Diffie-Hellman key exchange

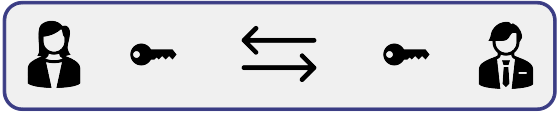
IT융합공학부 윤세영

유투브 주소: https://youtu.be/K57Vid8Mt9w

키 교환(키 합의)

두 사람이 동일한 비밀키(세션키)를 공유할 수 있도록,
일련의 패킷 등을 교환해가며 대칭 키를 합의하는 과정을 말한다.

직접적으로 키를 교환하는 것은 아니지만,
특정 규칙에 의해 각자 비밀키를 생성하더라도 결국 같은 비밀키를 갖게되는 키 합의 과정이다.



Diffie-Hellman 키 교환

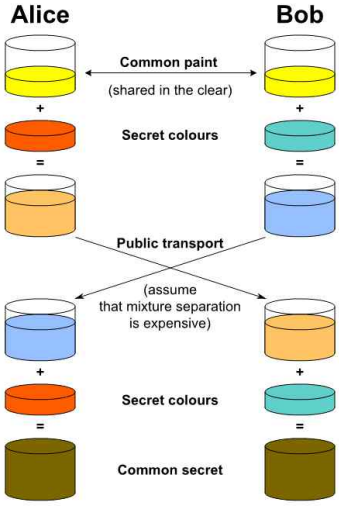
Whitfield Diffie와 Martin Hellman이 1976년에 제안한 암호 키 교환 방식이다.

두 사람이 암호화되지 않은 통신망을 통해 공통의 비밀키를 공유할 수 있도록 한다.

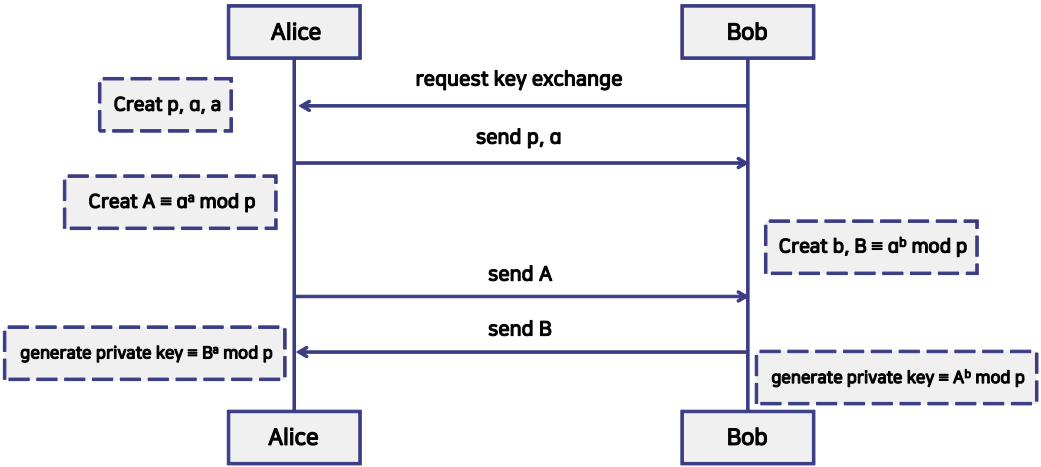
안전성은 이산대수 문제(DLP, Discrete Logarithm Problem)의 해를 찾는 것이
계산적으로 불가능하다는 것에 기반을 두고 있다.

SSH(Secure Shell), TLS(Transport Layer Security), IPSec(Internet Protocol Security)과 같이
공개되고 상업적인 암호 프로토콜에 구현되어 있다.

방법


Alice
Bob
Common paint
(shared in the clear)
+
Secret colours
+
=
=
Public transport
(assume
that mixture separation
is expensive)
+
Secret colours
+
=
=
Common secret

방법

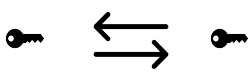

Alice
Bob
request key exchange
Creat p, α, a
send p, α
Creat A ≡ α^a mod p
Creat b, B ≡ α^b mod p
send A
send B
generate private key ≡ B^a mod p
generate private key ≡ A^b mod p
Alice
Bob

방법

A: p(소수), α, $K_{pr,a}$ 선택 (α, $K_{pr,a}$ ∈ {2, 3, ···, p-2})

B: $K_{pr,b}$ 선택 (α, $K_{pr,b}$ ∈ {2, 3, ···, p-2})

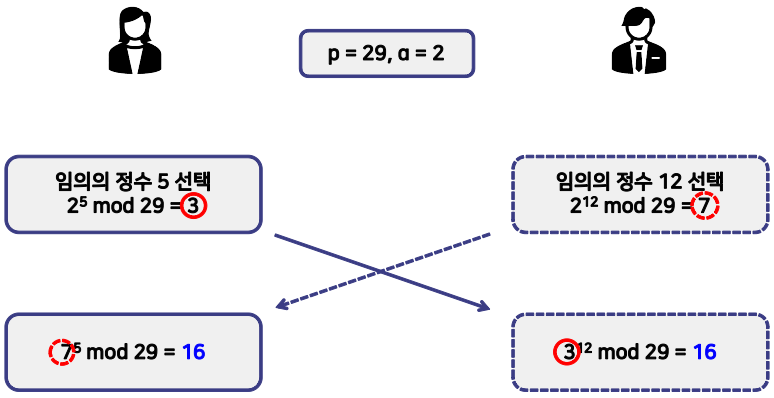
A: $K_{pub,A} \equiv \alpha^a \bmod p$ 계산 / B: $K_{pub,B} \equiv \alpha^b \bmod p$ 계산



A($K_{pub,A}$)와 B($K_{pub,B}$) 교환

$K_{AB} \equiv B^a \bmod p$ / $K_{AB} \equiv A^b \bmod p$ / ($A^b \equiv B^a \equiv \alpha^{ab}$)

Example


p = 29, α = 2
임의의 정수 5 선택
$2^5 \bmod 29 = 3$
임의의 정수 12 선택
$2^{12} \bmod 29 = 7$
$7^5 \bmod 29 = 16$
$3^{12} \bmod 29 = 16$

장점 및 단점

장점

- 신뢰할 수 있는 제 3자를 이용하지 않고도, 사전에 공유된 비밀키 없이도, 당사자들 간에 동일한 세션 키를 계산해내는 방법
- 비밀키 필요시 마다 달리 생성하여, 비밀키 보관에 따른 노출 위험성이 작아짐

단점

- 세션키를 교환하는 과정에서 진짜 상대방을 신뢰할 수 없음
- 즉, 상대방에 대한 인증 기능 없음

안전성

- Diffie-Hellman problem (디피-헬먼 문제)

α^a와 α^b로부터 α^{ab}를 구해야 하는 문제로, 이 문제를 푸는 효율적인 알고리즘이 아직까지 알려지지 않았다.

(이산 로그 문제를 효율적으로 풀 수 있을 경우 디피-헬먼 문제 또한 효율적으로 풀 수 있지만, 그 역이 참인지는 알려지지 않았음)

- 중간자 공격(man-in-the-middle attack)

공개키 알고리즘에 대한 심각한 공격으로, 악의적인 목적을 가진 사용자가 통신 객체가 전송하는 공개키를 자신의 공개키로 바꾸는 방법이다. 공개키가 인증되지 않았을 경우 이 공격이 가능하다.

Q & A