[Security]

Encryption

Bill Kim(김정훈) | ibillkim@gmail.com

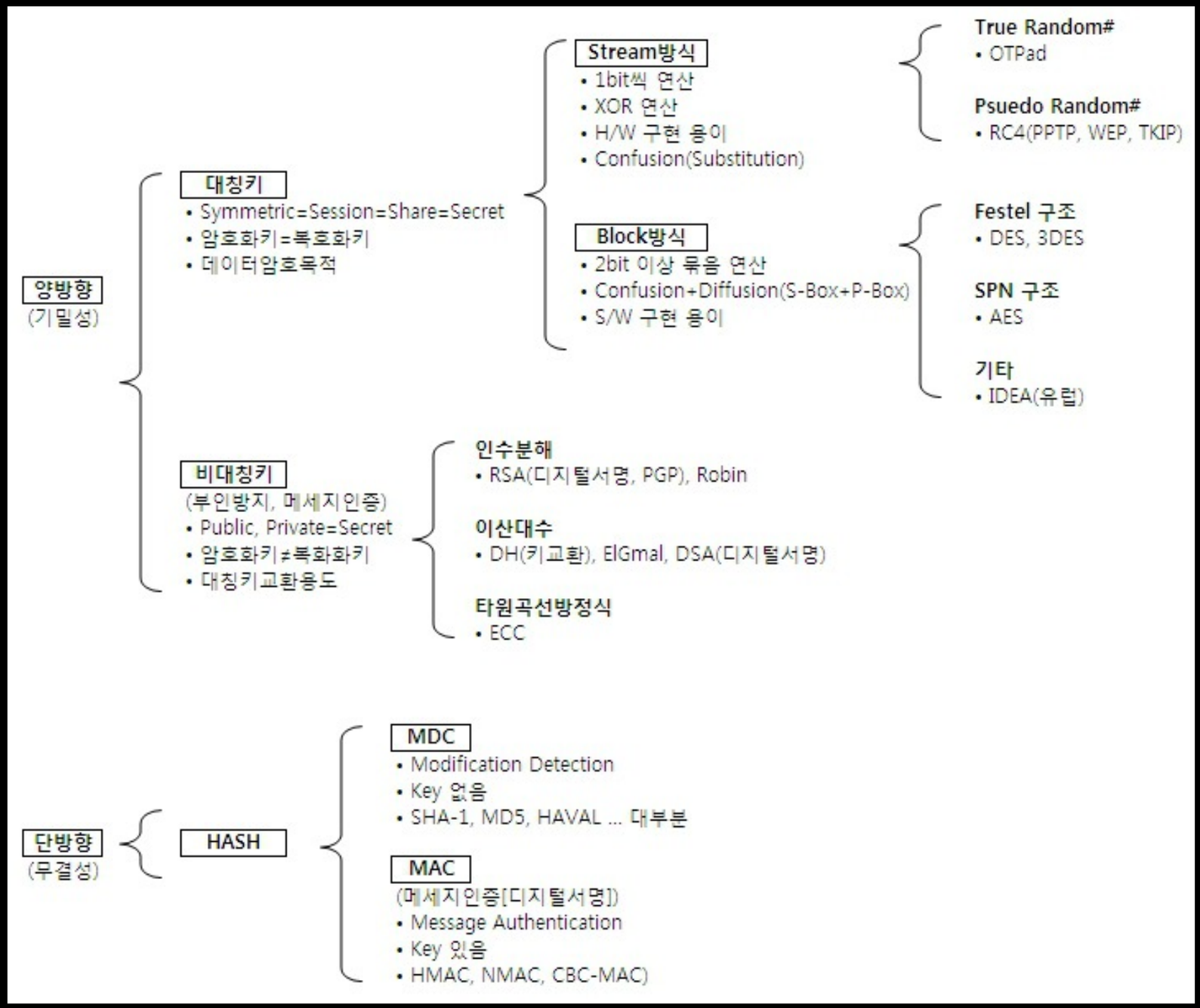
목차

Encryption?

Encryption?

평문(Plain Text) : 암호화 하기 전의 메시지
암호문(Cipher Text) : 암호화된 메시지
암호화(Encryption) : 평문을 암호문으로 변환하는 과정
복호화(Decryption) : 암호문을 평문으로 변환하는 과정

Encryption Method



Encryption Method

양방향 알고리즘 : 암호화, 복호화 가능
DES, AES, RSA

단방향 알고리즘 : 암호화 가능, 복호화 불가
MD5, SHA-1, MAC, HMAC

본 강좌에서는 양방향 알고리즘에 대해서만 다룹니다
단방향 알고리즘은 다른 강좌에서 별도로 강의

Encryption Method

블록 암호(Block cipher) :
어느 특정 비트 수의 (집합)을 한번에 처리하는 암호 알고리즘을 총칭

사용 예) DES, AES, RSA, 전자서명, 인증서 등

스트림 암호(Stream cipher) :
데이터 흐름(스트림)을 순차적으로 처리해가는 암호 알고리즘
실시간성이 중요하게 생각되는 음성, 영상 스트리밍에서 주로 사용

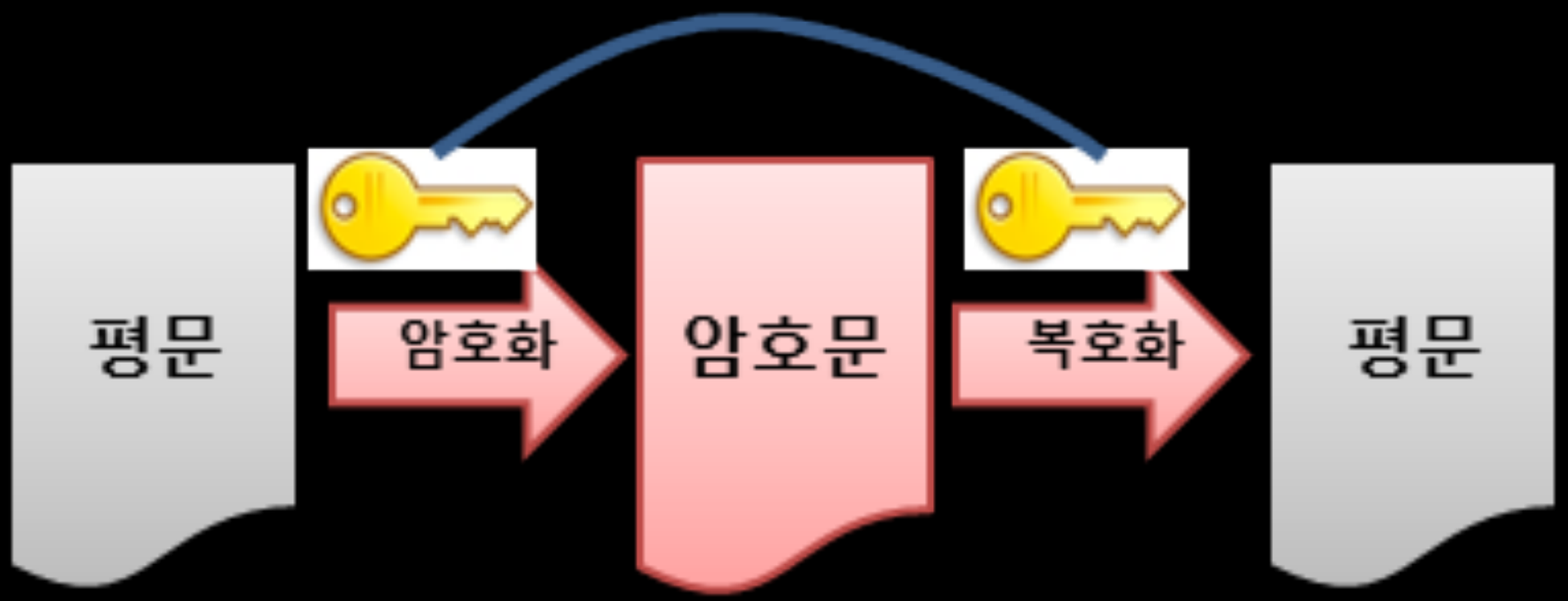
사용 예) RC4(동기식), A5/1, A5/2, A5/3 (자기 동기식)

Symmetric Encryption

대칭키(비공개키) 방식 :

- 암호화와 복호화 키가 동일함
- 키를 비공개로 하여 관리하고 복호화를 위해 전달하여야 한다
- 속도가 빠르다
- 키 배송의 위험성이 있다
- DES(Data Encryption Standard),
  AES(Advanced Encryption Standard)가 대표적임

Symmetric Encryption

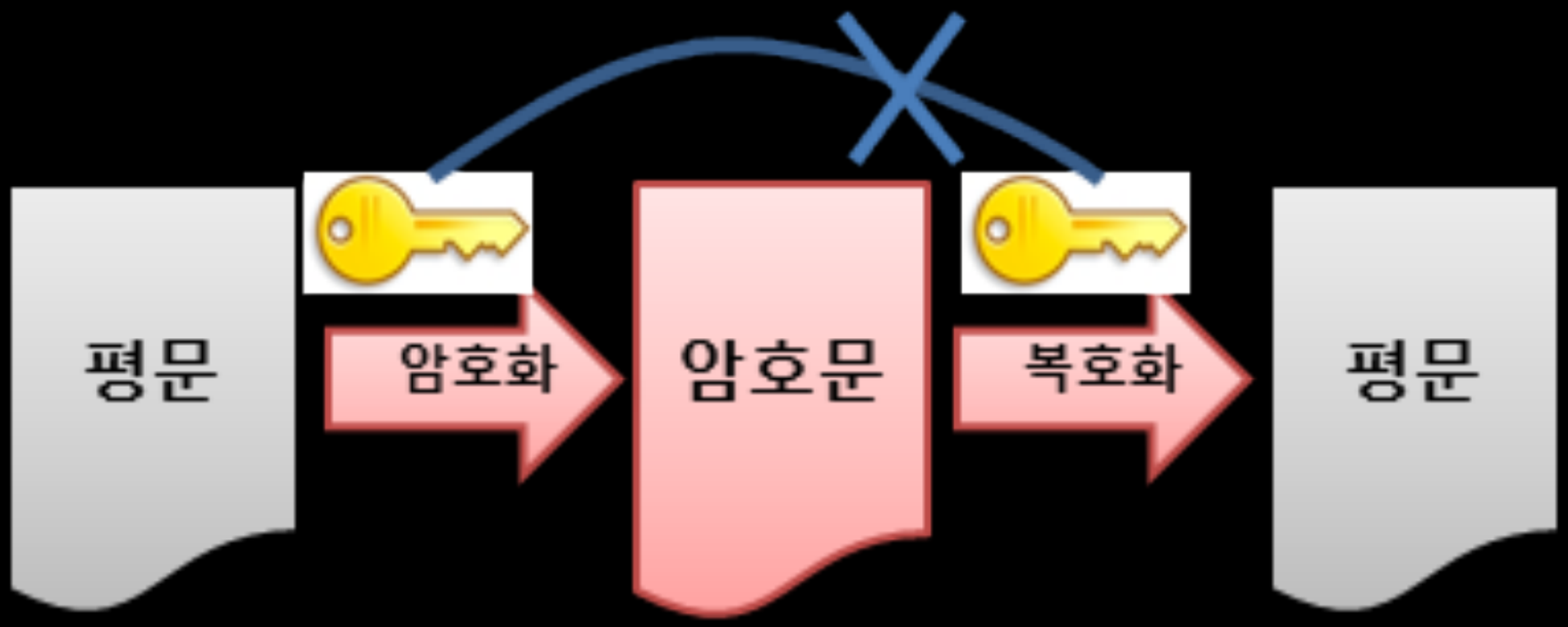


Asymmetric Encryption

비대칭키(공개키) 방식 :

- 암복호화에 사용하는 키가 서로 다른 방식
- 공개키로 암호화하고 개인키로 복호화를 한다
- 키 배송의 위험성 문제를 근본적으로 차단하여 안정성이 높다
- 대칭키 방식에 비해서 느림
- RSA(Rivet, Shamir, Adelman), DSA(디지털서명)

Asymmetric Encryption



Libraries

CryptoSwift :
https://github.com/krzyzanowskim/CryptoSwift

AndroidX :
https://thdev.tech/android/2019/12/21/Android-Security-Library/

References

References

[1] [암호화] 양방향/단방향 암호화 : https://godd.tistory.com/46

[2] 암호화 알고리즘 종류 : https://jusungpark.tistory.com/34

[3] 암호화(Encryption)와 해시(Hash) : https://baekjungho.github.io/technology-encrypt/

[4] 보안 그리고 암호화 알고리즘 : https://naleejang.tistory.com/218

[5] 암호화 양방향, 단방향, 공개키(비댕칭키), 비공개키(대칭키) 개념/분류 알고리즘 정리 : https://javaplant.tistory.com/26

References

[6] 보안 그리고 암호화 알고리즘 : https://naleejang.tistory.com/218

[7] 암호화 양방향, 단방향, 공개키(비댕칭키), 비공개키(대칭키) 개념/분류 알고리즘 정리 : https://javaplant.tistory.com/26

[8] AES와 SHA 차이 : https://brownbears.tistory.com/73

[9] 블록암호 알고리즘 vs 스트림 암호 알고리즘 : https://zoonvivor.tistory.com/140

[10] 스트림 암호화(stream cipher)와 블록 암호화(block cipher) : https://cornswrold.tistory.com/103

References

[11] AES, SHA 암호화, Swift : https://aircook.tistory.com/entry/AES-SHA-암호화-5-Swift?category=12207

[12] AndroidX에 추가된 Android Security 라이브러리는? : https://thdev.tech/android/2019/12/21/Android-Security-Library/

Thank you!