Diffie-Hellman Key Change

목차

Diffie-Hellman Key Exchange

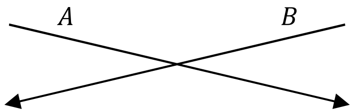
Reference: (Stallings, 2014)

- Diffie-Hellman Key Exchange
  - 최초 소개된 공개키 알고리즘 (1976)
  - 두 사용자 간에 안전하지 않은 채널을 통해 안전한 방식으로 서로 간에 공유하는 대칭키를 확보할 수 있는 방법 제공
    - 확보된 대칭키는 AES 등의 대칭키 암호알고리즘의 키로 사용
  - 이산로그 계산의 어려움에 기반

Diffie-Hellman Key Exchange

Reference: (Stallings, 2014; Paar & Pelzl, 2010)

Alice	Bob
큰 소수 p와 Z_p^*에서의 원시근 α는 공개되어 있다고 가정	큰 소수 p와 Z_p^*에서의 원시근 α는 공개되어 있다고 가정
Alice는 개인값 a를 선택 $(1 \leq a \leq p-1)$	Bob은 개인값 b를 선택 $(1 \leq b \leq p-1)$
Alice는 $A = \alpha^a \ mod \ p$를 계산하여 얻은 공개값 A를 Bob에게 송신	Bob은 $B = \alpha^b \ mod \ p$를 계산하여 얻은 공개값 B를 Alice에게 송신
Alice는 Bob의 공개값 B를 평문으로 수신	Bob은 Alice의 공개값 A를 평문으로 수신
Alice는 $K = B^a \ mod \ p$를 계산하여 대칭키 K를 획득	Bob은 $K = A^b \ mod \ p$를 계산하여 대칭키 K를 획득



Alice와 Bob이 각각 계산한 대칭키 K는 동일한가?

- Alice가 $B^a \ mod \ p$를 통해 계산하는 대칭키는 다음과 같은 값이다
  $$K_{Alice} = B^a \ mod \ p = \left(\alpha^b \ mod \ p\right)^a \ mod \ p = \boldsymbol{\alpha^{ab} \ mod \ p = K}$$
- Bob이 $A^b \ mod \ p$를 통해 계산하는 대칭키는 다음과 같은 값이다
  $$K_{Bob} = A^b \ mod \ p = (\alpha^a \ mod \ p)^b \ mod \ p = \boldsymbol{\alpha^{ab} \ mod \ p = K}$$
- 즉 Alice와 Bob이 계산한 대칭키는 동일함 $K_{Alice} = \alpha^{ab} \ mod \ p = K_{Bob}$

공격자는 알려진 값들 p, α, A, B로부터 K를 계산할 수 있는가?

- $K = B^a \ mod \ p$를 계산하려면 a를 계산해야 함
- 그러나 a를 계산하려면 $\alpha^a \ mod \ p = A$를 만족하는 a를 찾아야 하므로 이는 이산대수문제에 해당 → a의 모든 가능한 값을 하나씩 대입하면서 $\alpha^a \ mod \ p = A$를 만족하는지 확인해야 함

DHKE 예

Reference: (Paar & Pelzl, 2010)

Alice

큰 소수 $p = 29$, 원시근 $\alpha = 2$ 공개되어 있음

Alice는 개인값 $a = 5$를 선택 $(1 \leq a \leq p-1)$

Alice는 $A = \alpha^a \; mod \; p = 2^5 \; mod \; 29 = 3$를 계산하여 얻은 공개값 $A = 3$을 Bob에게 송신

Alice는 Bob의 공개값 $B = 7$을 평문으로 수신

Alice는 $K = B^a \; mod \; p = 7^5 \; mod \; 29 = 16$를 계산하여 대칭키 $K = 16$을 획득

$K = B^a \; mod \; p = \left(\alpha^b \; mod \; p\right)^a \; mod \; p = \alpha^{ab} \; mod \; p$

$A = 3$ $\qquad$ $B = 7$

Bob

큰 소수 $p = 29$, 원시근 $\alpha = 2$ 공개되어 있음

Bob은 개인값 $b = 12$를 선택 $(1 \leq b \leq p-1)$

Bob은 $B = \alpha^b \; mod \; p = 2^{12} \; mod \; 29 = 7$를 계산하여 얻은 공개값 $B = 7$을 Alice에게 송신

Bob은 Alice의 공개값 $A = 3$을 평문으로 수신

Bob은 $K = A^b \; mod \; p = 3^{12} \; mod \; 29 = 16$를 계산하여 대칭키 $K = 16$을 획득

$K = A^b \; mod \; p = (\alpha^a \; mod \; p)^b \; mod \; p = \alpha^{ab} \; mod \; p$

Alice와 Bob이 각각 계산한 대칭키 K는 동일한가?

- Alice가 $B^a \; mod \; p$를 통해 계산하는 대칭키는 다음과 같은 값이다
  $B^a \; mod \; p = \left(\alpha^b \; mod \; p\right)^a \; mod \; p = \alpha^{ab} \; mod \; p = 2^{5 \cdot 12} \; mod \; 29 = 16 = K$
- Bob이 $K = A^b \; mod \; p$를 통해 계산하는 대칭키는 다음과 같은 값이다
  $A^b \; mod \; p = (\alpha^a \; mod \; p)^b \; mod \; p = \alpha^{ab} \; mod \; p = 2^{5 \cdot 12} \; mod \; 29 = 16 = K$

공격자는 $p = 29, \alpha = 2, A = 3, B = 7$로부터 K를 계산할 수 있는가?

- $K = B^a \; mod \; p = 7^a \; mod \; 29$를 계산하려면 a를 계산해야 함
- 그러나 a를 계산하려면 $\alpha^a \; mod \; p = A$로부터 $2^a \; mod \; 29 = 3$을 만족하는 a를 찾아야 하므로 이는 이산대수문제에 해당 → a의 모든 가능한 값을 하나씩 대입하면서 $2^a \; mod \; 29 = 3$을 만족하는지 확인해야 함

DHKE 예

Reference: (Stallings, 2014)

Alice

큰 소수 $p = 353$, 원시근 $\alpha = 3$ 공개되어 있음

Alice는 개인값 $a = 97$를 선택 $(1 \le a \le p - 1)$

Alice는 $A = \alpha^a \ mod\ p = 3^{97} \ mod\ 353 = 40$를 계산하여 얻은 공개값 $A = 40$을 Bob에게 송신

Alice는 Bob의 공개값 $B = 248$을 평문으로 수신

Alice는 $K = B^a \ mod\ p = 248^{97} \ mod\ 353 = 160$를 계산하여 대칭키 $K = 160$을 획득

$K = B^a \ mod\ p = \left(\alpha^b \ mod\ p\right)^a \ mod\ p = \alpha^{ab} \ mod\ p$

$A = 40$ $\quad$ $B = 248$

Bob

큰 소수 $p = 353$, 원시근 $\alpha = 3$ 공개되어 있음

Bob은 개인값 $b = 233$를 선택 $(1 \le b \le p - 1)$

Bob은 $B = \alpha^b \ mod\ p = 3^{233} \ mod\ 353 = 248$를 계산하여 얻은 공개값 $B = 248$을 Alice에게 송신

Bob은 Alice의 공개값 $A = 40$을 평문으로 수신

Bob은 $K = A^b \ mod\ p = 40^{233} \ mod\ 353 = 160$를 계산하여 대칭키 $K = 160$을 획득

$K = A^b \ mod\ p = (\alpha^a \ mod\ p)^b \ mod\ p = \alpha^{ab} \ mod\ p$

Alice와 Bob이 각각 계산한 대칭키 K는 동일한가?

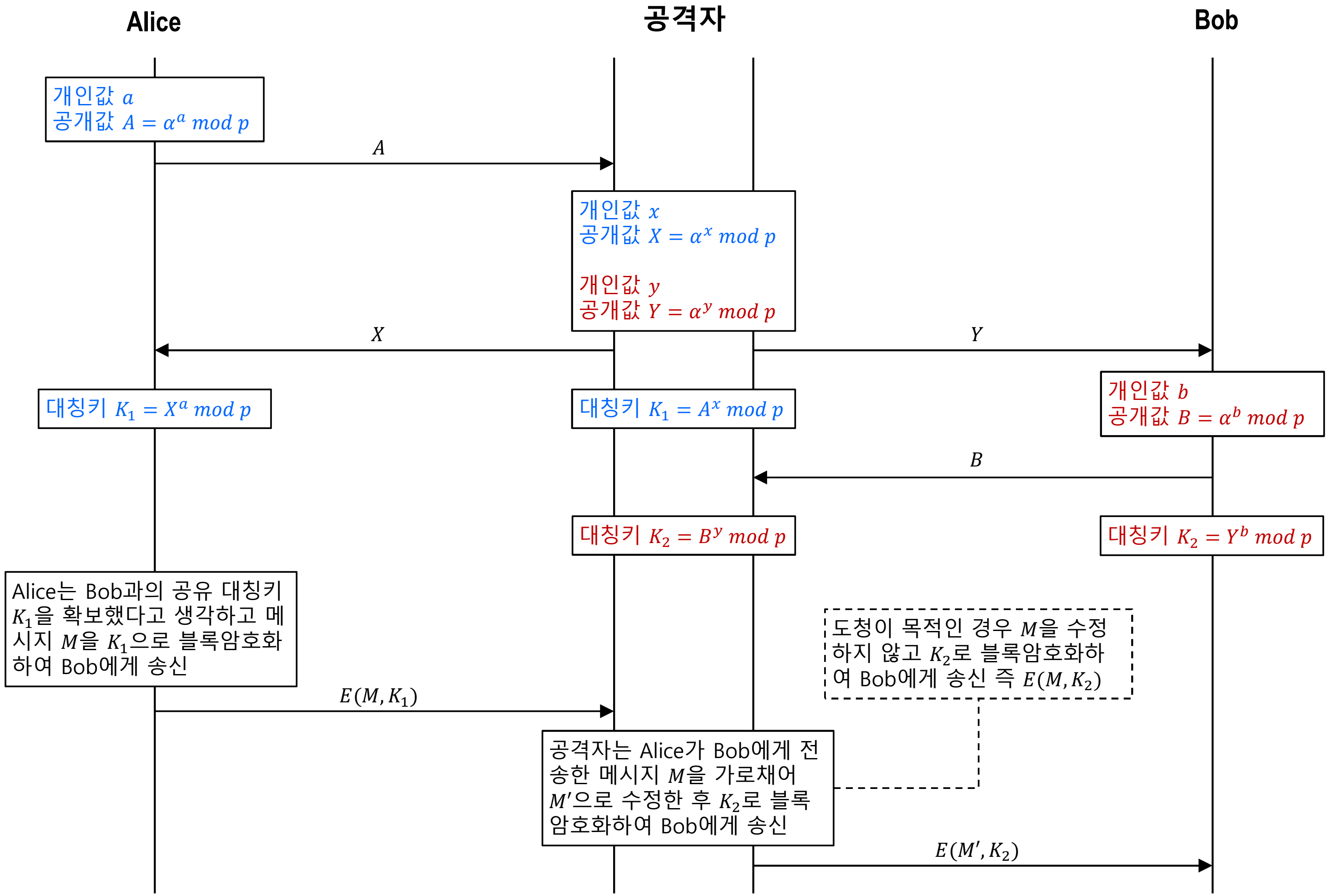
- Alice가 $B^a \ mod\ p$를 통해 계산하는 대칭키는 다음과 같은 값이다
  $B^a \ mod\ p = \left(\alpha^b \ mod\ p\right)^a \ mod\ p = \alpha^{ab} \ mod\ p = 3^{97 \cdot 233} \ mod\ 353 = 160 = K$
- Bob이 $K = A^b \ mod\ p$를 통해 계산하는 대칭키는 다음과 같은 값이다
  $A^b \ mod\ p = (\alpha^a \ mod\ p)^b \ mod\ p = \alpha^{ab} \ mod\ p = 3^{97 \cdot 233} \ mod\ 353 = 160 = K$

공격자는 $p = 353, \alpha = 3, A = 40, B = 248$로부터 K를 계산할 수 있는가?

- $K = B^a \ mod\ p = 248^a \ mod\ 353$를 계산하려면 a를 계산해야 함
- 그러나 a를 계산하려면 $\alpha^a \ mod\ p = A$로부터 $3^a \ mod\ 353 = 40$을 만족하는 a를 찾아야 하므로 이는 이산대수문제에 해당
  → a의 모든 가능한 값을 하나씩 대입하면서 $3^a \ mod\ 353 = 40$을 만족하는지 확인해야 함

DHKE에서의 Man-in-the-middle attack

Reference: (Stallings, 2014)



References

- Behrouz A. Forouzan, Cryptography and Network Security, McGraw-Hill, 2008
- William Stallings, Cryptography and Network Security: Principles and Practice, Sixth Edition, Prentice Hall, 2014
- Christof Paar, Jan Pelzl, Understanding Cryptography: A Textbook for Students and Practitioners, Springer, 2010
- 김명환, 수리암호학개론, 2019
- 정민석, 암호수학, 경문사, 2017
- 최은미, 정수와 암호론, 북스힐, 2019
- 이민섭, 정수론과 암호론, 교우사, 2008
- Kevin S. McCurley, The Discrete Logarithm Problem, Proceedings of Symposia in Applied Mathematics, Vol 42, 1990