인증

- Entity(대상) 인증

  본인 확인

- Data Origin 인증

  메시지 변조 확인

Authentication - 인증

- 인증 방법

  열쇠, 손 서명, 홀로그램 등등

- 인증 요소
  - 가지고 있는 것(Has)
  - 알고 있는 것(Knows)
  - 대상의 특성(IS)

Authentication - 인증

- 인증 요소
  - 가지고 있는 것(Has)

    열쇠, OTP, 카드, 신분증 등등

    분실의 위험

  - 알고 있는 것(Knows)

    암호문, PIN 번호 등등

Authentication - 인증

- 인증 요소
  - 알고 있는 것(Knows)

Graphical Password

- 그림이나 사진으로 비밀번호를 정하는 것
- 망각의 위험 및 사람의 선택 성향이 유사함

Pattern Lock

- 패턴 흔적 추적

Authentication - 인증

- 인증 요소

  – 대상의 특성(IS)

  지문, 얼굴, 홍채 등등

  행위 – 타이핑 속도, 패턴 등

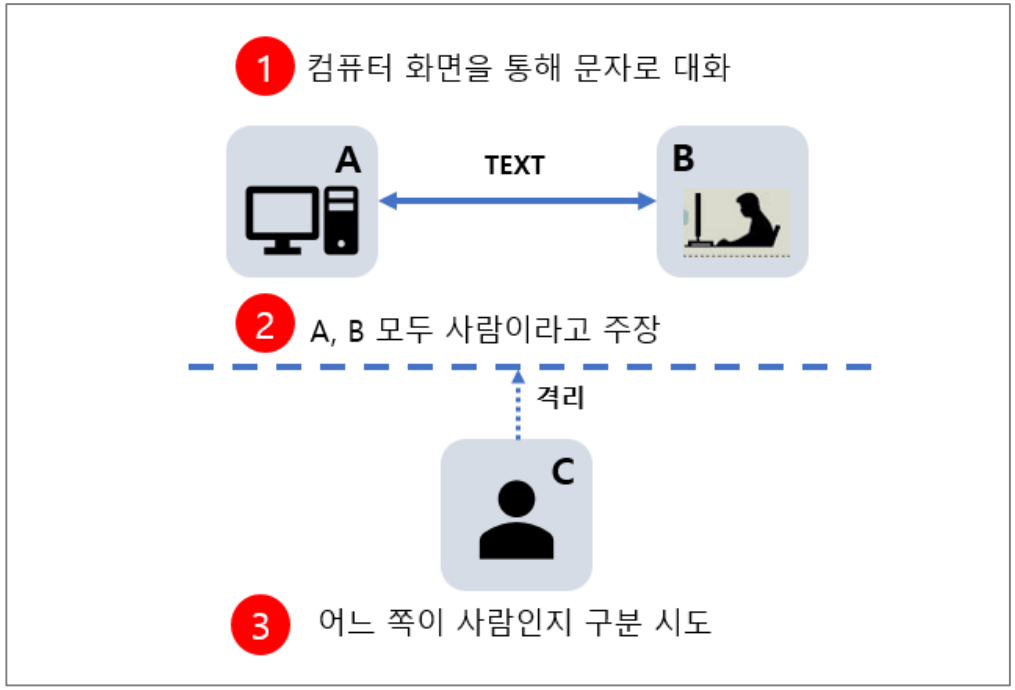
  2가지 인증 요소 결합

  Ex) ATM – 카드(Has) + 비밀번호(Knows)

Authentication - 인증

- Turing Test

  AI를 얼마나 사람답게 만들었는지 테스트

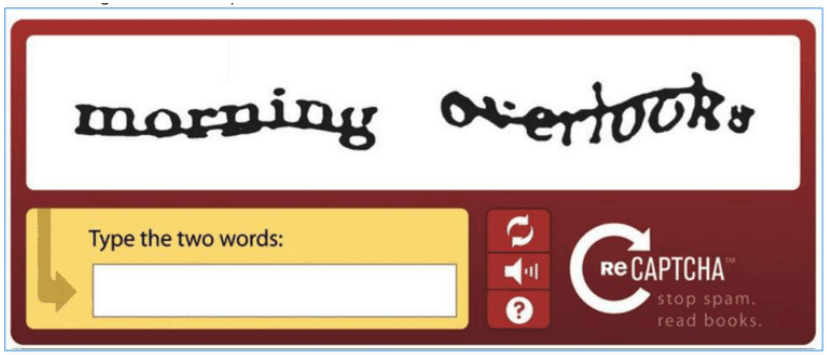


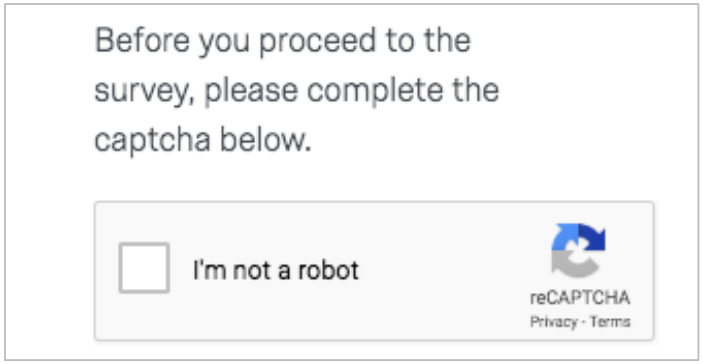
Authentication - 인증

- CAPTCHA

  Completely Automated Public Turing test to tell Computers and Humans Apart

  사람과 AI를 구별하기 위한 테스트





추가 내용

- 모듈러 연산
- 페르마의 정리
- 오일러의 정리
- RSA와 소인수 분해

감사합니다