Chapter 10
Other Public-Key Cryptosystems

Chapter 10
Other Public-key Cryptosystems

$n = pq$

$y = g^x \bmod p$

Diffie-Hellman Key Exchange 공개키 암호

- History Public key cryptography
  - The scheme was first published by Whitfield Diffie and Martin Hellman in 1976, although it had been separately invented a few years earlier within GCHQ (The Government Communications Headquarters) but was kept classified.
- Key exchange [안전하지 않은데 key를 교환] 도청할 수 있는 환경 가정
  - The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel.
- The (Computational) Diffie-Hellman problem
  - Let g be a generator of some group G. For randomly chosen integers x and y, the DHP is stated informally as follows.
    - Given an element g and the values g^x and g^y, what is the value of g^{xy}?
  - Over many groups, the DHP is almost as hard as the DLP.

$g^{x1}, g^{x2} \rightarrow g^{x_1 x_2}$ 맞출수 있나? $g^{283} \bmod P, g^{782}$ 283 안알려주고 결과값 알려주고 맞추게하기

Diffie-Hellman Key Exchange

- Scheme
  1. Alice and Bob agree on a cyclic group G of (prime) order q and a generator $g \in G$.
     (Note: A cyclic group of prime order is recommended.)
  2. Alice chooses a random integer $1 \le a < q$ and sends $\mathrm{pk}_A = g^a$ to Bob.
  3. Bob chooses a random integer $1 \le b < q$ and sends $\mathrm{pk}_B = g^b$ to Alice.
  4. Alice computes $(\mathrm{pk}_B)^a = (g^b)^a = g^{ab}$.
  5. Bob computes $(\mathrm{pk}_A)^b = (g^a)^b = g^{ab}$.

0~q-1

숫자가 크기때문에 0이 나올 확률은 거의 없음. 등호는 있으나마나.

Alice

Public key : PK

Bob

g.P는 공개된 값

$PK_a = g^a \bmod P$

Alice는 $(PK_B)^a = (g^b)^a = g^{ab}$

PKA →

$PK_B = g^b \bmod P$

← PKB

BOB은 $(PK_A)^b = (g^a)^b = g^{ab}$

a는 BOB도 모름 g^b 해서 B를 보냄 결과만 앎. 서로 a.b는 모름

Diffie-Hellman Key Exchange

- Example
  1. Alice and Bob agree on $G = Z_{23}^*$ ($p = 23$, $q = 22$) and $g = 5$.
  2. Alice chooses $a = 6$ and sends $pk_A = 5^6 \bmod 23 = 8$.
  3. Bob chooses $b = 15$ and sends $pk_B = 5^{15} \bmod 23 = 19$.
  4. Alice computes $(pk_B)^a = 19^6 \bmod 23 = 2$.
  5. Bob computes $(pk_A)^b = 8^{15} \bmod 23 = 2$.

$5^{22} \equiv 1$ generator

- Alice 가 보관

- BOB이 보관

5^6 인지 5^7 인지 모름

실제로는 10진수로 천자리

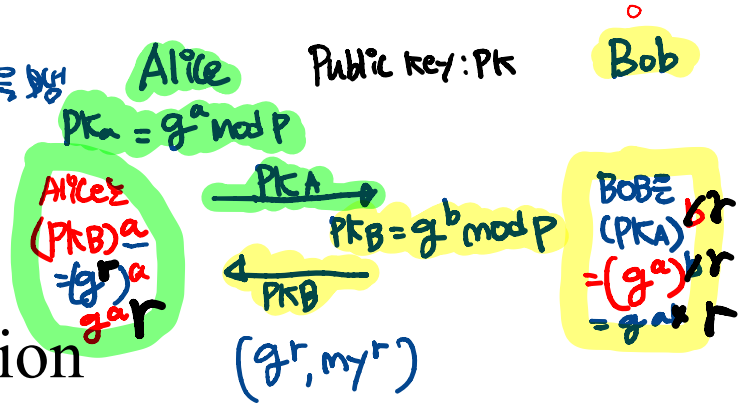
두사람만 그라는 것을 앎.

ElGamal Encryption Diffi hellman 의확장. 불적바꿈

- Key generation
  - Alice chooses a cyclic group G of (prime) order q and a generator $g \in G$.
  - Alice chooses a private key $x \in \{1, \ldots, q-1\}$ randomly and computes her public key $y = g^x$. x는 보통 알고있음. b를 한번쓰고 버리는적 $y^r = g^x$
- Encryption
  - Bob chooses a random integer $r \in \{1, \ldots, q-1\}$ and computes $c_1 = g^r$.
  - To encrypt a message $m \in G$, Bob calculates $c_2 = my^r$ $(= mg^{xr})$.
  - Bob sends the ciphertext (c_1, c_2) to Alice.
- Decryption PK를 다시 보내줘야만 한번쓰고 버리는것을 확인
  - Alice computes $c_2 (c_1^x)^{-1} = mg^{xr} (g^{rx})^{-1} = m$.

Extend Euclidean

a대신 x



- Decisional Diffie-Hellman assumption
  - The DDH assumption states that the probability distributions (g^a, g^b, g^{ab}) and (g^a, g^b, g^c) are computationally indistinguishable, where a, b, and c are randomly chosen from Z_q.

ElGamal Encryption

- Example

(Key generation)

- Alice chooses $G = Z_{19}^*$ ($p = 19$, $q = 18$) and $g = 10$.
- Alice chooses the private key $x = 5$ and computes the public key $y = g^x = 10^5 \bmod 19 = 3$.

(Encryption)

- Bob chooses $r = 6$ and computes $c_1 = g^r = 10^6 \bmod 19 = 11$.
- To encrypt $m = 17$, Bob calculates $c_2 = my^r = 17 \cdot 3^6 \bmod 19 = 5$.
- Bob sends the ciphertext $(c_1, c_2) = (11, 5)$ to Alice.

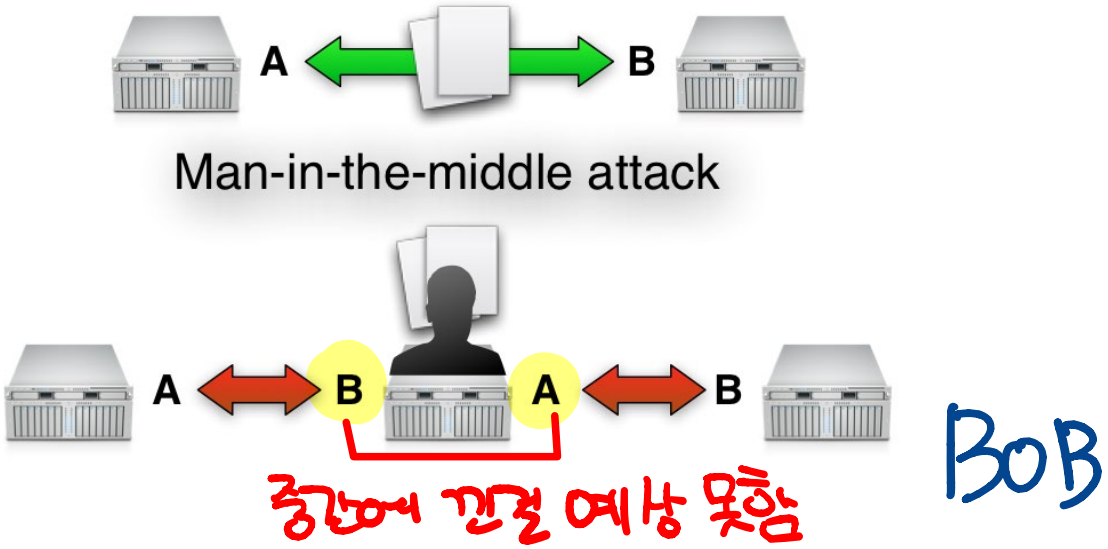
(Decryption)

- Alice computes $m = c_2 (c_1^x)^{-1} = 5 \cdot (11^5)^{-1} \bmod 19 = 17$

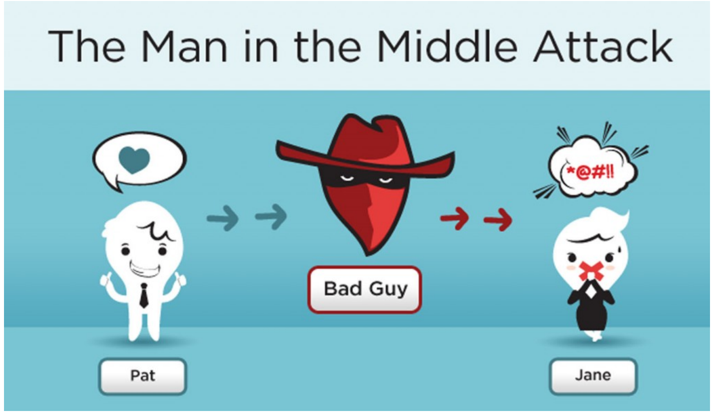
where $5 \cdot (11^5)^{-1} \equiv 5 \cdot (7)^{-1} \equiv 5 \cdot 11 \equiv 17 \pmod{19}$.

Man-in-the-Middle Attack

- In cryptography and computer security, a man-in-the-middle attack (often abbreviated to MITM, MitM, MIM, MiM or MITMA) is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other.



Man-in-the-Middle Attack



DH

Alice g^a → g^a

Carol c

Bob g^b ← b

g^c ← g^{ac} g^{bc} → g^c

Alice랑 Bob은 서로 통신하는줄 앎. Carol이랑 소통 (문제3)