6장 : 공개키 암호시스템

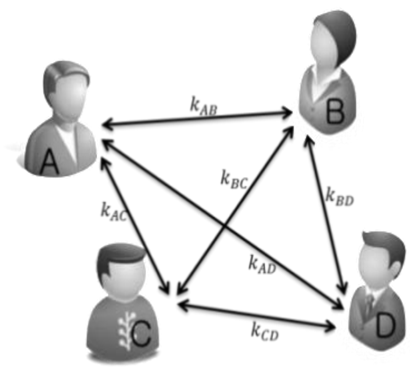
정보보호이론

Spring 2015

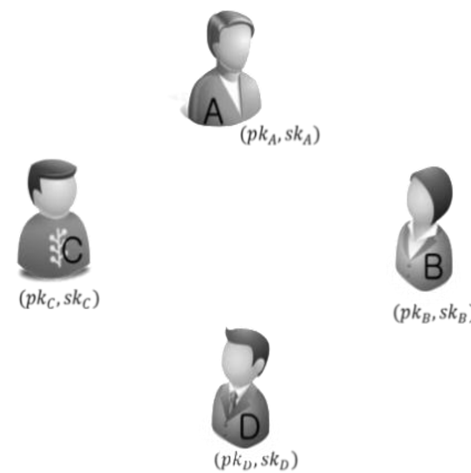
고려대학교
KOREA UNIVERSITY

6.1 공개키 암호 개요

- 대칭키 암호
  1. 안전한 채널을 통해서 사용자가 서로 동일한 키를 사전 공유
  2. n명이 서로 비밀통신을 하기 위해서는 $\frac{n(n-1)}{2}$개의 키가 필요
  3. 송신자나 수신자의 부인방지를 제공하지 못함.



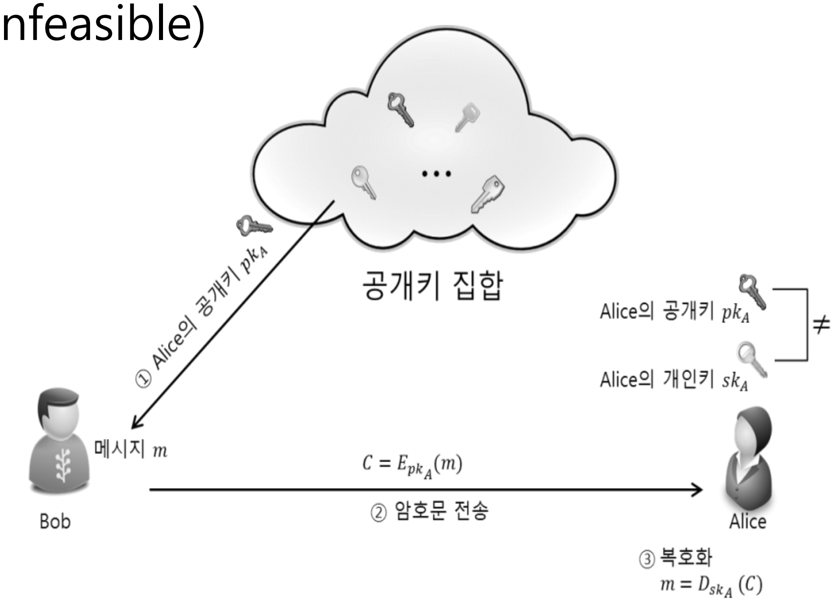
대칭키 암호시스템



공개키 암호시스템

6.1 공개키 암호 개요

- 공개키 (or 비대칭키(Asymmetric) 암호시스템)
  - Diffie와 Hellman은 1976년 발표된 논문 "New Directions in Cryptography"에서 공개키 암호시스템 소개
  - 각 사람마다 한 쌍의 키(공개키 pk, 개인키 sk)
    - 공개키는 모두에게 공개되고, 개인키는 비밀로 보관
    - 공개키 pk로부터 개인키 sk를 도출하는 것은 계산적으로 불가능 (Computationally Infeasible)



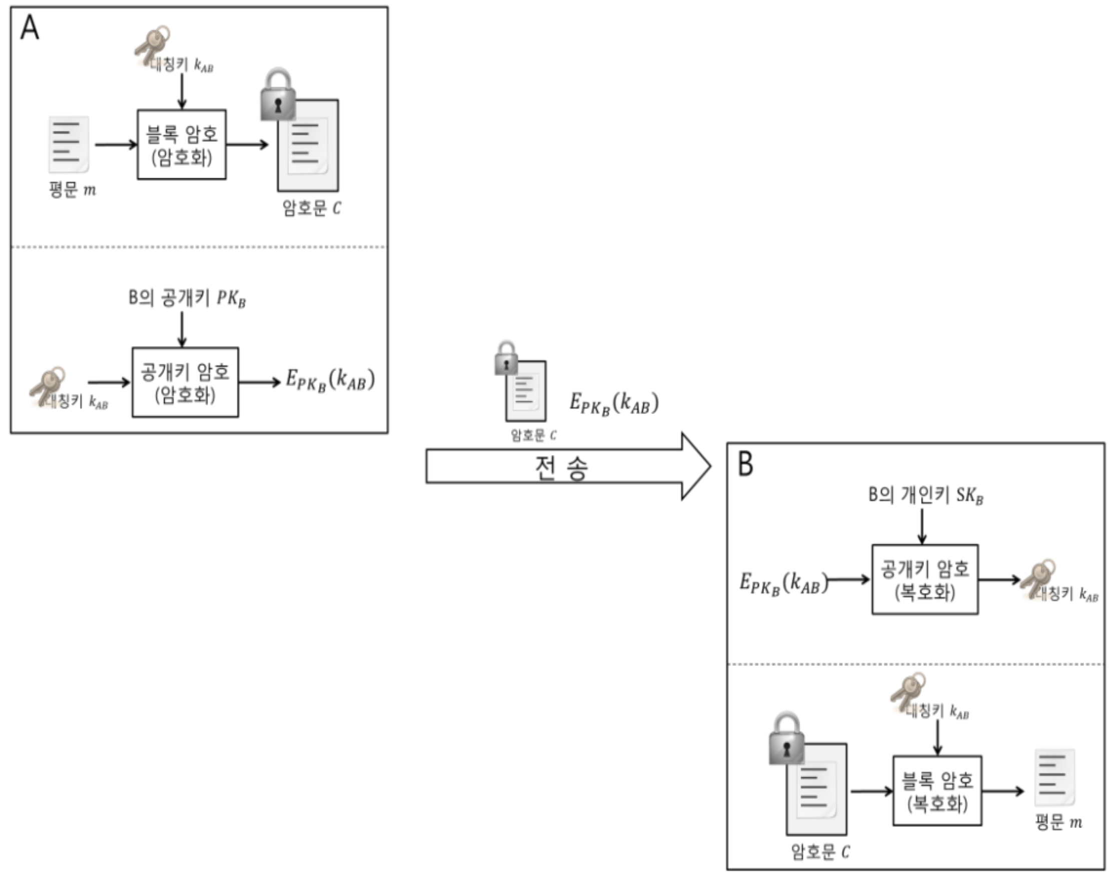
6.1 공개키 암호 개요

- 공개키 암호시스템과 대칭키 암호시스템의 차이점

	대칭키 암호시스템	공개키 암호시스템
비밀키 분배	필요	불필요
보유 비밀키 개수 (n명이 비밀통신 하는 경우)	$(n-1)$개 (상대방별로 키가 필요)	1개 (자신의 비밀키만 보유)
암호화 & 복호화 속도	빠름	느림
대표 예	DES, AES, SEED, ARIA	RSA, ElGamal

6.1 공개키 암호 개요

- 하이브리드 암호시스템
  - 대용량의 데이터를 암호화하기 위해서 대칭키 암호시스템에서 사용되는 비밀키 k를 공개키 암호시스템으로 암호화 ($\boldsymbol{E_{pk}}$(비밀키 $\boldsymbol{k}$)) 하여 분배하고, 수신자는 분배된 비밀키를 이용하여 대용량의 데이터를 대칭키 암호시스템으로 암호화



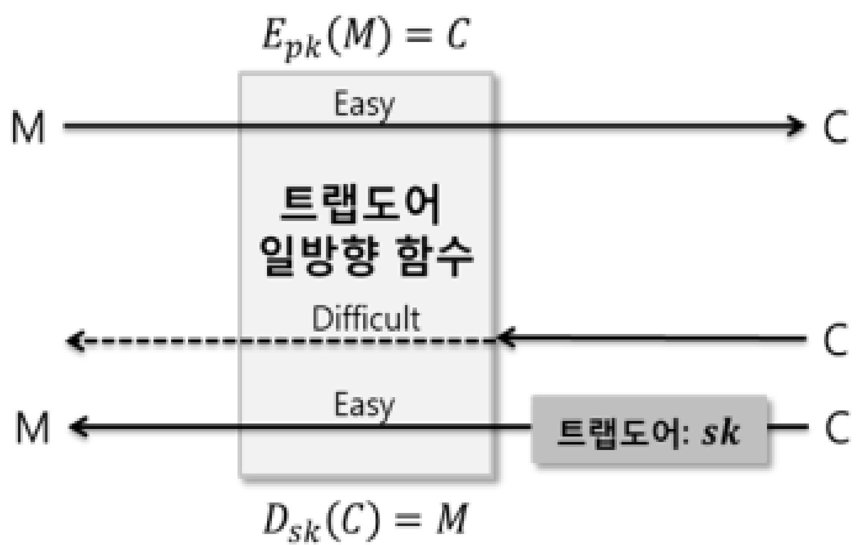
6.1 공개키 암호 개요-기본개념

- 일방향 함수 (One-Way Function) f
  1. f is easy to compute.
  2. f^{-1} is difficult to compute.

- 소인수분해 문제
  - When n is large, $n = p \times q$ is a one-way function.
  - Given p and q , it is always easy to calculate n ; given n, it is very difficult to compute p and q.
  - 최근까지 알려진 결과로는 2009년에 232자리의 십진수를 수 백대의 컴퓨터를 사용하여 2년만에 인수분해에 성공
    - 232자리 십진수는 이진수로 나타내면 768 비트가 필요하며 위의 결과는 768비트 RSA의 경우 동일한 계산능력으로 2년만에 평문이 복호화 될 수 있음을 의미

6.1 공개키 암호 개요-기본개념

- Trapdoor One-Way Function(TOWF)
  1. f is easy to compute.
  2. f^{-1} is difficult to compute.
  3. Given y and a trapdoor, x can be computed easily.
  - 공개키 설계의 기본 개념



6.2 수학적 배경 지식

- P-NP 문제
  - Undecidable
    - No algorithm that solves it
  - Decidable
    - If a problem can be solved in poly-time, it is tractable. Otherwise, it is intractable.
    - P : there exists a poly-time algorithm
    - NP : We don't know if there exists a poly-time algorithm and nobody insists that it cannot be solvable in poly-time.

6.2 수학적 배경 지식

- NP 문제
  1. 비결정적 단계(Nondeterministic Phase)
     - Guess
  2. 결정적 단계(Deterministic Phase)
     - 다항식 시간 검증

- 예) 소인수 분해 문제
  - 입력 : 합성수 n
    - 비결정적 단계 : p와 q를 Guess
    - 결정적 단계 : p x q =? N 을 다항식시간 안에 검증

6.2 수학적 배경 지식

- NP 예) 소인수분해 문제(Integer Factorization Problem, IFP)
  - $n = p_1^{r_1} \times p_2^{r_2} \times \cdots \times p_n^{r_n}$
- 인수분해 방법

1. Trivial Division
2. Fermat Method

   $n = x^2 - y^2 = a \times b$ with a = (x + y) and b = (x − y)

3. Pollard p – 1 Method
4. Pollard rho Method : particularly effective at splitting composite numbers with small factors.
5. More Efficient Methods : Quadratic Sieve, Number Field Sieve

NOTE : On a quantum computer, factorization is a tractable problem using Shor's algorithm.

6.2 수학적 배경 지식

- NP 예) 소인수분해 문제(Integer Factorization Problem, IFP)
  - $n = p_1^{r_1} \times p_2^{r_2} \times \cdots \times p_n^{r_n}$
- Trivial Division → 입력 $n\ (= p \times q)$을 $n^{1/2}$까지 나눈다.
  - $n = n^{1/2} \times n^{1/2}$. 따라서 $\min(p, q) \leq n^{1/2}$
  - 시간복잡도
    - 입력의 크기 x = $\log_2 n$ (즉 n의 이진수 비트 수)
    - $n = 2^x$, 따라서 $n^{1/2} = 2^{x/2}$ → 다항식시간이 아님!

NOTE : 시간 복잡도는 입력의 크기의 함수로 표현됨

- 입력의 크기 : 입력에 사용된 비트수

6.2 수학적 배경 지식

- 이산 대수 문제 (Discrete Logarithm Problem, DLP)
  - 유한 순환 군 $\mathbb{Z}_p^*$에 생성자 g와 어떤 원소 $y \in G$가 있을 때, $x = log_g\, y \bmod p$ 를 계산하는 문제
  - 실수 $\mathbb{R}$상에서 $log_g\, y$ 에 대한 계산은 효율적으로 계산. 하지만, $\mathbb{Z}_p^*$상에서는 로그 연산이 정의되어 있지 않기 때문에, x를 구하는 효율적인 계산이 존재하지 않음

$$\{g^0, g^1, \ldots g^{p-1}\} = Z_p^*$$

$$\xrightarrow{(p, g, y = g^x)}$$

$$x = ?$$

6.2 수학적 배경 지식

- 중국인의 나머지 정리(CRT)
  - 쌍마다 서로 소인 자연수 $n_1, n_2, \ldots, n_k$와 정수 $a_1, a_2, \ldots, a_k$에 대하여 $x \equiv a_i \pmod{n_i}$, $1 \le i \le k$, 를 만족하는 x는 법 $(n_1 \times n_2 \times \cdots \times n_k)$ 안에서 유일하게 존재

$$
\begin{aligned}
x &\equiv a_1 \pmod{m_1} \\
x &\equiv a_2 \pmod{m_2} \\
&\cdots \\
x &\equiv a_k \pmod{m_k}
\end{aligned}
$$

- Example : solve x ≡ 2 (mod 3), x ≡ 3 (mod 5), and x ≡ 2 (mod 7).
  - x = 23. 즉 23 ≡ 2 (mod 3), 23 ≡ 3 (mod 5), and 23 ≡ 2 (mod 7).

6.2 수학적 배경 지식

- CRT 해법(Gaussian Method)

1. Find $M = m_1 \times m_2 \times \ldots \times m_k$. This is the common modulus.
2. Find $M_1 = M/m_1$, $M_2 = M/m_2$, …, $M_k = M/m_k$.
3. Find the multiplicative inverse of M_1, M_2, …, M_k using the corresponding moduli (m_1, m_2, …, m_k). Call the inverses M_1^{-1}, M_2^{-1}, …, M_k^{-1}.
4. The solution to the simultaneous equations is

$$\boxed{x = (a_1 \times M_1 \times M_1^{-1} + a_2 \times M_2 \times M_2^{-1} + \cdots + a_k \times M_k \times M_k^{-1}) \bmod M}$$

6.2 수학적 배경 지식

- 이차합동(Quadratic Congruence)

$$x^2 \equiv a \pmod{n}$$

  - 해를 갖는다면 a를 이차 잉여 (Quadratic Residue, QR), 해를 갖지 않는다면 이차 비잉여(Quadratic Nonresidue, QNR)
    - 해를 갖는다면 서로 합동이 아닌 두 개의 해
  - 원소의 개수가 $p-1$개인 $\mathbb{Z}_p^*$에 대하여 이차 잉여와 이차 비잉여의 개수는 정확하게 $(p-1)/2$개로 동일
  - 예) $\mathbb{Z}_{13}^*$에서 $x^2 \equiv 4\ (mod\ 13)$과 $x^2 \equiv 7\ (mod\ 13)$의 해

a	1	2	3	4	5	6	7	8	9	10	11	12
a^2	1	4	9	3	1	10	10	12	3	9	4	10

    - $x^2 \equiv 4\ (mod\ 13)$를 만족하는 해는 **2, 11**
    - $x^2 \equiv 7\ (mod\ 13)$에 대한 **해는 존재하지 않음**
    - $\mathrm{QR} = \{1,3,4,9,10,12\}$이고 $\mathrm{QNR} = \{2,5,6,7,8,11\}$

6.2 수학적 배경 지식

- 오일러 판정법(Euler's Criterion)
  - 소수 p에 대해여 $\mathbb{Z}_p^*$의 원소 a 가 QR에 속하는지 QNR에 속하는지에 대한 판정 기준

$$a^{(p-1)/2} \equiv 1 \quad \Longrightarrow \quad a \in \mathrm{QR}$$
$$a^{(p-1)/2} \equiv -1 \quad \Longrightarrow \quad a \in \mathrm{QNR}$$

6.2 수학적 배경 지식

이차 합동 방정식의 해

- $n = 4k + 3 \ \ (k \in \mathbb{Z}^{+})$인 경우
  - $x \equiv a^{\frac{n+1}{4}} \pmod{n}$, $x \equiv -a^{\frac{n+1}{4}} \pmod{n}$

- n이 합성수인 경우

$$\boxed{x^2 \equiv a \pmod{n}} \rightarrow \boxed{n = p_1 \times p_2 \times \cdots \times p_k} \rightarrow \boxed{\begin{array}{c} x^2 \equiv a_1 \pmod{p_1} \\ x^2 \equiv a_2 \pmod{p_2} \\ \cdots \\ x^2 \equiv a_3 \pmod{p_k} \end{array}}$$

$$\rightarrow \boxed{\begin{array}{c} x_1 \equiv \pm b_1 \pmod{p_1} \\ x_2 \equiv \pm b_2 \pmod{p_2} \\ \cdots \\ x_k \equiv \pm b_k \pmod{p_k} \end{array}} \rightarrow \boxed{\text{CRT를 이용하여 해 구하기}}$$

6.2 수학적 배경 지식

- 예)다음 이차 합동 방정식의 해를 구하시오
  - $x^2 \equiv 53\ (mod\ 77)$
  - 풀이
    1. $77 = 7 \times 11$로 소인수분해 되며, 7과 11은 모두 $4k + 3$의 형태
    2. $\mathrm{x}^2 \equiv 4\ (\mathrm{mod}\ 7) \quad \Rightarrow \quad \mathrm{x} \equiv 4^{\frac{7+1}{4}} \equiv \pm 2\ (\mathrm{mod}\ 7)$
    3. $\mathrm{x}^2 \equiv 9\ (\mathrm{mod}\ 11) \quad \Rightarrow \quad \mathrm{x} \equiv 9^{\frac{11+1}{4}} \equiv \pm 3\ (\mathrm{mod}\ 11)$
    4. 4가지 경우로 CRT를 적용
       1. $x \equiv 2\ (mod\ 7),\quad x \equiv 3\ (mod\ 11)$
       2. $x \equiv 2\ (mod\ 7),\quad x \equiv -3\ (mod\ 11)$
       3. $x \equiv -2\ (mod\ 7),\quad x \equiv 3\ (mod\ 11)$
       4. $x \equiv -2\ (mod\ 7),\quad x \equiv -3\ (mod\ 11)$
  - 해: $\mathrm{x} \equiv \pm 58\ (\mathrm{mod}\ 77),\ \mathrm{x} \equiv \pm 30\ (\mathrm{mod}\ 77)$

6.2 수학적 배경 지식

- 제곱-곱 연산 방법(Square-and-Multiply Method)
  - 공개키 암호시스템에서는 지수승 연산이 수행 → 효율적 방법이 요구됨
    - $y = a^{13} = a^{1101}$
      1. $a^{10} = (a^1)^2$, $a^{11} = (a^1)^2 \times a$
      2. $a^{110} = (a^{11})^2$
      3. $a^{1100} = (a^{110})^2$, $a^{1101} = (a^{110})^2 \times a$

6.2 수학적 배경 지식

- 제곱-곱 연산 방법(Square-and-Multiply Method)

square_and_multiply (a, x, n) {

$r = a;$

for(i = t − 1 downto 0), t : x의 비트 수

{

$r \equiv r^2 \pmod{n}$

If$(b_i = 1)$ $r \equiv r \times a \pmod{n}$; b_i: x의 i번째 비트;

}

return $(\boldsymbol{r})$

}

6.2 수학적 배경 지식

- 페르마 소정리(Fermat’s Little Theorem)
  - p: prime, $\forall a \in \mathbb{Z}_p^*$, $\Rightarrow$ $a^{p-1} \equiv 1 \pmod p$
  - p: prime, $\forall a \in \mathbb{Z}_p^*$, $\Rightarrow$ $a^p \equiv a \pmod p$
  - 예) $7^{111} \bmod 11$
    1. $7^{10} \equiv 1\ (mod\ 11)$, $7^{11} \equiv 7\ (mod\ 11)$
    2. $111 = 11 \times 10 + 1$
    3. $7^{111} \equiv (7^{11})^{10} \times 7^1 \equiv (7)^{10} \times 7^1 \equiv 1 \times 7 \quad (mod\ 11)$

6.2 수학적 배경 지식

- 오일러 함수(Euler's Phi Function)
  - 오일러 함수 $\varphi(\cdot)$는 1부터 n까지 n과 서로소인 정수의 개수

$$\varphi(n) = |\{a \in \mathbb{N} |\, \gcd(a, n) = 1\}|$$

  - p가 소수일 때, $\varphi(p) = p - 1$
  - 서로소인 정수 m, n에 대하여, $\varphi(m \times n) = \varphi(m) \quad \times \varphi(n)$
- 예)) $\varphi(10)$
  - $gcd(1,10) = 1,\ gcd(2,10) = 2,\ gcd(3,10) = 1$
  - $\gcd(4,10) = 2,\ \gcd(5,10) = 5,\ \gcd(6,10) = 2$
  - $\gcd(7,10) = 1,\ \gcd(8,10) = 2,\ \gcd(9,10) = 1$
  - $\boldsymbol{\varphi(10) = 4}$

6.2 수학적 배경 지식

- 오일러 정리 (Euler's Theorem)
  - $n \in \mathbb{Z}, \quad \forall a \in Z_n^* \quad \Rightarrow \quad a^{\varphi(n)} \equiv 1 \ (\mathrm{mod}\ n)$
  - $n \in \mathbb{Z}, \quad \forall a \in \mathbb{Z}_n^*, \quad \Rightarrow \quad a^{\varphi(n)+1} \equiv a \ (\mathrm{mod}\ n)$
  - 예) 3^{-1} mod 14
    - $\varphi(14) = 6 \rightarrow 3^6 \equiv 1 \ (mod\ 14)$
    - $3 \times 3^5 \equiv 1 \ (mod\ 14)$: 곱셈상의 역원에 대한 정의와 동일
    - $3^{-1} \equiv 3^5 \ (\mathrm{mod}\ 14)$
    - $3^{-1} \equiv 3^5 \equiv 243 \ \equiv 5 \ (\mathrm{mod}\ 14)$

6.2 수학적 배경 지식

- 소수의 개수
  - 가장 큰 소수 : 6,320,430자리의 소수 (MSU)
  - 소수의 개수는 무한
  - n보다 작은 소수의 개수 : $f(n)$

$$[\frac{n}{ln\, n}] < f(n) < [\frac{n}{ln\, n - 1.08366}]$$

    - n의 값이 커질수록, 그 수가 소수일 확률도 $\frac{1}{\ln n}$의 분포를 따라서 작아짐
  - 1,000,000보다 적은 소수의 개수는?
    - 72,383 < f(1,000,000) <78,543.
    - 실제 78,498개의 소수

  - 선택된 수 k 가 소수일 확률

$$P(k \text{ is prime}) \approx \frac{1}{ln(k)}$$

6.2 수학적 배경 지식

- 소수 판정(Primality Test)
  - n 이 소수인가?
  - 결정적 방법
    - 에라토스테네스의 체(Sieve of Eratosthenes)
      - → $n^{1/2}$보다 작은 모든 소수로 나눈다.
      - – 비효율적

6.2 수학적 배경 지식

- 소수 판정(Primality Test)
  - n 이 소수인가?
  - 비결정적 방법
    - Fermat 소수 판정, Miller-Rabin 소수 판정
    - "composite" → 항상 true; "prime" → true일 확률이 높음
    - n번 알고리즘을 수행하여 모두 소수라고 판정한 경우 $1-(1-k)^n$의 확률로 "true"