암호프로토콜

이 병 천

2011. 11. 22

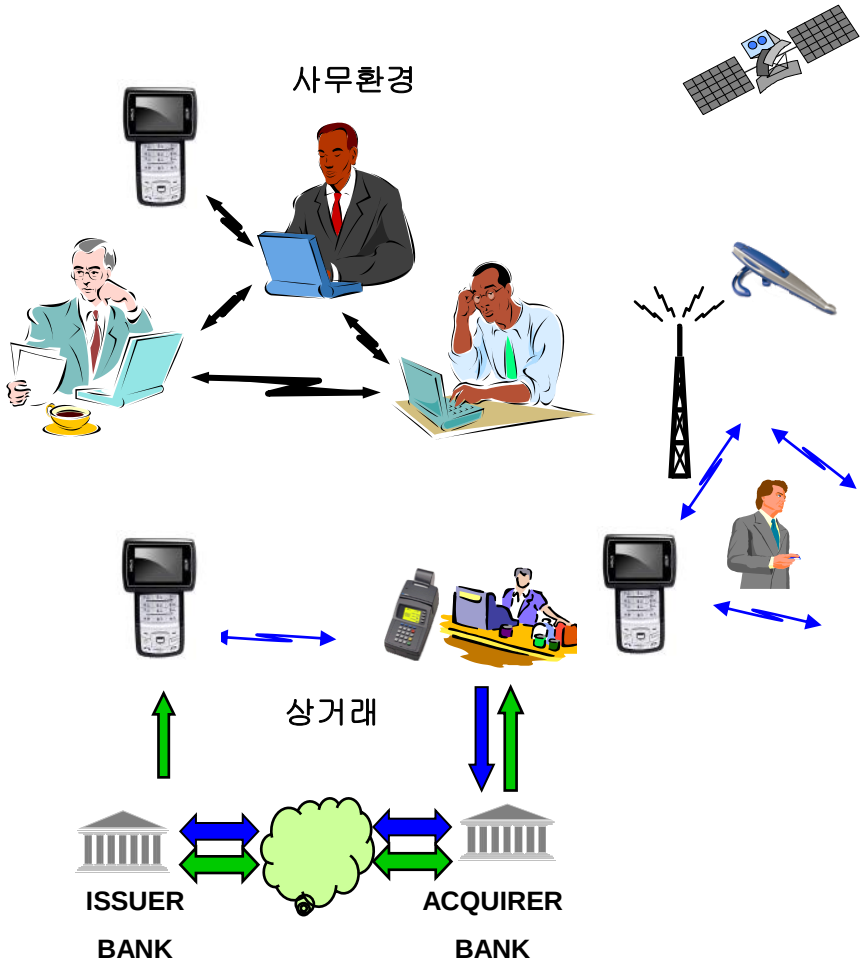
중부대학교 정보보호학과

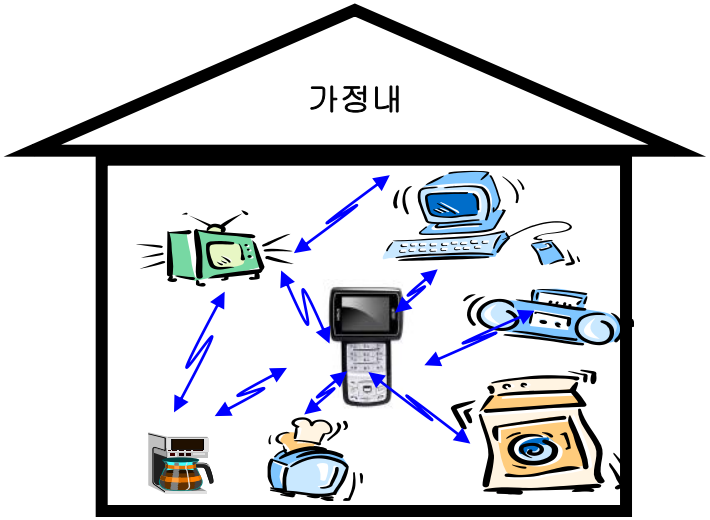
목차

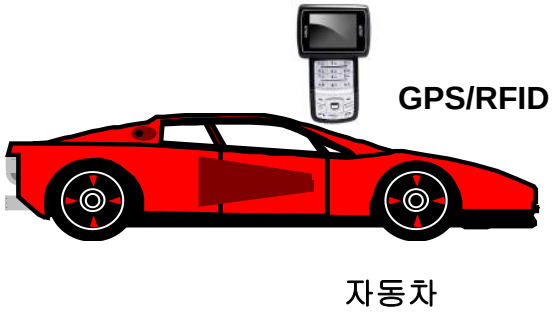
1. 암호프로토콜이란?
2. 사례
  2.1 동전던지기 게임
  2.2 키합의
  2.3 은닉서명
  2.4 비밀분산
  2.5 영지식증명
3. 암호프로토콜의 응용

1. 암호 프로토콜

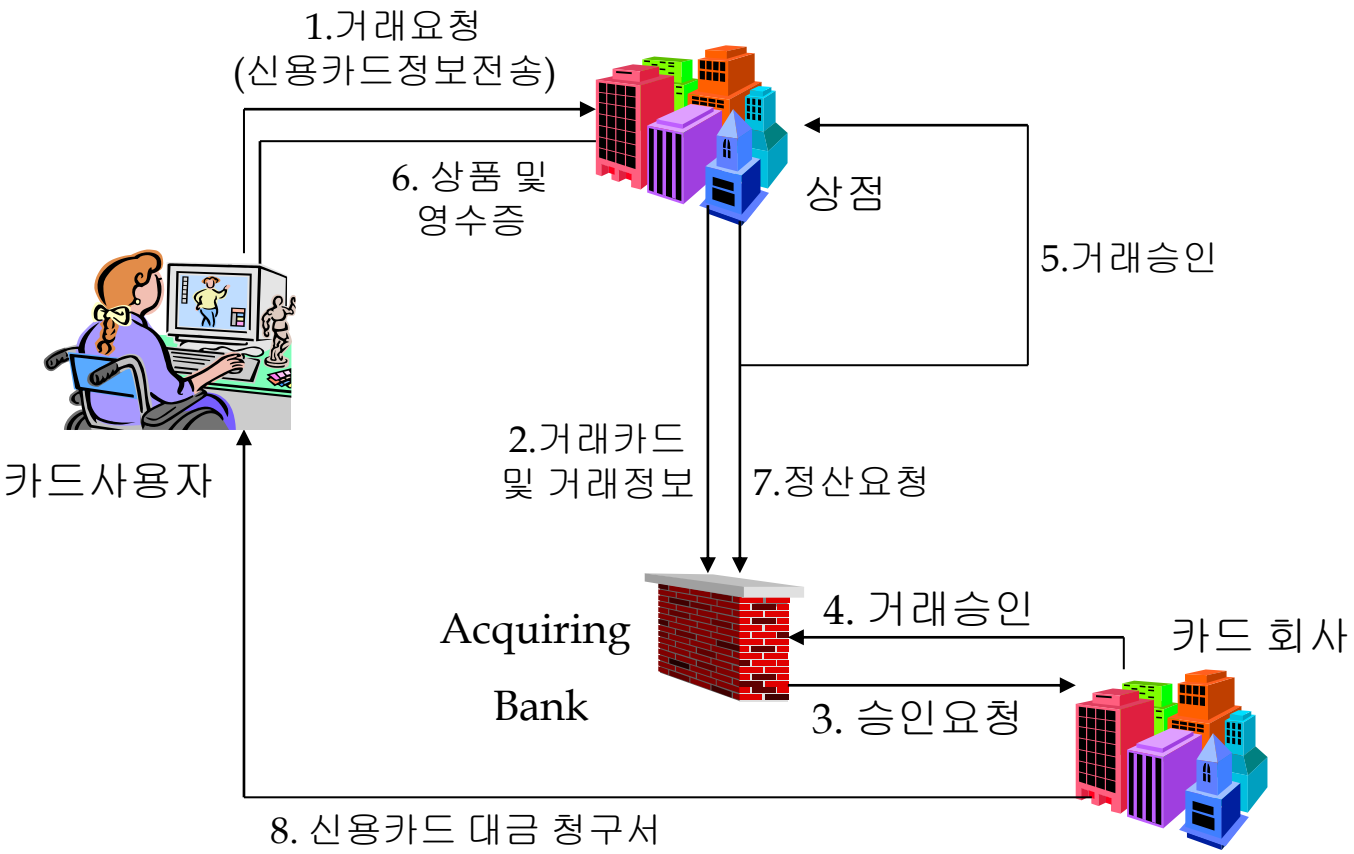
통신 환경의 발전, 유비쿼터스 환경







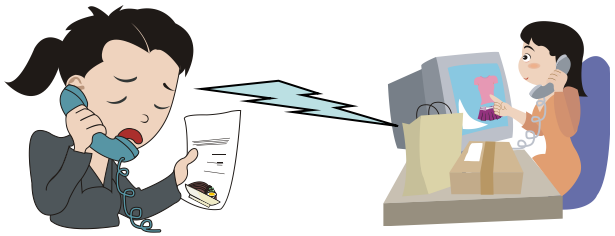
상거래 시나리오


1.거래요청
(신용카드정보전송)
6. 상품 및
영수증
상점
5.거래승인
카드사용자
2.거래카드
및 거래정보
7.정산요청
Acquiring
Bank
4. 거래승인
카드 회사
3. 승인요청
8. 신용카드 대금 청구서

대면 vs. 비대면

- 비대면 활동의 증가
  - 대면 활동의 감소, 비대면 활동의 증가
  - 업무의 효율성, 경쟁력 강화

대면 활동



비대면 활동

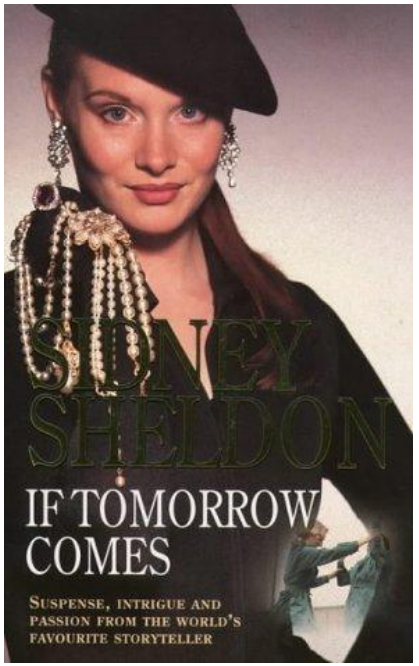
대면 vs. 비대면

On the Internet, Nobody knows you're a dog

"On the Internet, nobody knows you're a dog."

통신 상대방을 믿을 수 있나?

- 시드니 셸던**(Sidney Sheldon), "내일이 오면 (If Tomorrow Comes)"**
  - 사기꾼들의 이야기
  - 다면기 체스 게임
  - 중간자 공격 (man-in-the -middle attack)

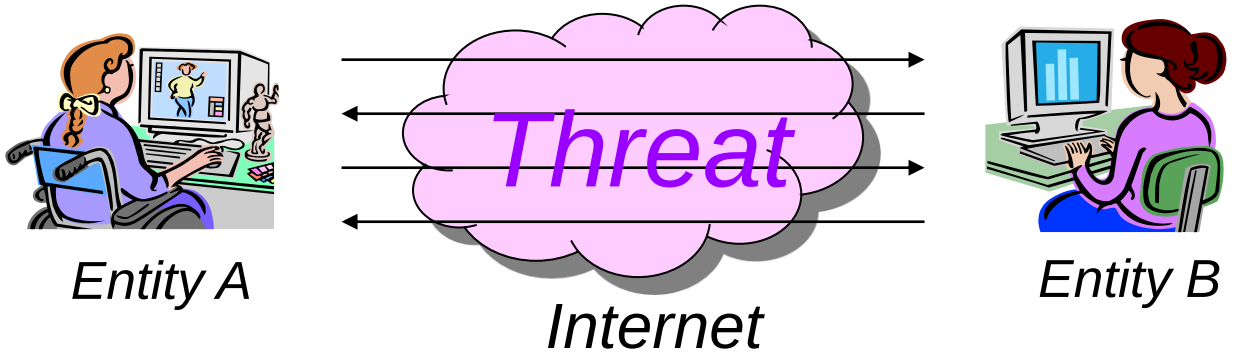


공정하게 빵 나누기

❖ 공평하게 빵을 나누려면?

암호 프로토콜이란?

- **프로토콜**
  - 다자간에 특정 작업을 수행하기 위해 정해진 계산 및 통신 절차
  - 외교에서 사용되는 의전 절차
- **암호 프로토콜**
  - 암호기술을 사용하는 프로토콜
  - 공개된 네트워크 환경에서 비대면 상황에서 신뢰할 수 없는 상대들과 공정한 작업을 수행하기 위한 기술



암호알고리즘과 암호프로토콜

- 암호 알고리즘
  - 한 개체에 의해 수행되는 알고리즘
  - 암호 기능을 수행하는 알고리즘
  - 사례: 암호화, 해쉬, 전자서명 등
- 암호 프로토콜
  - 복수의 개체들간에 특정 암호 기능을 수행하기 위해 정해진 절차에 따라 수행되는 통신 프로토콜
  - 신뢰할 수 없는 개체들간에 공정성을 담보하기 위한 기술
  - 사례: 인증, 키합의, 비밀분산, 은닉서명, 게임 등
  - 다자간의 복잡한 기능을 수행하기 위한 핵심 암호기술 : 전자상거래, 전자투표, 전자경매 등

보안 이슈

- 온라인 거래에서 생기는 의문
  - 내가 거래하고 있는 상대는 누구인가?
  - 이것은 공정한 거래인가?
  - 상대가 나를 속인다면?
  - 올바른 절차를 잘 따르고 있는 것 맞나?
  - 추후 문제가 발생했을 때 문제를 해결할 수 있는가?
  - 다른 사람이 우리의 거래를 보고 있다면?

암호프로토콜의 필요성

- 비대면 통신상의 거래에서 상대방을 신뢰하기 어려움 , 상대방의 신분을 확인할 수 있는 수단이 필요
- 공정성의 보장이 필요. 불공정한 게임은 인터넷으로 이루어질 수 없음
- 약속된 절차를 따르고 있음을 확인할 수 있어야 함. 증거 확보 가능
- 어느 순간 프로토콜이 정지되더라도 양측에 공정해야 함
- 거래 당사자간의 프라이버시 보호

암호프로토콜의 요구사항

- **공정성:**
  - 비대면 프로토콜에 참여하는 참여자들 사이에 어느 한쪽이 유리하거나 불리하지 않도록 공정성을 보장해야 한다. 어느 한쪽이 불리하다는 것이 알려지면 이런 비대면 프로토콜을 사용하려고 하지 않을 것이다.
- **인증성:**
  - 비대면 프로토콜에서 상대방의 신분이 맞는지 주고받는 메시지가 위조되지는 않는지 확인할 수 있어야 한다. 상대방에 대한 신뢰는 프로토콜을 수행할 수 있는 가장 기본적인 전제가 된다.
- **정확성과 검증성:**
  - 통신 프로토콜을 통해 약속된 절차가 맞게 이루어지고 있는지 정확성을 검증해 볼 수 있어야 한다.
- **프라이버시:**
  - 프로토콜 수행에 관한 정보가 제삼자에게 불필요하게 노출되지 않아야 한다. 이를 위해 암호화가 사용될 수 있다.

2. 암호프로토콜 사례

2.1 동전던지기 게임

2.2 키합의

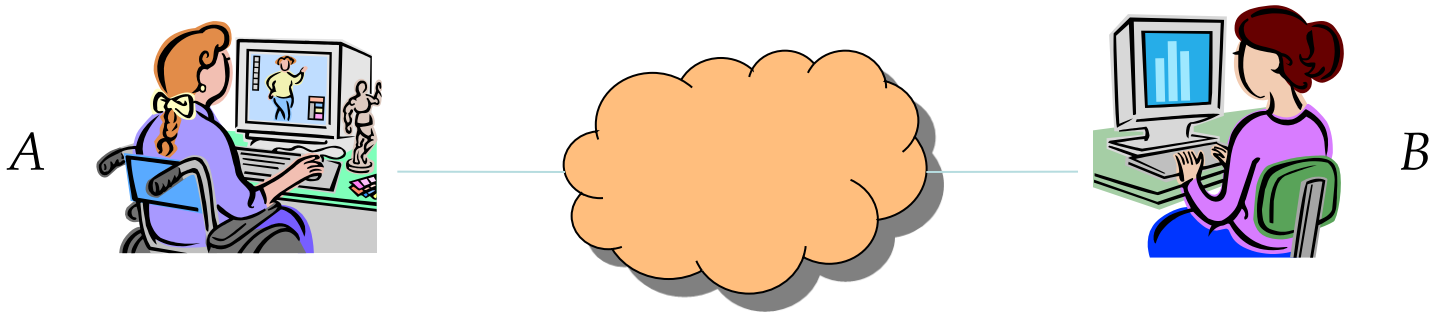
2.3 은닉서명

2.4 비밀분산과 문턱암호

2.5 영지식 증명

2.1 인터넷으로 동전던지기 게임을?

- 인터넷상의 두 사람은 동전던지기 게임을 할 수 있을까?



앞면, Alice

뒷면, Bob

인터넷으로 동전던지기 게임

- **블랙박스가 존재한다면? (한번 집어넣으면 마음대로 열어볼 수 없고 내용을 바꿀 수도 없으며, 나중에 열어볼 수 있음)**

1. A는 임의의 숫자를 종이에 써서 블랙박스에 넣는다. 이 박스를 열 수 있는 키는 A만이 가지고 있다. 그리고 이 박스를 B에게 전송한다.
2. B는 이 박스에 들어있는 숫자가 홀수인지, 짝수인지 추측하여 A에게 말한다.
3. A는 블랙박스를 열 수 있는 키를 B에게 제공한다.
4. B는 블랙박스를 열어서 숫자를 확인한다. 홀수/짝수를 B가 맞추었으면 B가 이기는 것이고 아니면 A가 이기는 것이다.

인터넷으로 동전던지기 게임

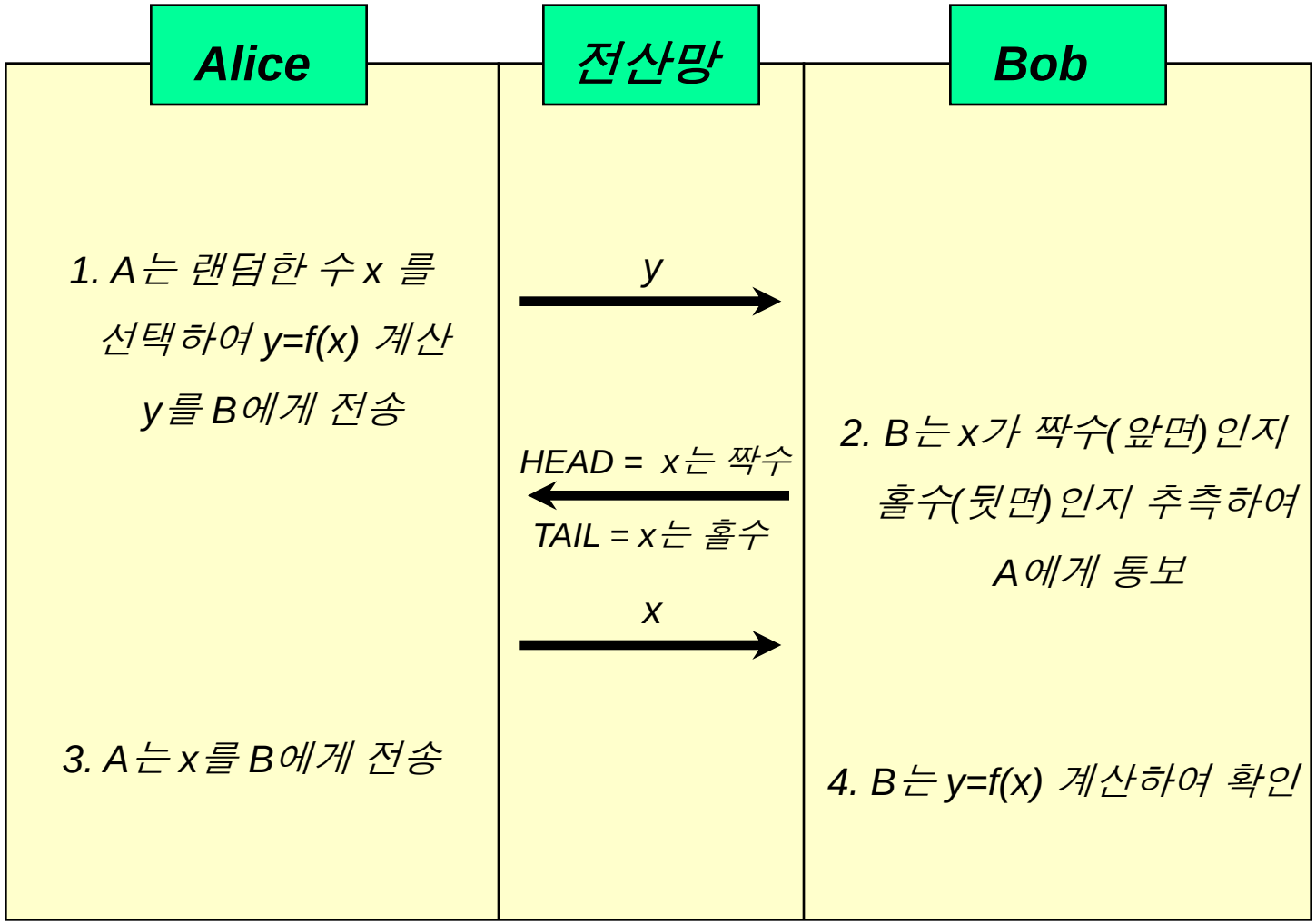
- 해쉬함수를 이용한 동전던지기

1. A는 임의의 정수 x를 선택하여 이것의 해쉬값 H(x)를 계산하고 이 값을 B에게 전송한다.
2. B는 정수 x가 홀수인지, 짝수인지 추측하여 A에게 말한다.
3. A는 원래의 정수 x를 B에게 전송한다.
4. B는 H(x)를 계산하여 앞에서 받은 값과 같은지 확인한다. 홀수/짝수를 B가 맞추었으면 B가 이기는 것이고 아니면 A가 이기는 것이다.

앞면, Alice

뒷면, Bob

인터넷을 통한 동전던지기 게임



2.2 키합의

- 키합의: 만나지 않고도 비밀키를 공유할 수 있다
  - 네트워크 상의 두 개체 A와 B가 암호알고리즘에 사용할 비밀키를 공유하는 방법
  - 만나지 않고 공유하는 방법
  - Diffie-Hellman 프로토콜 이용

키합의

❖ **Diffie-Hellman의 키합의**

A 

 B

난수 x_A선택 $\xrightarrow{\quad y_A \quad}$ 난수 x_B선택

$y_A = g^{x_A} \bmod p$ $\xleftarrow{\quad y_B \quad}$ $y_B = g^{x_B} \bmod p$

$$K = y_B^{\ x_A} = (g^{x_B})^{x_A} \bmod p$$

$$K = y_A^{\ x_B} = (g^{x_A})^{x_B} \bmod p$$

키합의 (사례)

❖ **Diffie-Hellman의 키합의**

Entity A

$g = 5$

$p = 23$

Entity B

난수 $x_A = 7$선택

$y_A = 5^7 \bmod 23 = 17$

$y_A = 17$ →

← $y_B = 11$

난수 $x_B = 9$선택

$y_B = 5^9 \bmod 23 = 11$

$$K = y_B{}^{x_A} = (11)^7 \bmod 23 = 7$$

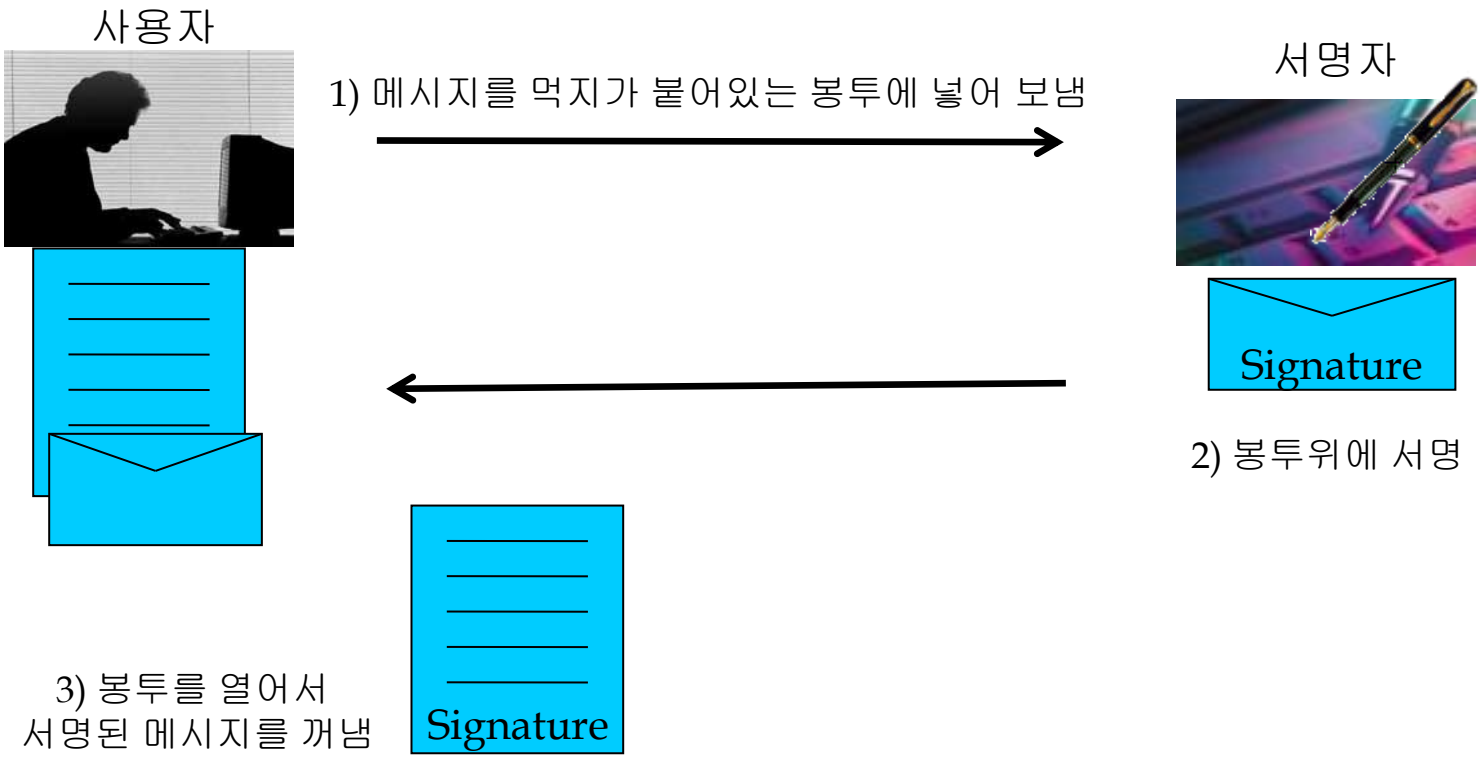
$$K = y_A{}^{x_B} = (17)^9 \bmod 23 = 7$$

2.3 은닉서명 (Blind Signature)

- 은닉서명
  - 사용자 A가 서명자 B에게 자신의 메시지를 보여주지 않고 서명을 얻는 방법
  - 메시지의 비밀성을 지키면서 타인의 인증을 받고자 하는 경우 사용
  - David Chaum 이 제안
- 은닉서명 응용
  - 고객은 은행에서 전자화폐를 인출
  - 투표자는 투표용지를 발급받음

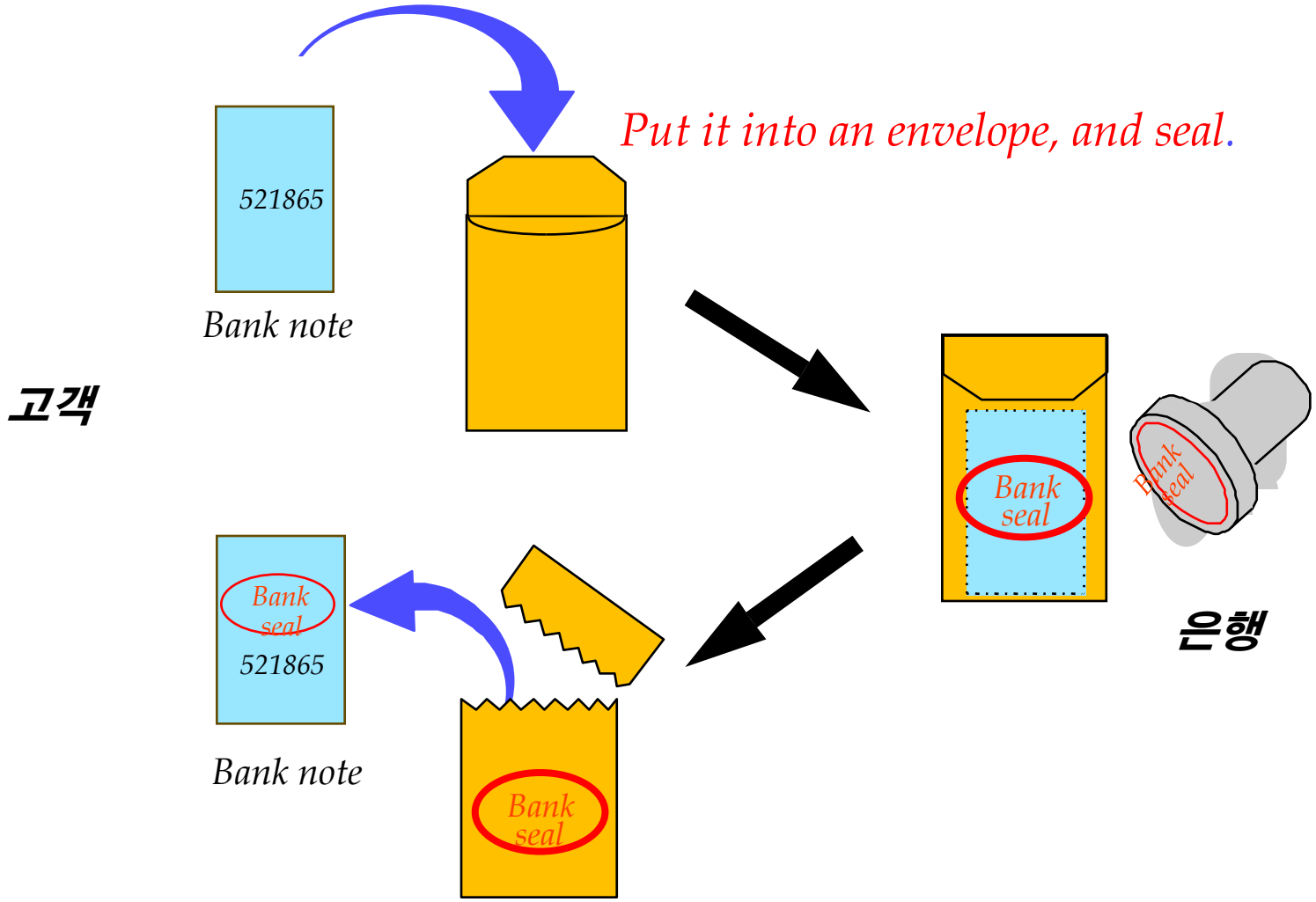
은닉서명

❖ 비유


사용자
서명자
1) 메시지를 먹지가 붙어있는 봉투에 넣어 보냄
Signature
2) 봉투위에 서명
3) 봉투를 열어서
서명된 메시지를 꺼냄
Signature

은닉서명 (Blind Signature)

❖ 전자화폐 발행에 이용



RSA 방식의 은닉서명

❖ **RSA 방식 은닉서명**

사용자 A

서명자 B

난수 r 선택

$K_1 = r^e M \bmod n$

K_1 →

← K_2

$K_2 = K_1^{\,d} \bmod n$

$= r \cdot M^d \bmod n$

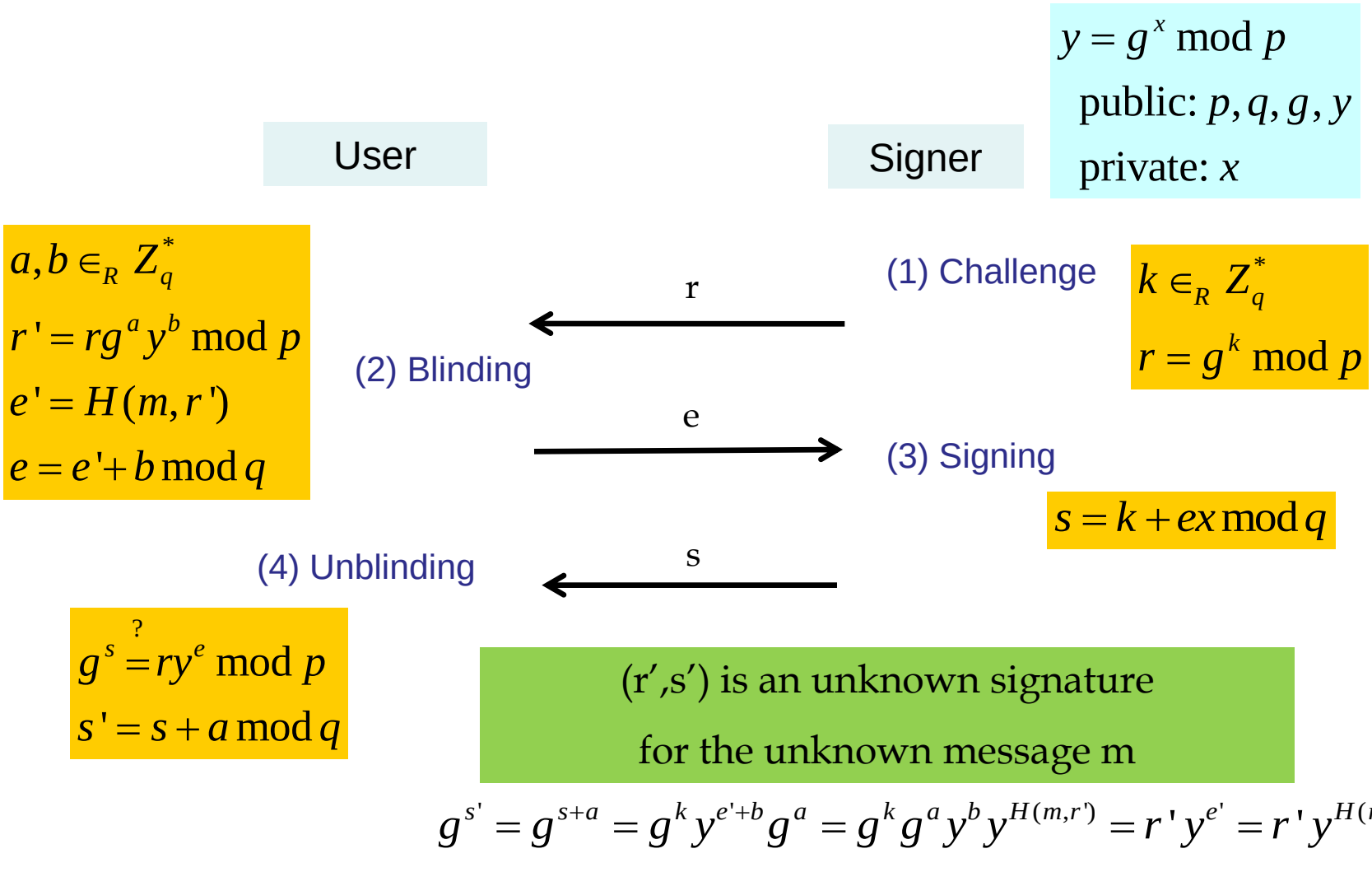
$$s = K_2 / r \bmod n = M^d \bmod n$$

RSA 방식의 은닉서명 (사례)

❖ 은닉서명 구성 예

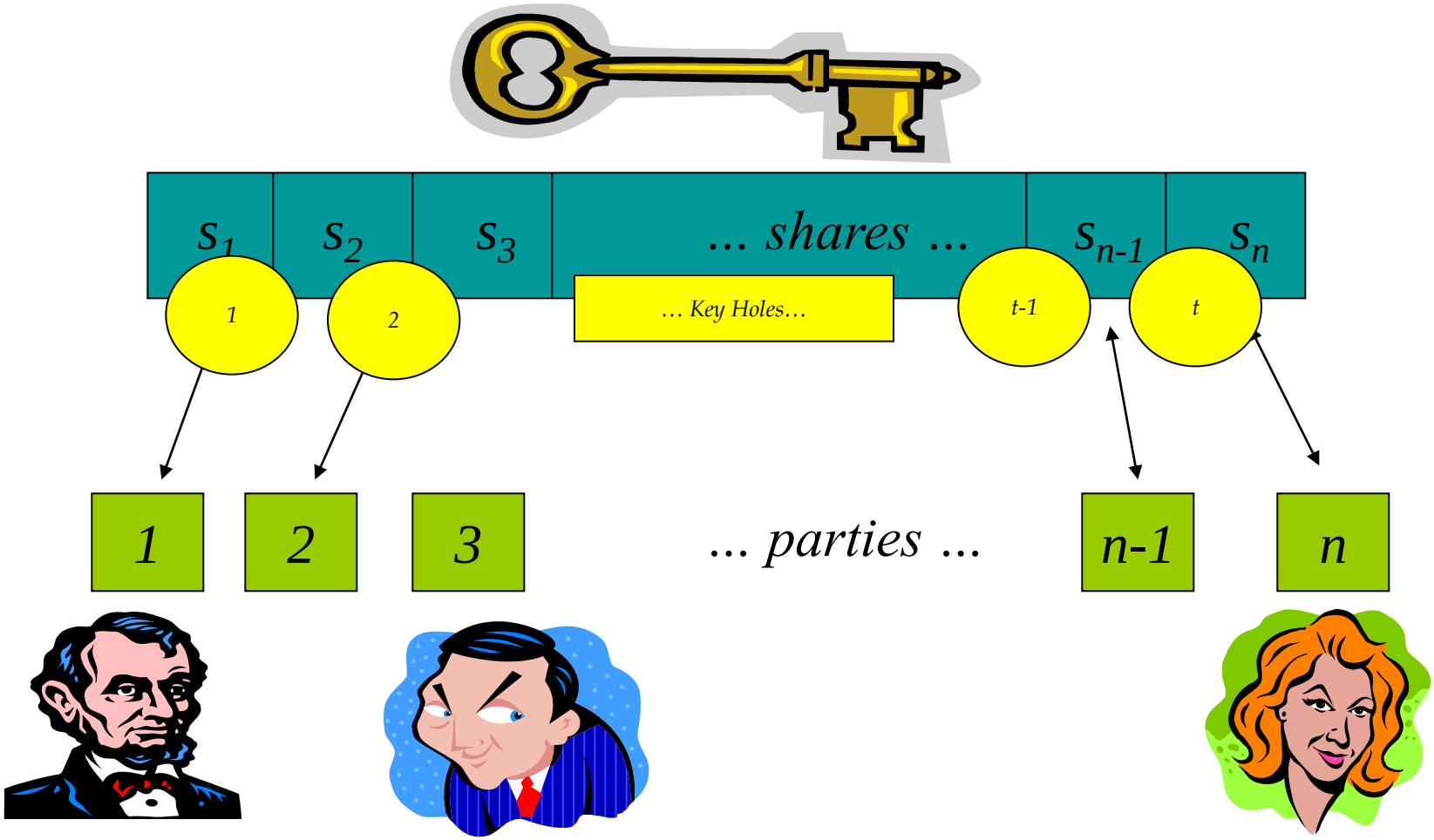
제공자 A	공개 정보 $n=55,\ e=7$	서명자 B
$r \in_R Z_n$ $r = 6$ $K_1 \equiv r^e M \mod n$ $\equiv 6^7 \times 5 \equiv 40 \mod 55$	$K_1 = 40$ →	$n = p \times q$ $= 11 \times 5 = 55$ $\phi(n) = \phi(55) = 40$ $\gcd(e, \phi(55)) = 1$ $e \times d \equiv 1 \mod \phi(n)$ $d = 23$ $K_2 \equiv K_1^d \mod n$ $\equiv 40^{23} \equiv 35 \mod 55$
$S \equiv \frac{K_2}{r} \equiv M^d \mod 55$ $\equiv \frac{35}{6} \equiv 15 \mod 55$	← $K_2 = 35$	

Schnorr 방식의 은닉서명



2.4 비밀분산

- 중요한 비밀정보를 여러 개로 나눔. 여러 사람에게 나누어서 보관



비밀분산과 문턱암호

- **필요성**
  - 매우 중요한 정보를 분산하여 보관해야 할 필요성
  - 어느 한 사람의 결정으로 업무를 수행하기 보다 합의에 의해 업무를 수행
  - 일부의 정보가 없어도 비밀정보를 복구 가능해야 함
  - 예: 핵무기 발사, 루트인증기관의 키 보관 (예: 5명 중에서 3명 이상이 합의하면 키복구 가능)
- **비밀분산**
  - n명 중 t명 이상이 합의하면 복구할 수 있도록 키를 분산
- **문턱암호**
  - n명 중 t명 이상이 합의하여 키를 복구하고 사용

비밀분산과 문턱암호

- **Shamir의 비밀분산 기법**
  - Lagrange Interpolating Polynomial Scheme
  - (t, n) 비밀 분산
    - n : share
    - t 개 이상의 share가 모이면 정보 복원 가능
    - t – 1차 다항식 이용

비밀 분산 (계속)

- **Lagrange Interpolating Polynomial Scheme** 예
  - $p = 17$, $K = 11$일 때 $a = 7$, $b = 8$로 (3, 5) 구성
  - $F(x) = ax^2 + bx + K \mod p$

  - $K_1 = F(1) = 7\times1^2 + 8\times1 + 11 \equiv 9 \mod 17$
  - $K_2 = F(2) = 7\times2^2 + 8\times2 + 11 \equiv 4 \mod 17$
  - $K_3 = F(3) = 7\times3^2 + 8\times3 + 11 \equiv 13 \mod 17$
  - $K_4 = F(4) = 7\times4^2 + 8\times4 + 11 \equiv 2 \mod 17$
  - $K_5 = F(5) = 7\times5^2 + 8\times5 + 11 \equiv 5 \mod 17$
  - K_1, K_2, K_3, K_4, K_5 : share

비밀 분산 (계속)

❖ **Lagrange Interpolating Polynomial Scheme 예 (계속)**

➢ K_2, K_3, K_4가 모이면 $K = 11$ 복원 가능

$$K_2 = a \times 2^2 + b \times 2 + K \equiv 4 \mod 17$$

$$K_3 = a \times 3^2 + b \times 3 + K \equiv 13 \mod 17$$

$$K_4 = a \times 4^2 + b \times 4 + K \equiv 2 \mod 17$$

K 계산 가능

비밀 분산 (계속)

❖ 비밀키 K의 복구 방법

$$K = \sum_{j \in \Lambda} K_j \lambda_{j,\Lambda}$$

$$\lambda_{j,\Lambda} = \prod_{l \in \Lambda \setminus \{j\}} \frac{l}{l-j} \qquad \Lambda \quad : \text{모여진 비밀값들의 집합}$$

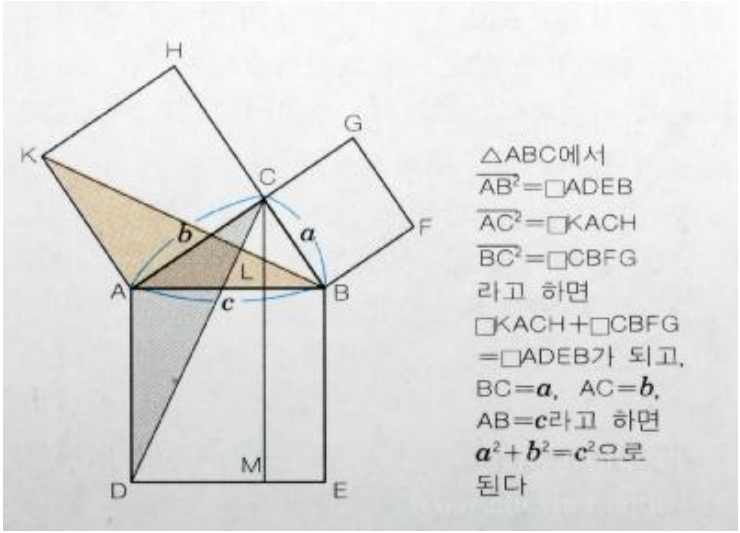
❖ 예: $\Lambda = \{1,2,3\}$ 인 경우

$$K = K_1\left(\frac{2}{2-1}\frac{3}{3-1}\right) + K_2\left(\frac{1}{1-2}\frac{3}{3-2}\right) + K_3\left(\frac{1}{1-3}\frac{2}{2-3}\right)$$

$$= 9 \cdot 3 + 4 \cdot (-3) + 13 \cdot 1 \bmod 17 = 11$$

2.5 영지식증명(Zero-knowledge Proof)

- **수학에서의 정리와 증명**
  - 자신이 주장하는 정리가 옳다는 것을 수학적으로 증명하여 공개
  - 피타고라스 정리
  - 공개적인 증명
- **공개할 수 없는 증명**
  - 비밀정보는 한번 공개하면 더 이상 쓸 수 없음
  - 알리바바와 40인의 도적
    – 보물동굴의 문을 여는 암호



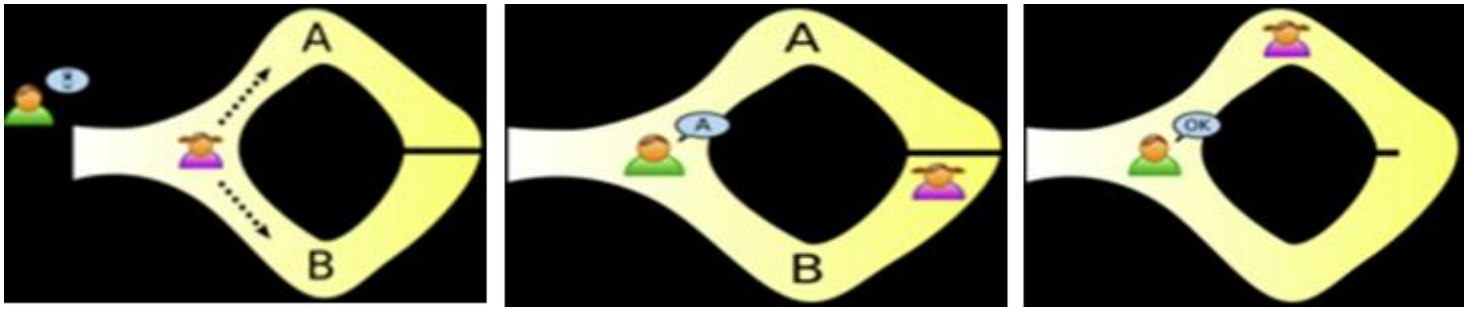
영지식증명(Zero-knowledge Proof)

- **영지식증명이란?**
  - 내가 알고 있는 어떤 중요한 정보에 대하여 그것을 보여주지 않으면서 그것을 알고 있다는 것을 상대방에게 증명해 보이는 방법
- **목적**
  - 비밀정보를 노출시키지 않고 반복해서 사용하기 위한 암호학적 방법

사례: 알리바바의 보물동굴

- 알리바바의 보물 동굴
  - 알리바바는 동굴의 문을 여는 암호를 알고 있지만 사람들에게 암호는 알려주지 않으면서도 자신이 암호를 알고 있다는 사실을 자랑하려고 한다.
  - 암호를 남들에게 얘기하는 순간 더 이상 암호가 아니다.

사례 : 동굴 실험



- **갑순이는 동굴의 문을 여는 암호를 알고 있지만 을돌이에게는 알려 주지 않고 자신이 암호를 알고 있다는 것을 증명하려고 한다.**
  1. 을돌이는 동굴 입구에서 기다리게 하고 갑순이는 갈라지는 지점에서 A 또는 B의 방향으로 임의로 선택하여 들어가서 비밀문 앞으로 간다. 이때 을돌이는 갑순이가 어느 방향으로 갔는지 알 수 없다.
  2. 을돌이는 동굴이 갈라지는 지점까지 와서 갑순이에게 A 또는 B의 어느 한 방향으로 나오도록 큰 소리로 말한다.
  3. 갑순이는 을돌이의 요구에 따라 A 또는 B의 방향으로 을돌이에게 간다. 갑순이는 필요한 경우 암호를 이용하여 비밀문을 열고 반대편으로 갈 수 있다.
  4. 1~3의 게임을 을돌이가 동의할 때까지 n회 반복한다.

이산대수값을 알고 있다는 것을 증명

- 증명자 **A**는 다음의 이산대수값 **x**를 알고 있다는 것을 **x**를 노출시키지 않고 증명하고자 함

$$x = \log_g Y, \qquad (\mathrm{Y} = g^x)$$

증명자 A

$t \in_R Z_q^*$

$R = g^t \bmod p$

$w = t - ux \bmod q$

검증자 B

$u \in_R Z_q^*$

R *Commitment* →

← u *Challenge*

w *Response* →

$\overset{?}{R} = g^w Y^u \bmod p$

Z_{23}에서의 승산표

x \ g	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
2	4	9	16	2	13	3	18	12	8	6	6	8	12	18	3	13	2	16	9	4	1
3	8	4	18	10	9	21	6	16	11	20	3	12	7	17	2	14	13	5	19	15	22
4	16	12	3	4	8	9	2	6	18	13	13	18	6	2	9	8	4	3	12	16	1
5	9	13	12	20	2	17	16	8	19	5	18	4	15	7	6	21	3	11	10	14	22
6	18	16	2	8	12	4	13	3	6	9	9	6	3	13	4	12	8	2	16	18	1
7	13	2	8	17	3	5	12	4	14	7	16	9	19	11	18	20	6	15	21	10	22
8	3	6	9	16	18	12	4	13	2	8	8	2	13	4	12	18	16	9	6	3	1
9	6	18	13	11	16	15	9	2	20	19	4	3	21	14	8	7	12	10	5	17	22
10	12	8	6	9	4	13	3	18	16	2	2	16	18	3	13	4	9	6	8	12	1
11	1	1	1	22	1	22	1	1	22	22	1	1	22	22	1	22	1	22	22	22	22
12	2	3	4	18	6	16	8	9	13	12	12	13	9	8	16	6	18	4	3	2	1
13	4	9	16	21	13	20	18	12	15	17	6	8	11	5	3	10	2	7	14	19	22
14	8	4	18	13	9	2	6	16	12	3	3	12	16	6	2	9	13	18	4	8	1
15	16	12	3	19	8	14	2	6	5	10	13	18	17	21	9	15	4	20	11	7	22
16	9	13	12	3	2	6	16	8	4	18	18	4	8	16	6	2	3	12	13	9	1
17	18	16	2	15	12	19	13	3	17	14	9	6	20	10	4	11	8	21	7	5	22
18	13	2	8	6	3	18	12	4	9	16	16	9	4	12	18	3	6	8	2	13	1
19	3	6	9	7	18	11	4	13	21	15	8	2	10	19	12	5	16	14	17	20	22
20	6	18	13	12	16	8	9	2	3	4	4	3	2	9	8	16	12	13	18	6	1
21	12	8	6	14	4	10	3	18	7	21	2	16	5	20	13	19	9	17	15	11	22
22	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

사례

- 암호시스템 파라메터 **p=23, g=7, q=22**
- 키생성 **x=13, y=20**
- 증명자는 **x=13**을 노출시키지 않고 이것을 알고 있다는 것을 증명하려고 함

증명자 A

$t = 5$

$R = 7^5 \bmod 23 = 17$

$R = 17$ *Commitment* →

$u = 8$ *Challenge* ←

$w = t - ux \bmod q$

$= 5 - 8 \times 13 \bmod 22 = 11$

$w = 11$ *Response* →

검증자 B

$u = 8$

$R \overset{?}{=} g^w Y^u \bmod p$

$17 = 7^{11} \times 20^8 \bmod 23$

$= 22 \times 6 \bmod 23 = 17$

두개의 이산대수값이 같다는 것을 증명

- X를 노출하지 않고 두개의 이산대수값이 같다는 것을 증명하는 방법

$$Y = g^x, Z = c^x$$
$$\log_g Y = \log_c Z$$

Prover

Verifier

$t \in_R Z_q^*$

$R_1 = g^t \bmod p$

$R_2 = c^t \bmod p$

R_1, R_2 *Commitment* →

$u \in_R Z_q^*$

← u *Challenge*

$w = t - ux \bmod q$

w *Response* →

$R_1 \overset{?}{=} g^w Y^u \bmod p$

$R_2 \overset{?}{=} c^w Z^u \bmod p$

두개의 이산대수값이 같다는 것을 증명

$Y = g^x, Z = c^x$ $\quad 7^5 = 17, 11^5 = 5$

$\log_g Y = \log_c Z$ $\quad \log_7 17 = \log_{11} 5$

Prover

Verifier

$t = 3$

$R_1 = g^t \bmod p = 7^3 = 21$

$R_2 = c^t \bmod p = 11^3 = 20$

$R_1 = 21, R_2 = 20$ *Commitment* →

$u = 6$

$u = 6$ *Challenge* ←

$w = t - ux \bmod q$

$= 3 - 6 \times 5 \bmod 22 = 17$

$w = 17$ *Response* →

$R_1 \overset{?}{=} g^w Y^u \bmod p$

$= 7^{17} \times 17^6 \bmod 23 = 19 \times 12 = 21$

$R_2 \overset{?}{=} c^w Z^u \bmod p$

$= 11^{17} \times 5^6 = 14 \times 8 = 20$

ElGamal 복호화의 정확성 증명

- 증명자의 키 쌍 $Y = g^x \bmod p$
- **ElGamal** 암호화 $U = g^r \bmod p$

  $V = mY^r \bmod p$
- **ElGamal** 복호화 $V / U^x \rightarrow m$

- 증명자는 암호문 **(U,V)**를 복호화하면 메시지 **m**이 얻어진다는 것을, 자신의 복호화 작업이 정확하게 이루어졌다는 것을, 비밀키 **x**를 노출시키지 않고 증명하고자 함.

ElGamal 복호화의 정확성 증명

- 증명자는 두개의 이산대수값이 같다는 것을 증명하는 방법을 이용하여 다음 두개의 이산대수가 같다는 것을 증명한다.

$$Y = g^x, \frac{V}{m} = U^x$$

$$\log_g Y = \log_U \frac{V}{m}$$

상호 통신이 필요 없는 영지식증명

- **Non-interactive Zero-knowledge (NIZK) proofs using Fiat-Shamir Heuristic**

$$x = \log_g Y \bmod p, \qquad (\mathrm{Y} = g^x \bmod p)$$

Prover		Verifier
$t \in_R Z_q^*$		
$R = g^t \bmod p$	$\xrightarrow{(R, w)}$	$u = H(Y, R)$
$u = H(Y, R)$		$R \overset{?}{=} g^w Y^u \bmod p$
$w = t - ux \bmod q$		

3. 암호프로토콜의 응용

- 현실세계 서비스의 안전한 구현
  - 전자정부
  - 전자지불 – 교통카드, 전자화폐, 신용카드 지불, 모바일 결제
  - 경매서비스
  - 전자투표
- 보안 요구사항에 따라 다양한 암호프로토콜 기술을 조합하여 적용