

암호학 기초

<https://youtu.be/Mcd0nnAigXc>

암호화란?

양방향 암호화 방식

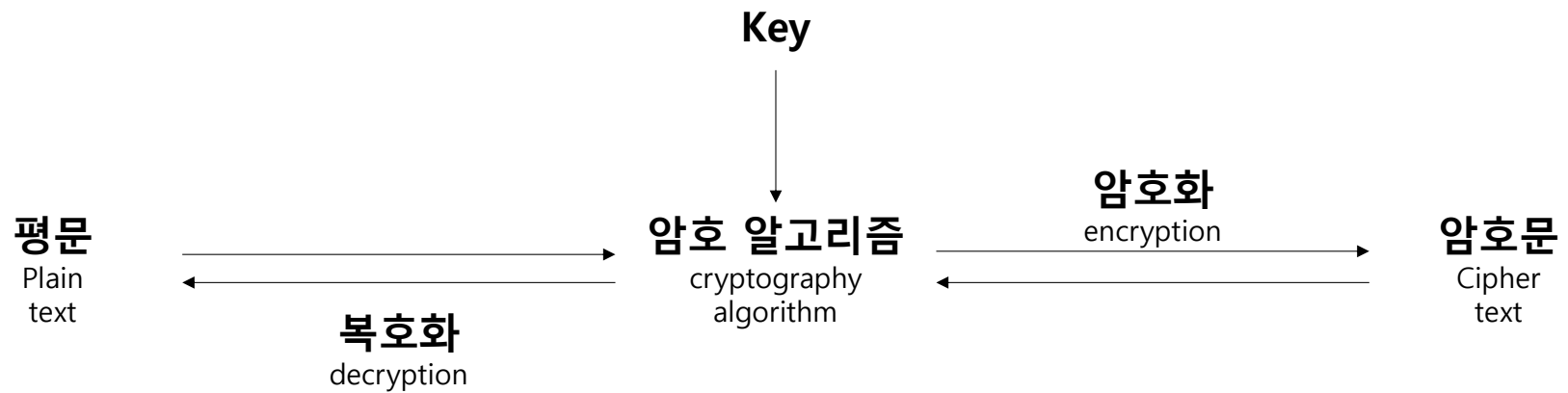
단방향 암호화 방식

암호화란?

Crypto + graphy

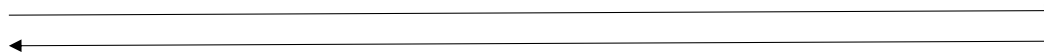
기밀성(Confidentiality), 무결성(Integrity), 인증(Authentication)

암호화란?



암호화란?

평문
Plain
text

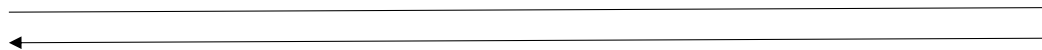


암호문
Cipher
text

양방향 암호화 방식
단방향 암호화 방식

양방향 암호화 방식

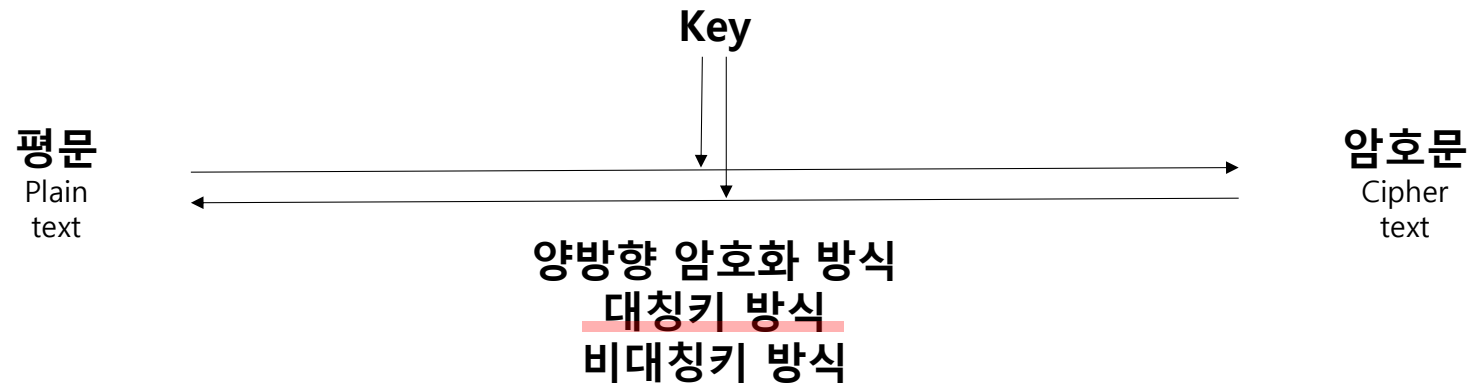
평문
Plain
text



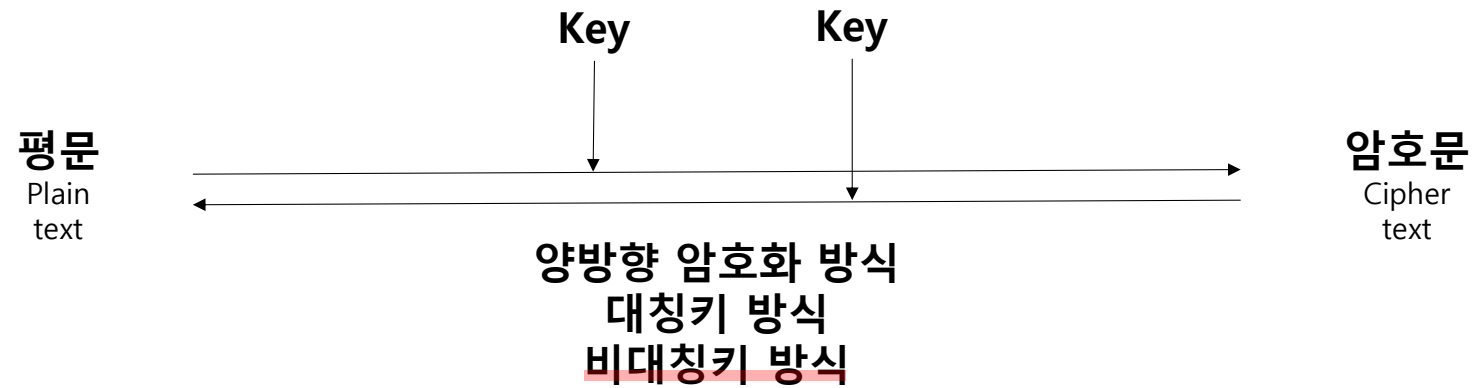
암호문
Cipher
text

양방향 암호화 방식
단방향 암호화 방식

양방향 암호화 방식



양방향 암호화 방식



단방향 암호화 방식

평문
Plain
text



양방향 암호화 방식
단방향 암호화 방식

암호문
Cipher
text

단방향 암호화 방식

HASH


CRC, MD5, RIPEMD160, SHA-1, SHA-256, SHA-512

단방향 암호화 방식

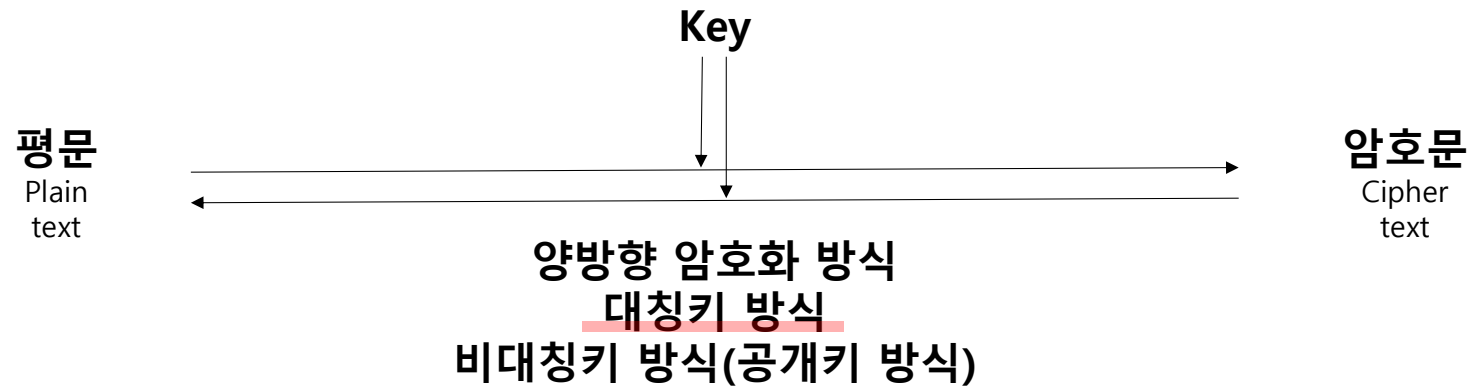


단방향 암호화 방식

macOS 13 (ARM, 64-bit), DMG Archive (mysql-8.2.0-macos13-arm64.dmg)	8.2.0	567.1M	Download
		MD5: f25feb218eb99e4ef50e06518402b330 Signature	
macOS 13 (x86, 64-bit), DMG Archive (mysql-8.2.0-macos13-x86_64.dmg)	8.2.0	572.3M	Download
		MD5: 50586d3e5ab582a65aed8719358a931a Signature	
macOS 13 (ARM, 64-bit), Compressed TAR Archive (mysql-8.2.0-macos13-arm64.tar.gz)	8.2.0	180.4M	Download
		MD5: c6d8b46d8921d030b28dd0d418862775 Signature	
macOS 13 (x86, 64-bit), Compressed TAR Archive (mysql-8.2.0-macos13-x86_64.tar.gz)	8.2.0	184.8M	Download
		MD5: ccb6c86bc5c4b84522b6c196e48ac174 Signature	
macOS 13 (ARM, 64-bit), Compressed TAR Archive Test Suite (mysql-test-8.2.0-macos13-arm64.tar.gz)	8.2.0	386.5M	Download
		MD5: cf20fcbff35457ca033d200509ae36d8 Signature	
macOS 13 (x86, 64-bit), Compressed TAR Archive Test Suite (mysql-test-8.2.0-macos13-x86_64.tar.gz)	8.2.0	387.1M	Download
		MD5: 40a8acd173fd43725cae7dfbc0b1f449 Signature	
macOS 13 (ARM, 64-bit), TAR (mysql-8.2.0-macos13-arm64.tar)	8.2.0	584.1M	Download
		MD5: 16fafe84a351d7ad4fa368302b05e105 Signature	
macOS 13 (x86, 64-bit), TAR (mysql-8.2.0-macos13-x86_64.tar)	8.2.0	590.1M	Download
		MD5: c84b733de811c1ee1444faf81f9c6679 Signature	

 We suggest that you use the [MD5 checksums and GnuPG signatures](#) to verify the integrity of the packages you download.

양방향 암호화 방식

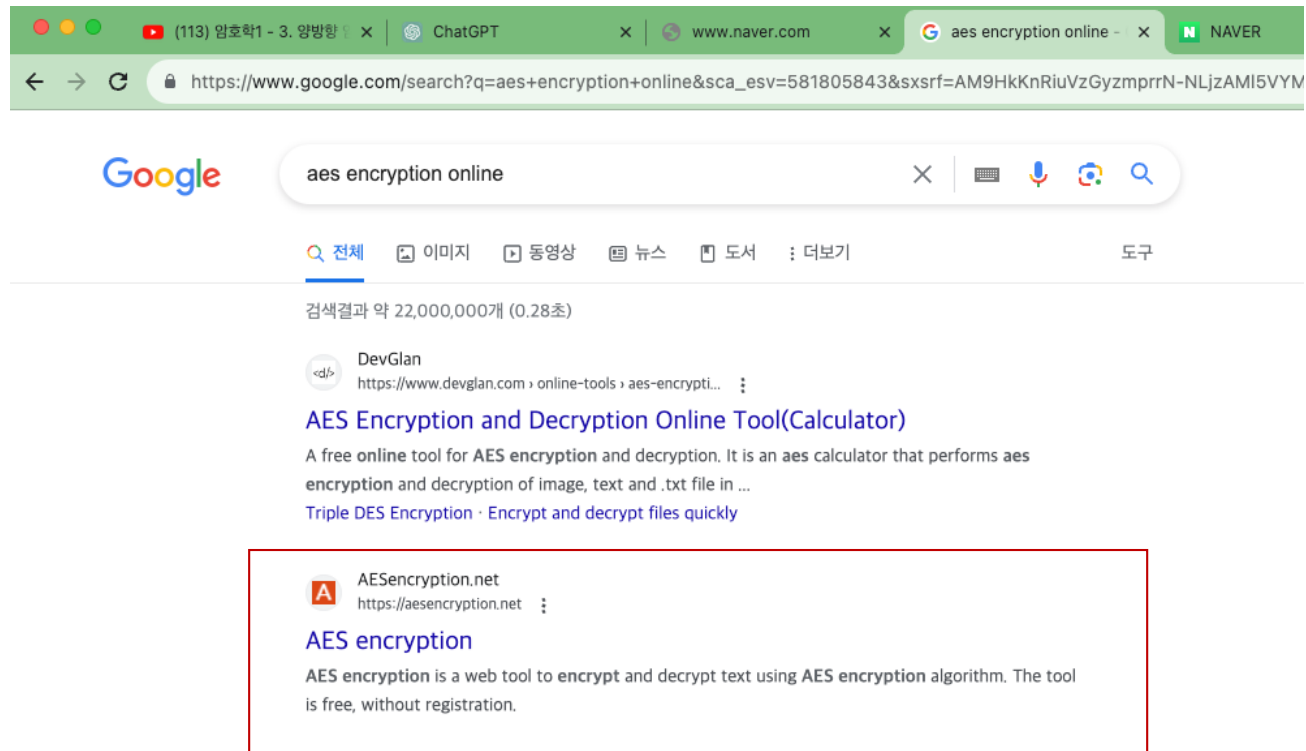


Twofish, Serpent, Blowfish, CAST5, Kuznyechik, RC4,
DES, 3DES, Skipjack, Safer+ / + + (Bluetooth), IDEA, AES

양방향 암호화 방식

AES

양방향 암호화 방식



양방향 암호화 방식

AES encryption
Encrypt and decrypt text with AES algorithm

Plain or encrypted text here

Key of the encryption

128 Bit ▼

양방향 암호화 방식

AES encryption
Encrypt and decrypt text with AES algorithm

secret

dukyoung

128 Bit

←

Ads by Google

[Stop seeing this ad](#) [Why this ad? ⓘ](#)

[Donate](#) [Encrypt](#) [Decrypt](#)

Result of encryption in base64

h5qqIWeQaQkCuBF0Kov6nw==

AES encryption
Encrypt and decrypt text with AES algorithm

h5qqIWeQaQkCuBF0Kov6nw==

dukyoung

128 Bit

←

Ads by Google

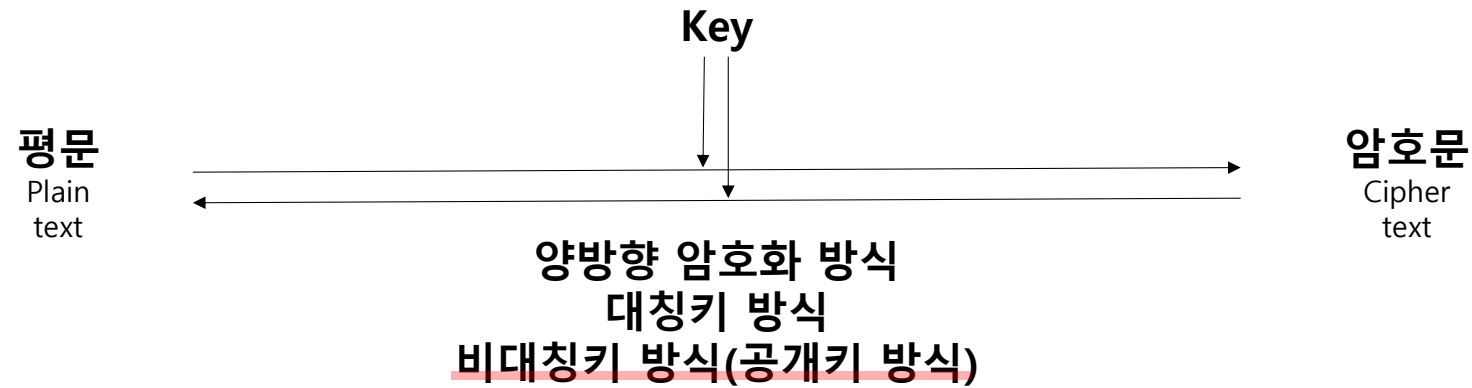
[Stop seeing this ad](#) [Why this ad? ⓘ](#)

[Donate](#) [Encrypt](#) [Decrypt](#)

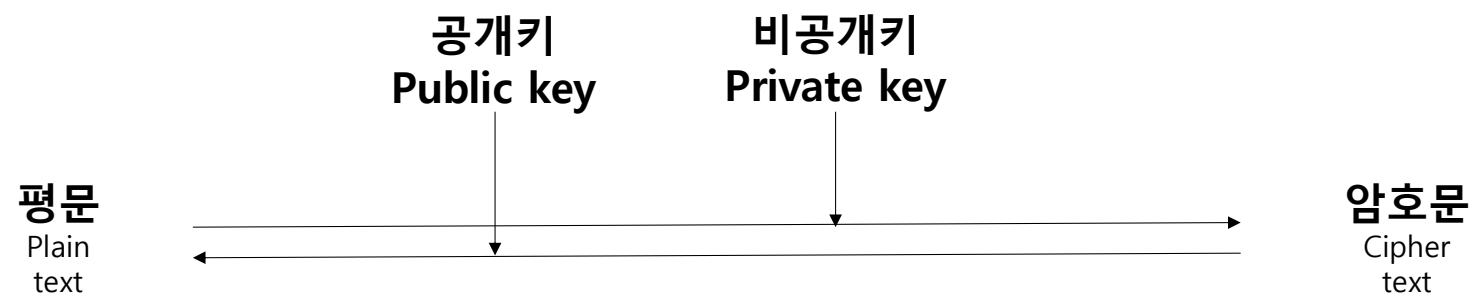
Result of decryption in plain text

secret

양방향 암호화 방식

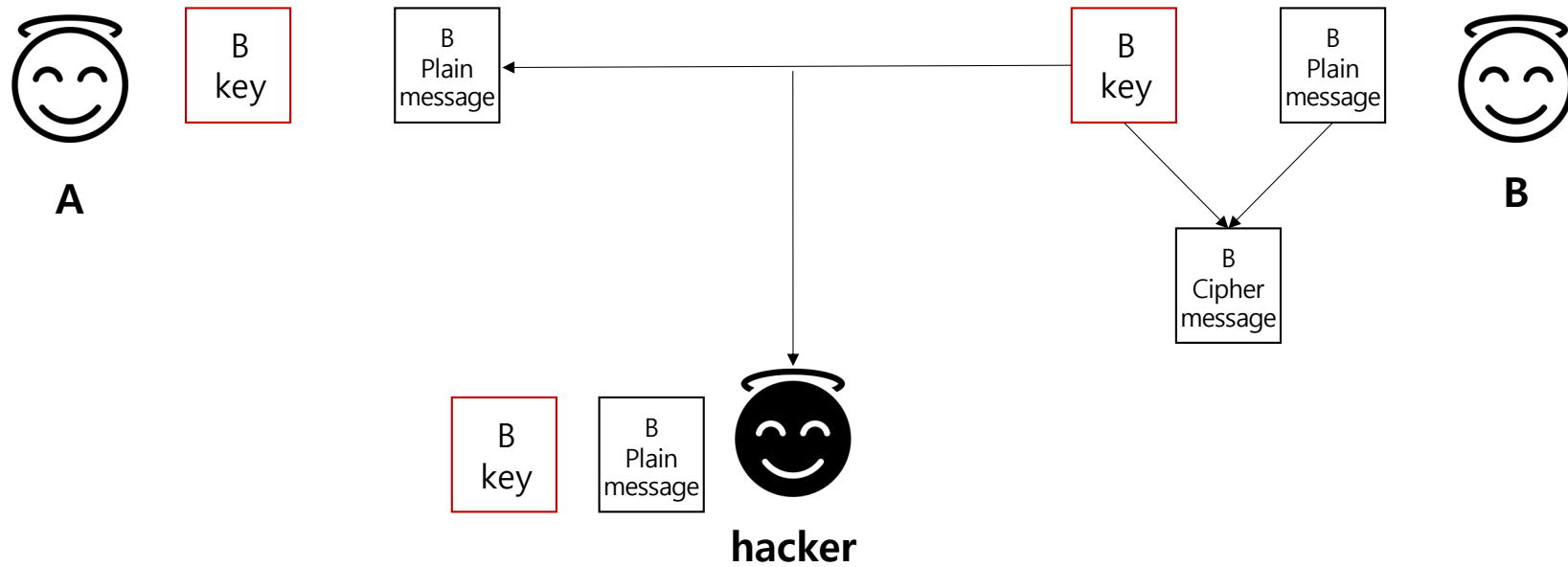


양방향 암호화 방식



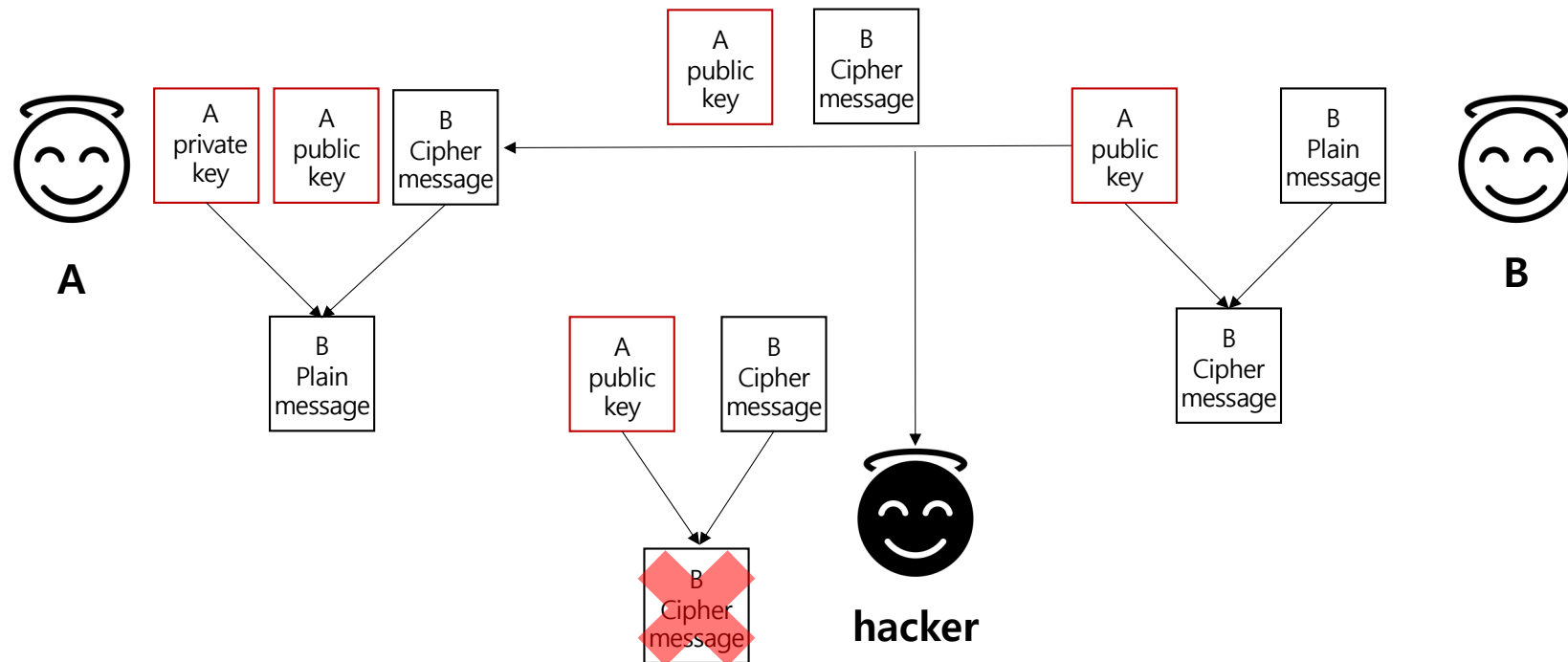
양방향 암호화 방식

대칭키(공개키) 방식의 문제점



양방향 암호화 방식

비대칭키



Q & A