네트워크 보안 에센셜

- 3장 공개키 암호와 디지털 서명 -

명 세 인 (sein@pel.smuc.ac.kr)

상명대학교 프로토콜공학연구실

목 차

- 공개키 암호 원리
- 공개키 암호 알고리즘
- 디지털 서명

공개키 암호 원리

- 공개키 암호 (Public-key Encryption)
  - 1976년 Diffie와 Hellman에 의해 개발
  - 수학적 함수에 근거
  - 두 개의 키를 사용하는 비대칭 방식
  - 기밀성, 키 분배, 인증분야에서 성능이 뛰어남

  - RSA 알고리즘, Diffie-Hellman 알고리즘 등이 있음

공개키 암호 원리

- 공개키 암호 (Public-key Encryption)
  - 공개 키와 비밀 키 비교 표

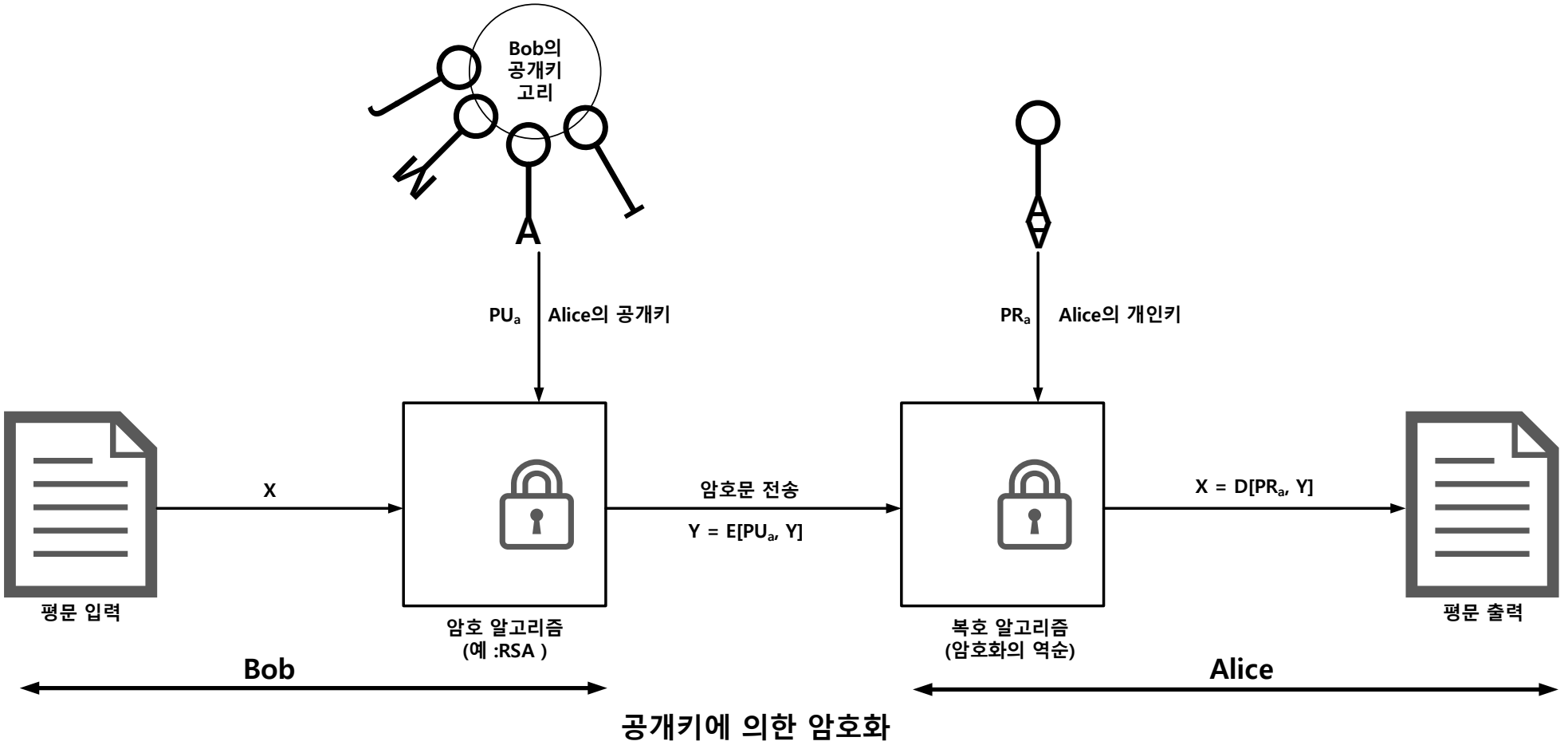
암호	비밀 키	공개키
키 사용	대칭 키	비대칭
암호 방식	대체, 치환	수학 함수 응용
장점	계산이 빠름 알고리즘이 다양	암호 키 사전 공유 불필요 통신 대상 추가
단점	키 분배, 관리	계산 이 느림
사용자(N)와 키의 개수	$\frac{N \times (N-1)}{2}$	$2 \times N$

공개키 암호 원리

- 공개키 암호 구조
  - 평문
    암호화 되지 않은 데이터
  - 암호 알고리즘
    평문을 변환하는 알고리즘
  - 공개 키와 개인 키
    한 쌍으로 이뤄짐, 하나는 암호화, 다른 하나는 복호화에 사용
  - 암호문
    암호 알고리즘의 출력으로 나오는 암호화된 메시지
  - 복호 알고리즘
    암호화시 사용한 키에 대응하는 키를 사용하여 평문으로 변환

공개키 암호 원리

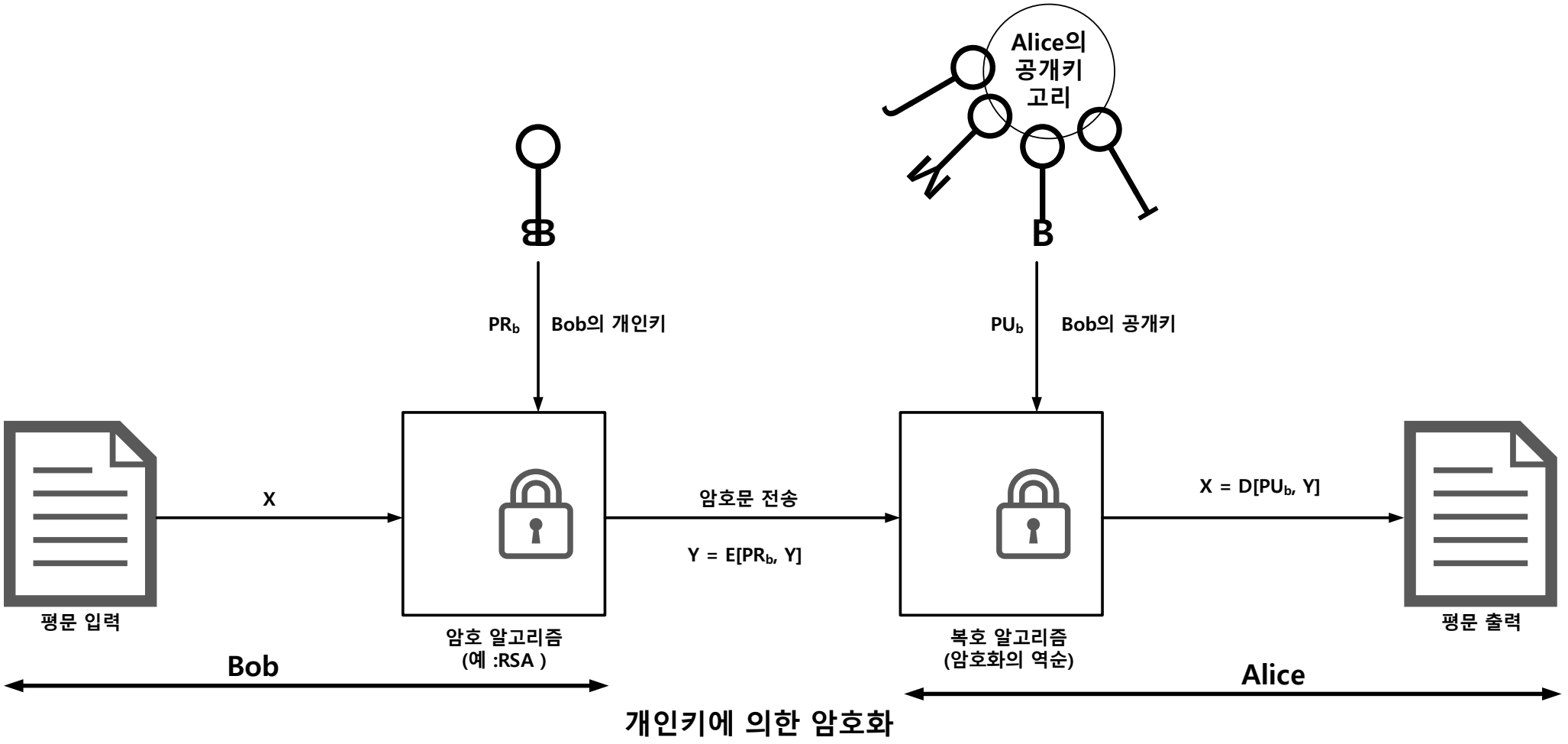
- 공개키 암호 구조



공개키에 의한 암호화

공개키 암호 원리

- 공개키 암호 구조



공개키 암호 원리

- 공개키 암호 요건

1. Bob이 한 쌍의 키 생성(공개키:PU_b, 개인키:PR_b)이 쉬워야 함 (수학 공식에 기반하여)
2. 암호문을 쉽게 만들 수 있어야 함
   - $C = E(PU_b, M)$
3. 복호화가 쉬워야 함
   - $M = D(PR_b, C) = D[PR_b, E(PU_b,M)]$
4. 키 쌍중 하나만 알더라도 경우 다른 하나를 예측할 수 없어야 함
5. 공개키로 암호화 된 암호문 과 공개 키를 알고 있어도 해독이 어려움
6. 키 쌍이 암호화 복호화 가 바뀔 수 있음
   - $M = D[PU_b, E(PR_b, M)] = D[PR_b, E(PU_b, M)]$
7. 평문은 키 값보다 짧아야 함

공개키 암호 원리

- 공개키 암호 응용
  - 암호화 복호화 (Encryption/Decryption)
    - 송신자는 수신자의 공개 키를 이용하여 메시지 암호화
  - 디지털 서명 (Digital Signature)
    - 송신자는 자신의 개인키로 서명을 함 (전체 메시지에 적용하거나 메시지를 대신하는 작은 데이터 블록 이용)
  - 키 교환 (Key Exchange)
    - 양측은 세션 키를 교환하기 위해 협조, 여러 방법이 있음
  - 공개키 알고리즘 비교 표

알고리즘	암호/ 복호	디지털 서명	키 교환
RSA	Y	Y	Y
Diffie-Hellman	N	N	Y
DSS	N	Y	N
ECC	Y	Y	Y

공개키 암호 알고리즘

- RSA 공개키 암호 알고리즘
  - 1977년 MIT의 Ron Rivest, Adi Shamir, Len Adleman 이 만들어 1978년 최초로 출판
  - 공개키로 암호화 하며, 개인키로 복호화
  - 키값, 평문, 암호문을 모두 숫자로 취급하는 연산

공개키 암호 알고리즘

- RSA 공개키 암호 알고리즘
  - RSA 알고리즘의 용어
    - M, C: 평문과 암호문
    - p, q: 키를 만들기 위해 생성된 소수 값
    - n: 키의 인자가 될 값 (p*q)
      사용되는 모든 값은 n보다 작아야 함
    - e: n과 공개키 인자로 유도된 값 (PU{e, n})
    - d: n과 개인키 인자로 유도된 값 (PR{d, n})
  - RSA 알고리즘의 조건
    - n보다 작은 모든 정수 M 에 대해서 $M = M^{ed} \bmod n$을 만족하는 값 e, d, n을 구할 수 있어야 함
    - n보다 작은 모든 정수 M 에 대해서 M^e와 C^d를 구하는 것이 비교적 쉬워야 함
    - e와 n이 주어지더라도 d를 구하는 것이 불가능 해야 함 (기밀성)
      (e와 n이 충분히 크면 충족)

공개키 암호 알고리즘

- RSA 공개키 암호 알고리즘
  - RSA 알고리즘의 동작
    - 키 생성
      1. 서로 다른 소수 p, q 선택
      2. $n = p \times q$계산
      3. $\varphi(n) = (p-1)(q-1)$을 계산 (소수에 대해 곱의 결합법칙 가능)
         - $\varphi(n)$: 주어진 자연수 n 보다 작은 자연수 중 n과 서로소인 수의 개수를 구하는 오일러(Euler)함수, n이 소수 일 경우 $\varphi(n) = n - 1$
      4. $\varphi(n)$ 보다작은 서로소 e 값 계산, PU={e, n}
      5. $de \bmod \varphi(n) = 1$ 를 만족하는 d를 계산 PR={d, n}
      6. 공개키 PU = {e, n}, 개인키 PR = {d, n}

공개키 암호 알고리즘

- RSA 공개키 암호 알고리즘
  - RSA 알고리즘의 동작
    - 위 조건을 만족하면
      - $C = M^e \bmod n$
      - $M = M^{ed} \bmod n$ 이 성립
    - 암호화, 복호화
      1. 암호화: PU{e, n} 에 대하여 암호문 C는 $M^e \bmod n$
      2. 복호화: PR{d, n} 에 대하여 평문 M은 $C^d \bmod n$
      - 모든 송신자는 수신자의 공개키로 암호화 하여 전송하면 수신자의 개인키로 복호화 하여 평문을 얻을 수 있음 (기밀성)

공개키 암호 알고리즘

- RSA 공개키 암호 알고리즘
  - RSA 알고리즘의 보안
    - 전수공격
      - 공격자는 공개키, 암호문을 얻을 수 있고 가능한 모든 개인키 를 시도할 수 있음
      - n, e, d 의 크기가 충분히 크면 막을 수 있음
      - n, e, d 의 크기가 너무 크면 알고리즘이 늦어짐
    - 인수분해
      - n이 두 개의 소인수의 곱
      - 두 소인수를 찾게 된다면 해독 가능

공개키 암호 알고리즘

- Diffie-Hellman 키 교환 (Key Exchange)
  - 두 사용자가 비밀 키를 안전하게 교환해서 메시지를 암호화
  - Diffie-Hellman 알고리즘의 보안은 이산 대수 문제(Discrete Logarithms Problem)를 풀기가 어려움에 근거를 둠

공개키 암호 알고리즘

- Diffie-Hellman 키 교환 (Key Exchange)
  - 알고리즘 용어
    - 원시근 (Primitive Root)

      소수 p의 원시근: 자기 자신의 거듭제곱을 이용하여 1부터 p-1까지의 정수를 모두 생성해 낼 수 있는 어떤 수(a)

      a mod p, a^2 mod p, …, a^{p-1} mod p 인 수

      집합적으로 1부터 p-1까지의 수와 같음 (치환 됨)

    - 이산 대수 (Discrete Logarithm)

      P 보다 작은 임의의 정수 b와 p의 원시근 a 에 대하여

      $$b = a^i \ mod \ p\,, \qquad 0 \le i \le p-1$$

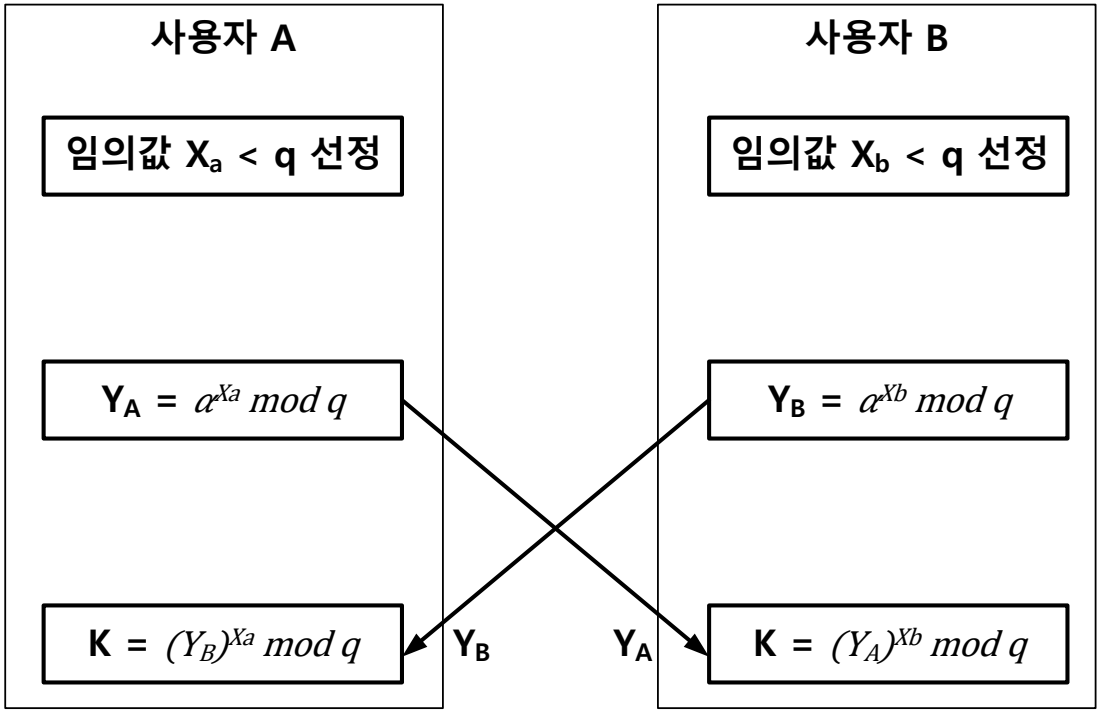
      지수(Exponent) i를 밑수 a를 갖는 b의 이산대수 혹은 지수(Index)라고함

      - 표기: $dlog_{a,\,p}(b)$

공개키 암호 알고리즘

- Diffie-Hellman 키 교환 (Key Exchange)
  - 알고리즘 동작
    - 소수 q와 q에 대한 원시근 정수α 가 공개됨

$$
\begin{aligned}
K &= {Y_B}^{X_A} \bmod q \\
&= (\alpha^{X_B} \bmod q)^{X_A} \bmod q \\
&= (\alpha^{X_B})^{X_A} \bmod q \\
&= \alpha^{X_B X_A} \bmod q \\
&= (\alpha^{X_A})^{X_B} \bmod q \\
&= (\alpha^{X_A} \bmod q)^{X_B} \bmod q \\
&= {Y_A}^{X_B} \bmod q
\end{aligned}
$$



Diffie-Hellman키 교환 프로토콜

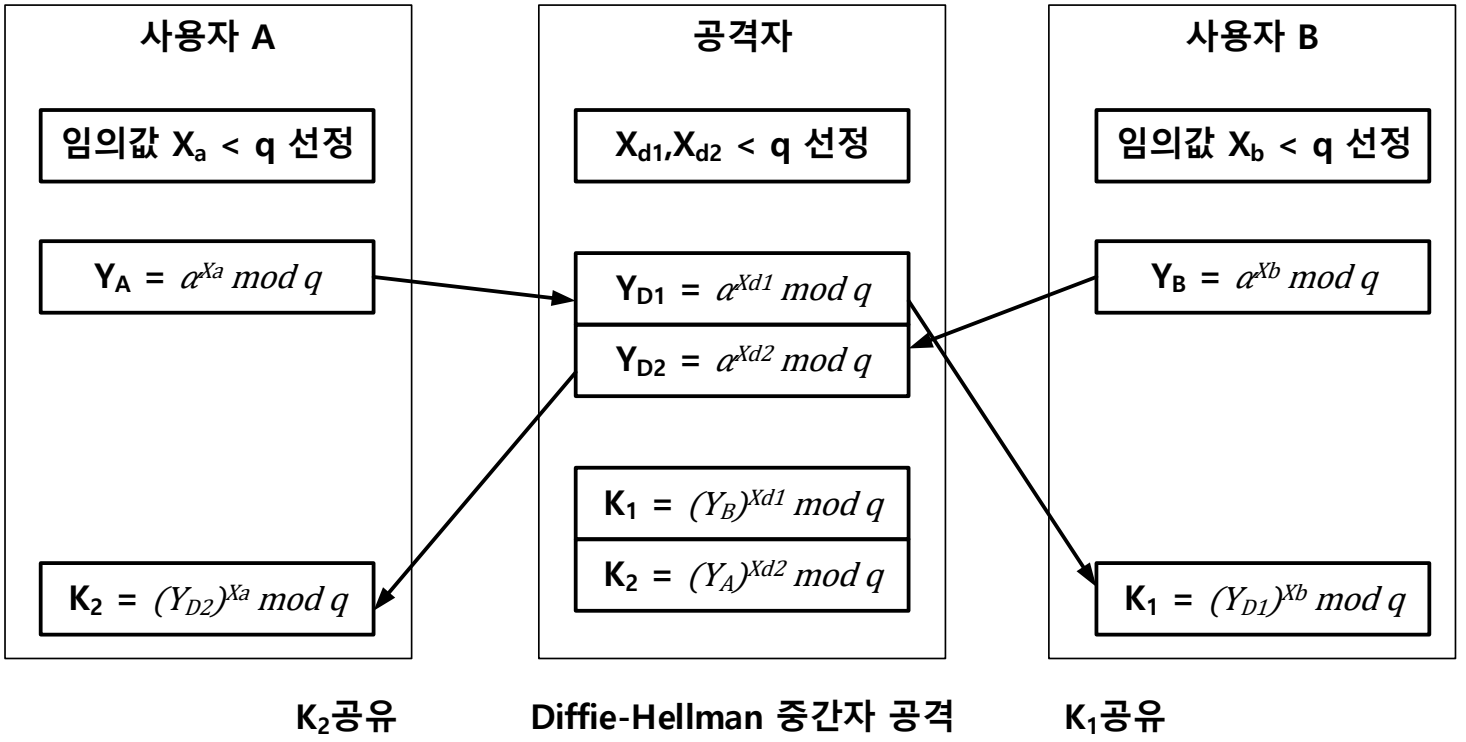
노출되는 값 : α, q, Y_A, Y_B

공개키 암호 알고리즘

- Diffie-Hellman 키 교환 (Key Exchange)
  - 알고리즘 공격
    - 공유하는 값을 저장할 중앙 디렉터리를 신뢰할 수 있다면 기밀성, 인증을 보장
      - 오직 A와 B만이 비밀 키를 계산할 수 있고 다른 사람은 메시지를 읽을 수 없음
      - 한 수신자는 오직 대응되는 송신자만 메시지암호화가 가능함을 알고 있음
    - 재전송 공격, 중간자 공격에 취약
      - 디지털서명 기법
      - 공개키 인증서 기법

공개키 암호 알고리즘

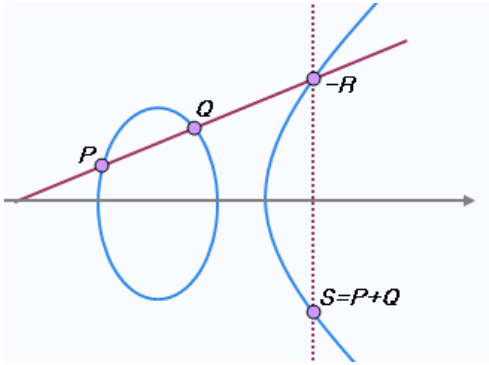
- Diffie-Hellman 키 교환 (Key Exchange)
  - 중간자 공격



- A와 Darth, B와 Darth가 통신이 연결 됨,
- A와 B는 사이에 Darth의 존재를 모르고 통신
- 무결성, 기밀성이 보장되지 않음

공개키 암호 알고리즘

- 타원 곡선 암호 (ECC: Elliptic Curve Cryptography)
  - RSA의 안전을 보장 하기위해 키의 길이가 매우 커지고, 이로 인해 RSA에 기초한 응용들의 연산이 많아짐
  - RSA보다 짧은 키 길이로 RSA와 비슷한 보안성이 목표
    - 현재 오버헤드가 적어 무선환경에서 사용중
  - 타원곡선을 설명하는 수학에 근거하여 만들어짐
    - 계산이 가능하지만 실제 계산이 오래 걸리는 이산대수 (Intractability)
    - $y^2 = x^3 + ax + b$



공개키 암호 알고리즘

- 디지털 서명 표준 (DSS: Digital Signature Standard)
  - NIST의 FIPS PUB186에 DSS표준을 발표
  - DSS는 SHA-1을 사용한 새로운 디지털 서명기법인 DSA(Digital Signature Algorithm)소개
  - DSS는 오직 디지털 서명 기능만 제공하도록 설계됨 (인증)
    - 암호, 키 교환 불가능 (Hashed)

디지털 서명

- 디지털 서명 (Digital Signature)
  - 수신자가 받은 메시지가 송신자로부터 온 것을 확신 하기 위한 인증의 기법
  - 기본적으로 암호화에서 암호문 복호화시 디지털 서명 역할을 함
  - 디지털 서명만 제공하는 기법으로 인증자(Authenticator)블록을 만듦
    - 인증자: 인증자를 변경하지 않으면서 문서를 변경 하는것이 불가능 해야함, 개인키를 이용하여 암호화 되었다면 출처, 내용, 순서까지 확인해주는 서명이 될 수 있음 (SHA-1, RSA)
  - 기밀성 보장이 없음

감사합니다 !