암호학(Cryptography)

1.수업소개

암호화된 내용이 먼지 몰라야 함(기밀성)

내용이 원본과 같다는 확신을 줌(무결성)

권한이 있는 사람만 접근 가능(인증)

평문(plain text) <->암호 알고리즘 <->암호문(cipher text)

암호화<->복호화

예전에는 암호 알고리즘을 숨겼음

현대에는 암호 알고리즘을 공개하고 검증받음

대신 key를 사용하여 사용(key는 공개X)

암호법 종류

1. 양방향 암호화 방식(기밀성을 위한 것)

암호화와 복호화가 둘아 일어남

1. 대칭키: AES, Twofish
2. 비대칭키: RSA
3. 단방향 암호화 방식(무결성을 위한 것) : md5, sha, CRC, RIPEMD160

암호화는 되지만 복호화는 안됨

2.단방향 암호화 방법

HASH:재료를 다지다 (되돌릴 수 없음)

Earth – [sha256 algorithm] -> 7b74b418~~670

무결성(Integrity): 어떤 파일이 변형되거나 조작되었는지 검증

<https://emn178.github.io/online-tools/md5_checksum.html>

hash 알고리즘: 무결성, 전자서명, 비밀번호 저장, 블록체인

3. 대칭키 방식(예:~~)

암호화할 때 사용하는 키와 복호화할 때 사용하는 방식이 동일

그 중 AES를 예로

<https://aesencryption.net/>

평문과 key1를 이용해 암호문을 만듬

암호문과 key1을 이용해 평문을 만듬

4.비대칭키(공개키 방식)(for 기밀성)

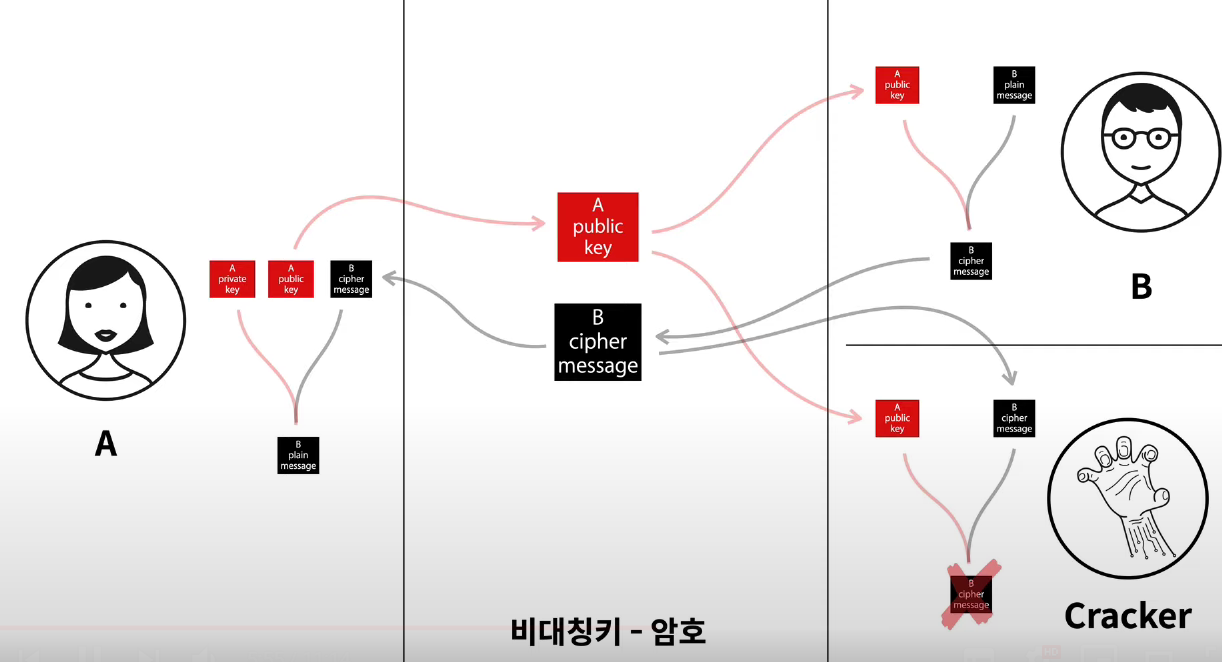
공개키(public key), 비공개키(private key)

공개키로 암호화, 비공개키로 복호화 or 비공개키로 암호화, 공개키로 복호화

내가 가진 정보를 남이 보게 하려면 키를 전달해 줘야하는데 공개키를 주면 위험해짐(제 3자도 볼 수 있기 때문에)

따라서 비대칭키 방식을 사용

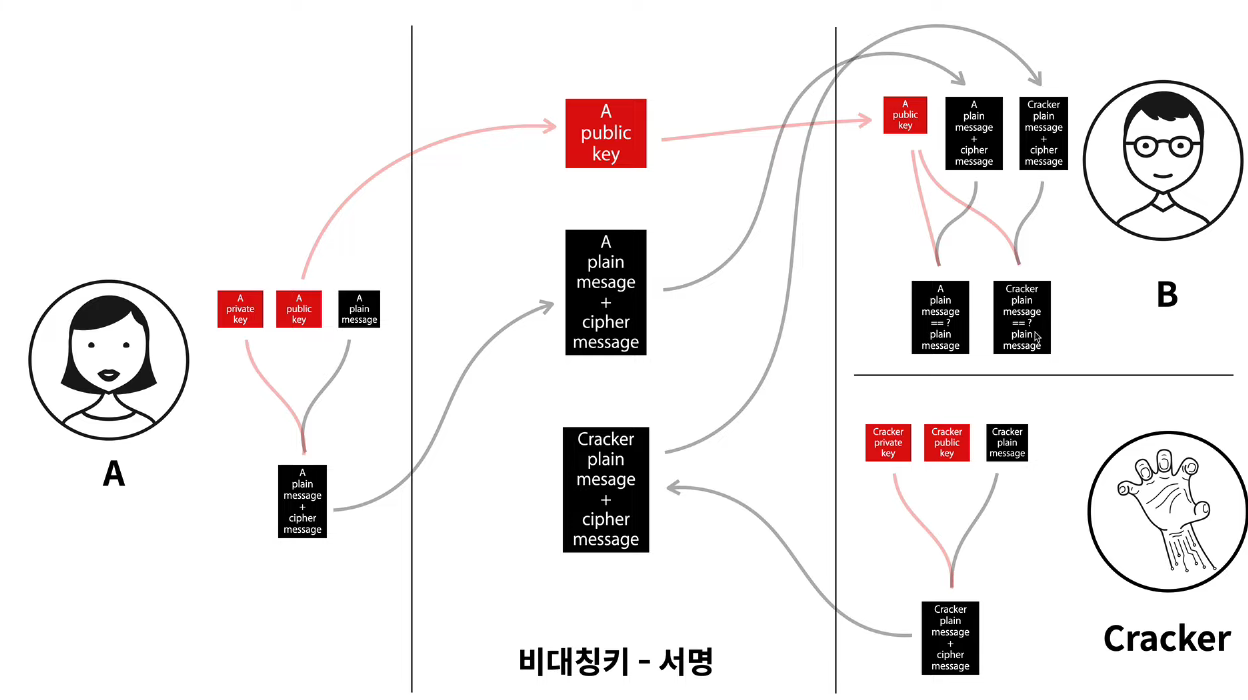
Public key는 공개하고 각자의 private key로 암호화 복호화 함



<https://www.devglan.com/online-tools/rsa-encryption-decryption>

RSA로 비밀 댓글

전자서명



A가 평문과 비공개 키로 암호문을 만들고 공개키랑 같이 공유함

B가 암호문과 공개키를 가지고 평문을 복호화함

5. 수업을 마치며

키를 잘 보관해야 함(보안)

암호의 보안=키값이 길어질수록 안전, but 관리해야 할 자원이 늘어남

국가에서 권고하는 암호 알고리즘 및 키 길이 이용 안내서

<https://www.kisa.or.kr/public/laws/laws3_View.jsp?mode=view&p_No=259&b_No=259&d_No=82&ST=total&SV=>

기술 발달에 따라 권고사항이 달라짐