RSA를 공격하는 방법

ZeroPage 31기 김도엽

목차

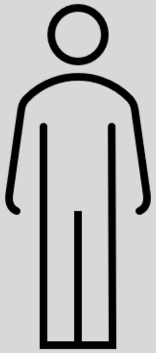
1. RSA는 공개키 암호 시스템 중 하나입니다
    1. 예시 - 작은 숫자로 이해해봅시다
    2. 개인키와 소수를 목숨 걸고 지켜야 하는 이유
2. Elementary Attack
    1. Common Modulus – 같은 N을 쓴다면?
    2. Blinding – 전자서명의 우회
3. Low Private Exponent
    1. 실제 공격 과정 – Wiener’s Attack
    2. 증명
4. Low Public Exponent
    1. 실제 공격 과정 - Hastad’s Boradcast Attack
    2. 중국인의 나머지 정리

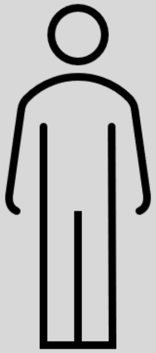
RSA는 공개키 암호 시스템 중 하나입니다

- $N = pq$ (p, q are primes), N is 1024 bits(p, q are 512 bits)
  - 1024 bits -> 309 decimal digits
- Select two integers e, d : $ed = 1 \, mod \, \varphi(N)$
  - $\varphi(N) = (p-1)(q-1)$
  - e와 d는 $\varphi(N)$과 서로소이면서 작아야 함

- e와 d는 어떻게 찾죠
  - e는 보통 (2의 16제곱 + 1)=65537
  - d는 확장 유클리드 호제법으로

RSA는 공개키 암호 시스템 중 하나입니다

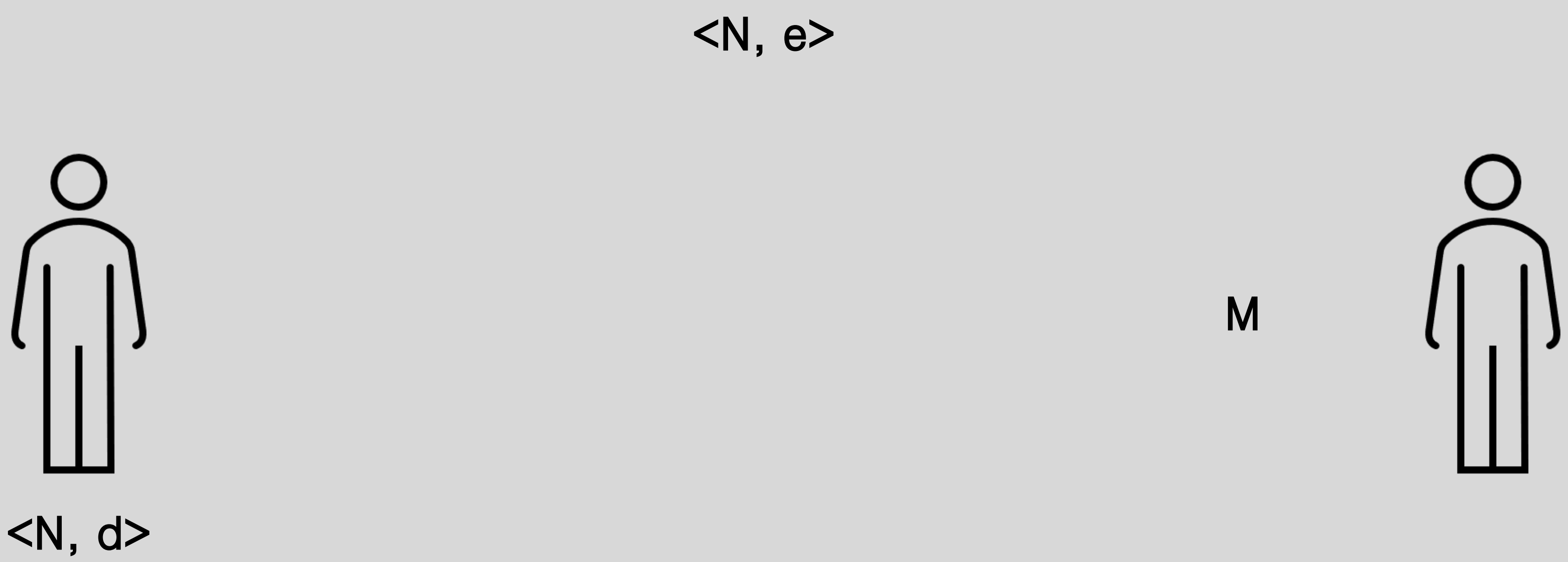




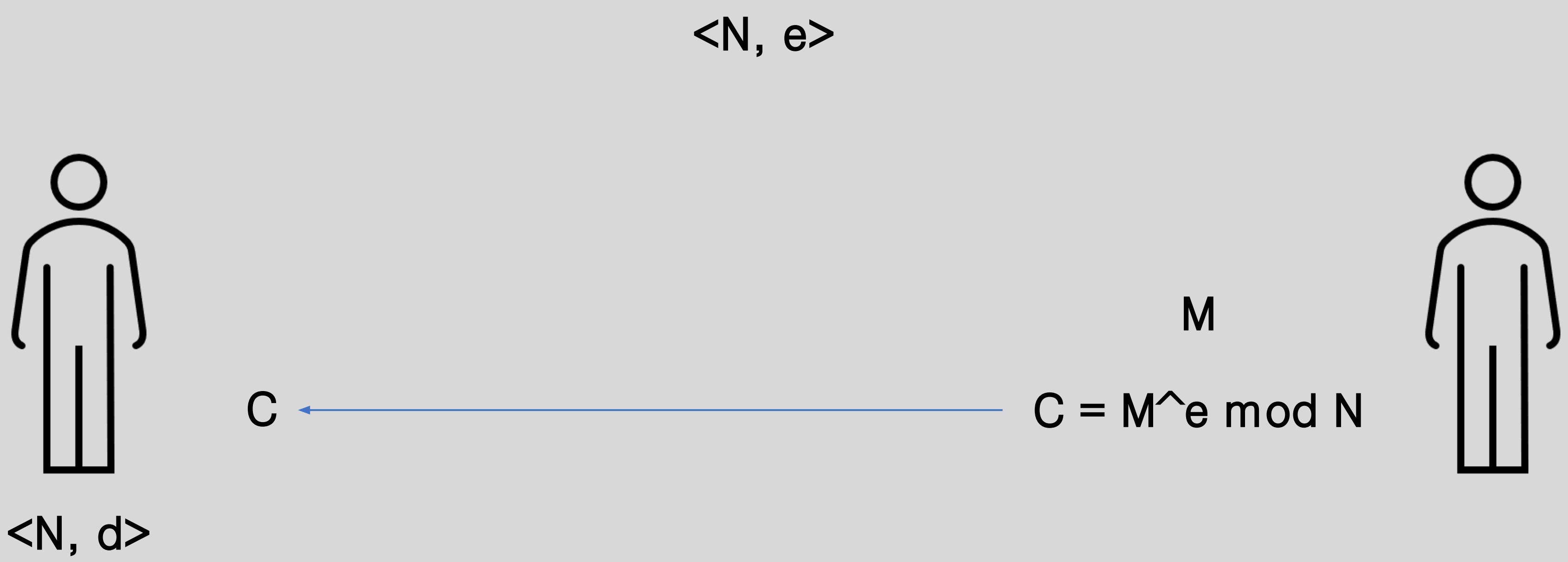
<N, e>

<N, d>

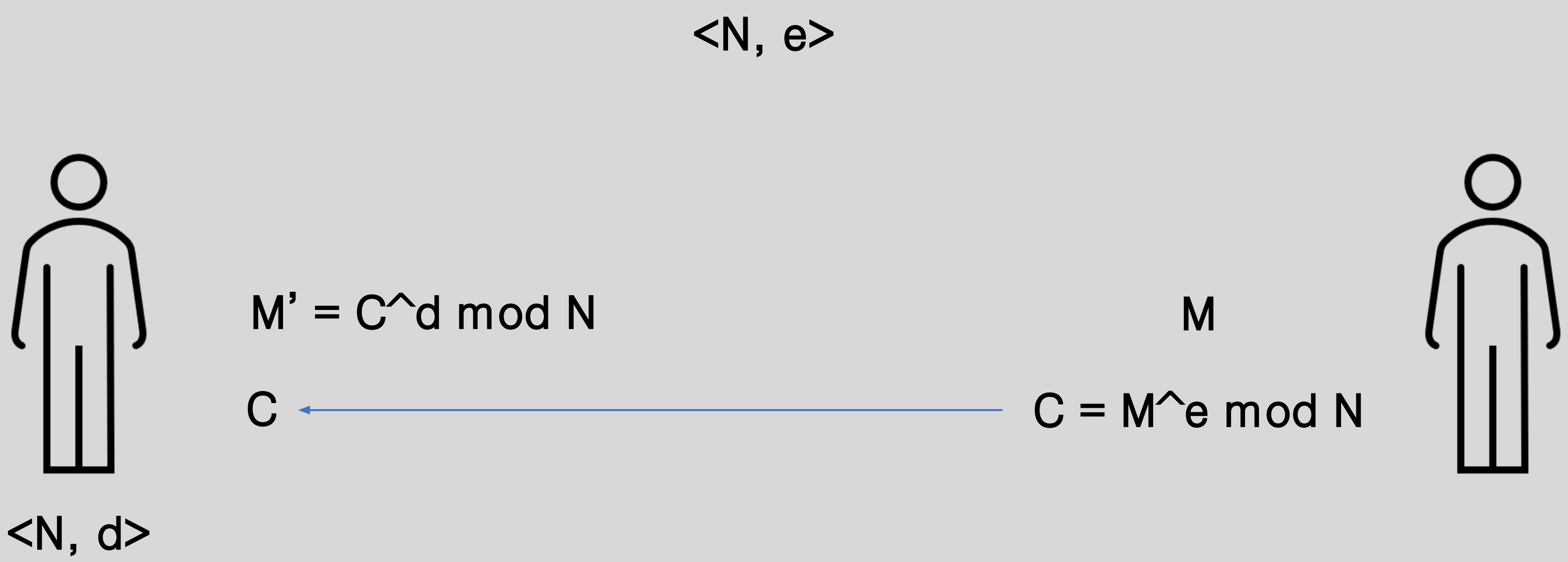
RSA는 공개키 암호 시스템 중 하나입니다



RSA는 공개키 암호 시스템 중 하나입니다



RSA는 공개키 암호 시스템 중 하나입니다



RSA는 공개키 암호 시스템 중 하나입니다

- 암호화 : $C \quad = M^e \bmod N$
- 복호화 : $M' = C^d \bmod N$

- $M = M'$ 가 성립하는가?

  $\Rightarrow$오일러의 정리 $a^{\varphi(N)} \equiv 1 \pmod N$

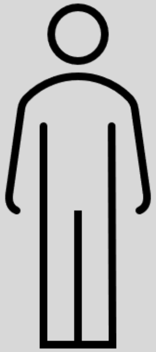
RSA는 공개키 암호 시스템 중 하나입니다

- $M' = C^d \ mod \ N = M^{ed} \ mod \ N = M^{k\varphi(N)+1} \ mod \ N$
  $= M \times M^{k\varphi(N)} \ mod \ N = M \times 1^k \ mod \ N = M$

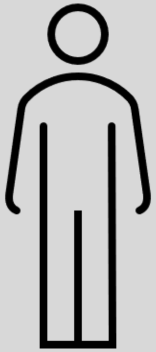
- $ed \equiv 1\left(mod \ \varphi(N)\right)$
  - $ed = k\varphi(N) + 1$

예시-작은 숫자로 이해해봅시다

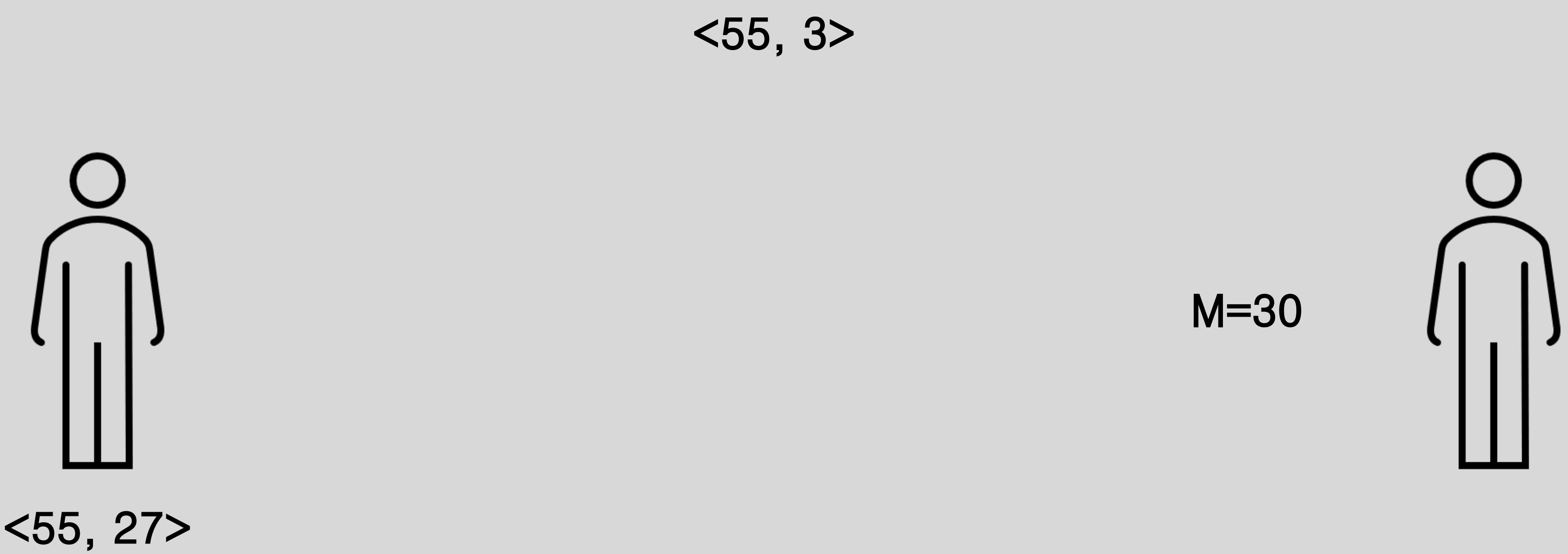
N=5*11=55
phi(55)=4*10=40
e=3, d=27



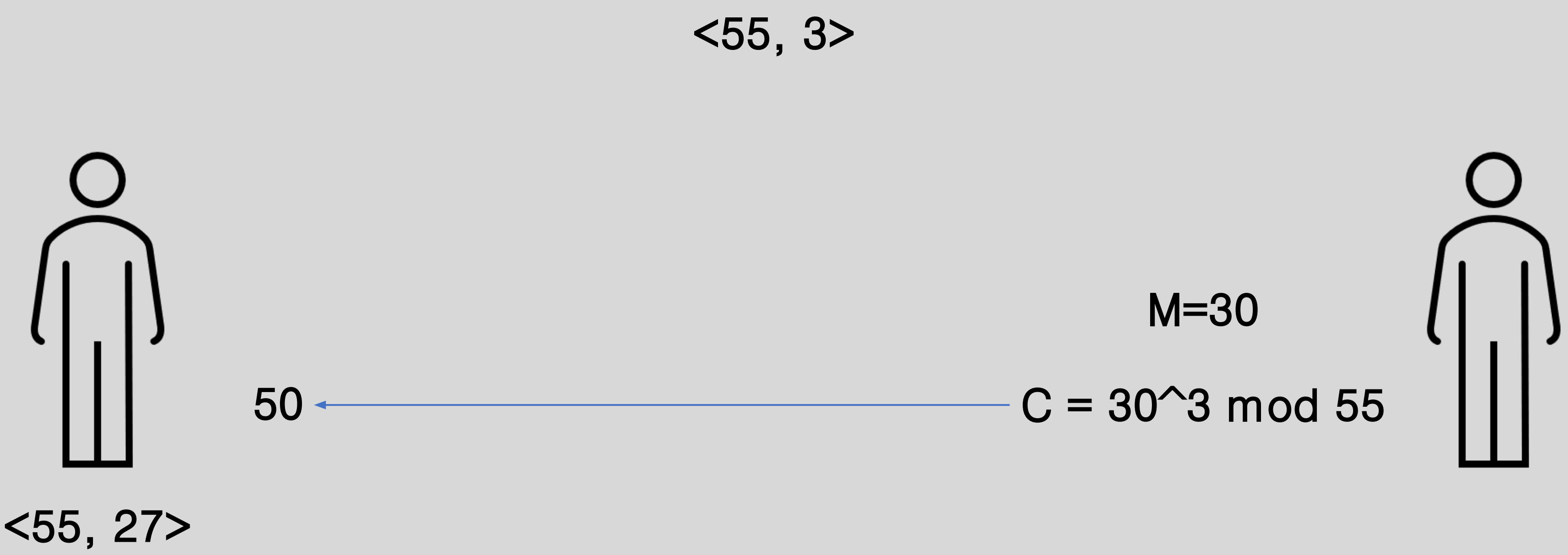
<N, e>
<N, d>



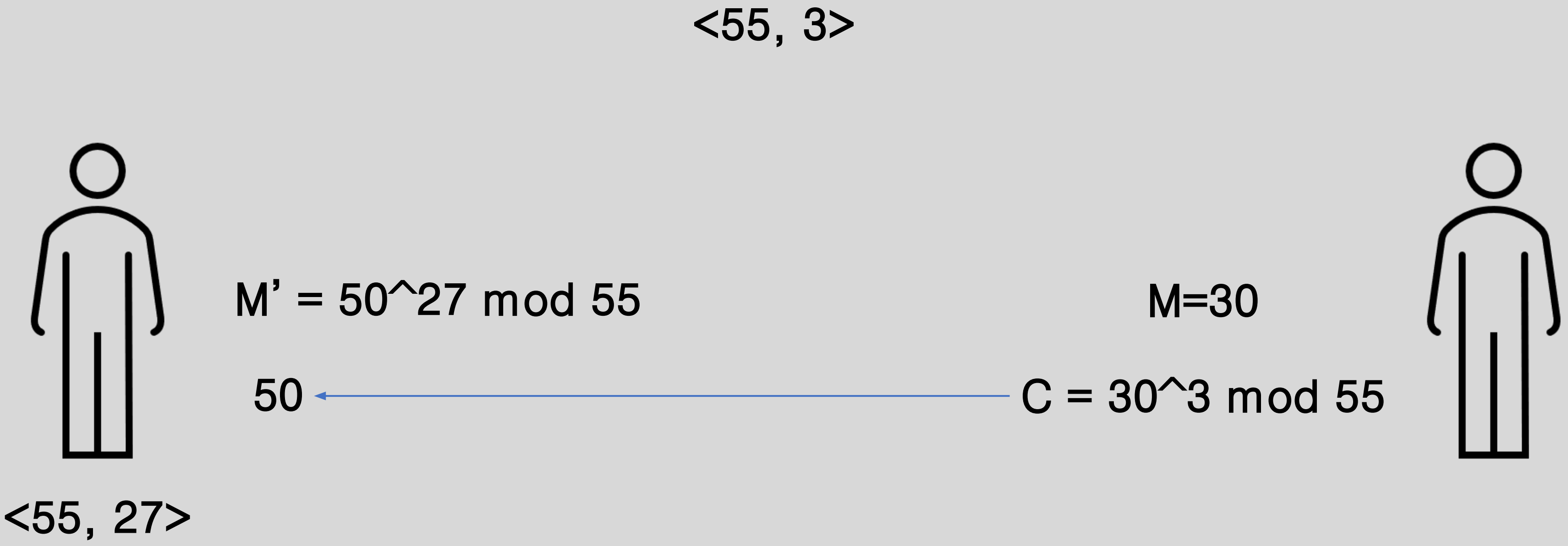
예시-작은 숫자로 이해해봅시다



예시-작은 숫자로 이해해봅시다



예시-작은 숫자로 이해해봅시다



개인키와 소수를 목숨 걸고 지켜야 하는 이유

- 공개 ：N, e
- 비밀(개인) ：d, phi(N), p, q
- 비밀 변수 중 하나라도 유출되면 개인키 복구 가능

- p or q -> N 인수분해
- phi(N) -> ed＝1(mod phi(N))으로 바로 d 복구
- d -> $O\left((\log_2 N)^3\right)$ 시간복잡도로 N 인수분해 가능
  - 중국인의 나머지 정리가 중심

RSA는 공개키 암호 시스템 중 하나입니다

- $N = pq$ (p, q are primes), N is 1024 bits(p, q are 512 bits)
  - 1024 bits -> 309 decimal digits
- Select two integers e, d : $ed = 1 \, mod \, \varphi(N)$
  - $\varphi(N) = (p-1)(q-1)$
  - e와 d는 $\varphi(N)$과 서로소이면서 작아야 함

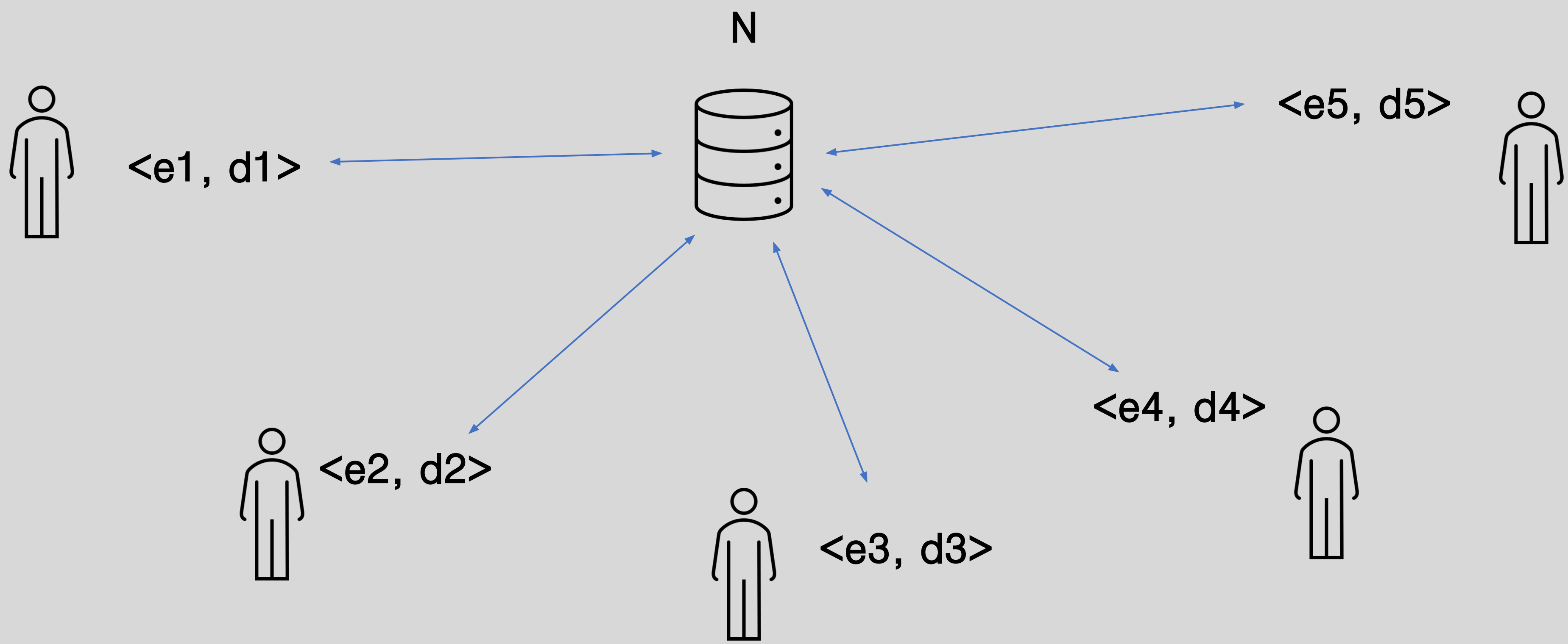
- e와 d는 어떻게 찾죠
  - e는 보통 (2의 16제곱 + 1)=65537
  - d는 확장 유클리드 호제법으로

Elementary Attack

- 직역 : 기본적인 공격

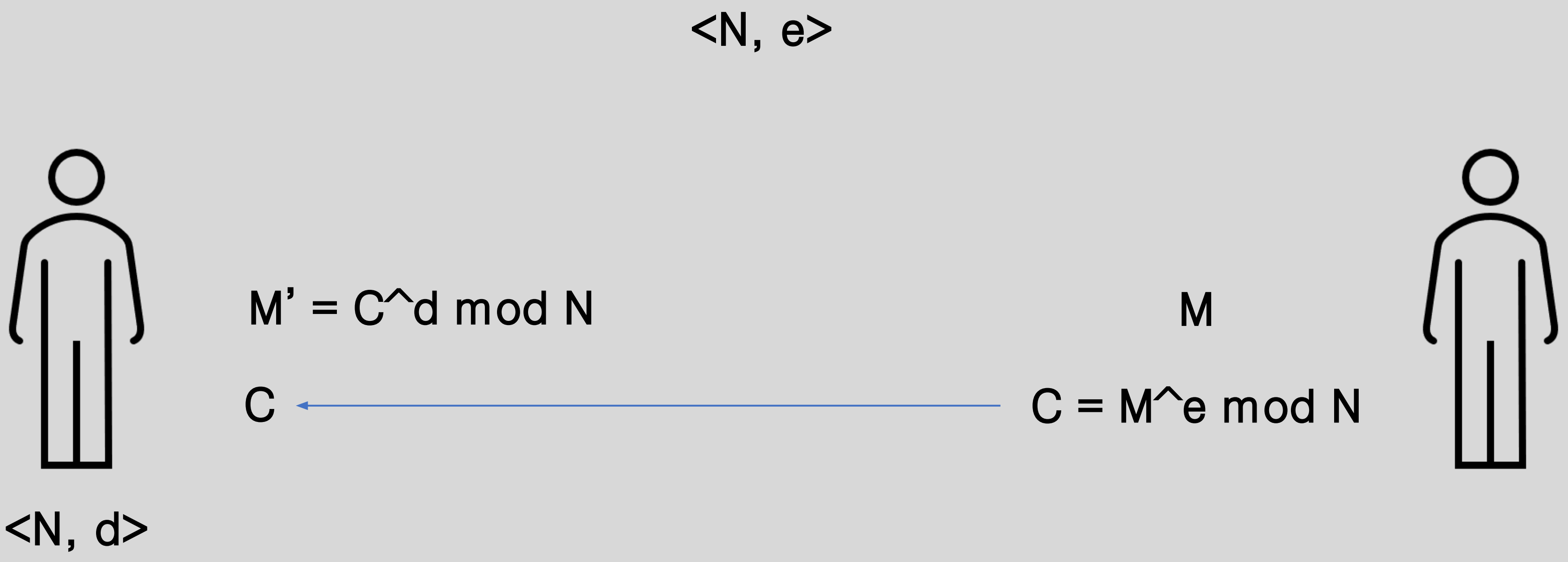
- Common Modulus
  - modulus : 법, mod N 에서 N 자리를 법이라고 함
  - 여러 사람이 같은 N을 사용할 때
- Blinding
  - 전자서명을 대충 보안처리 했다면?

Common Modulus



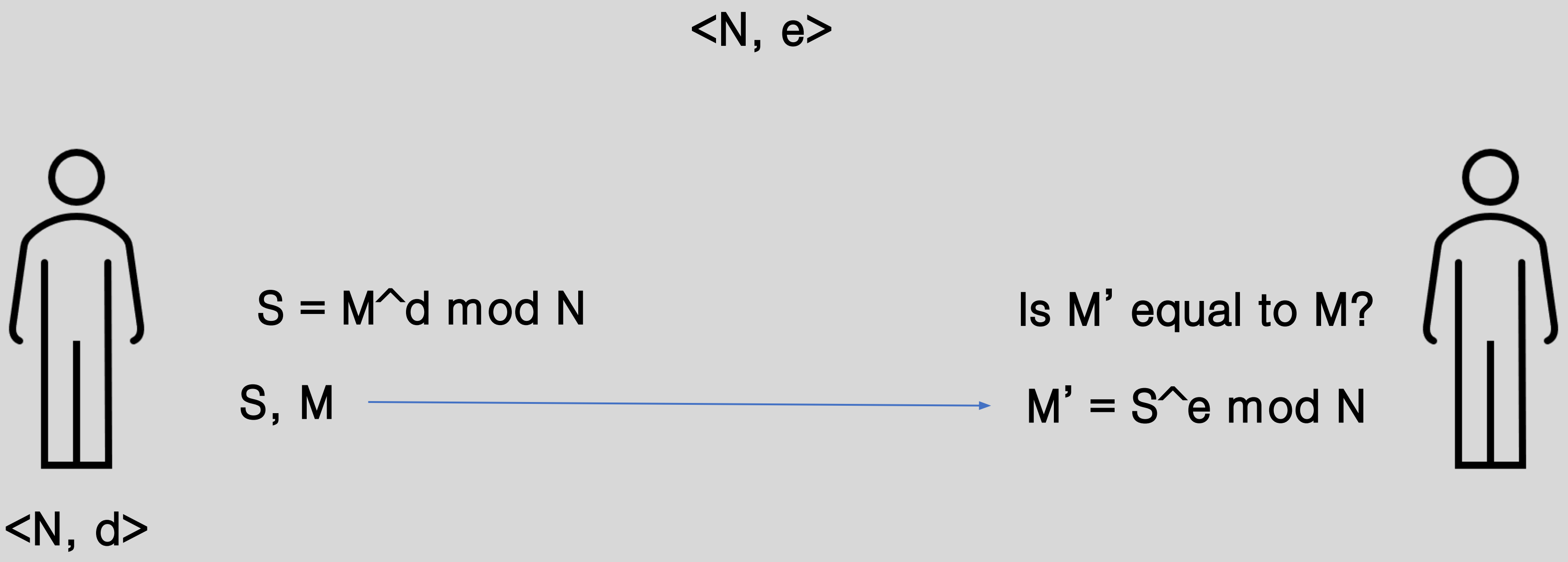
Blinding

- 전자서명이란?
  - 암복호화를 반대로 하면 전자서명



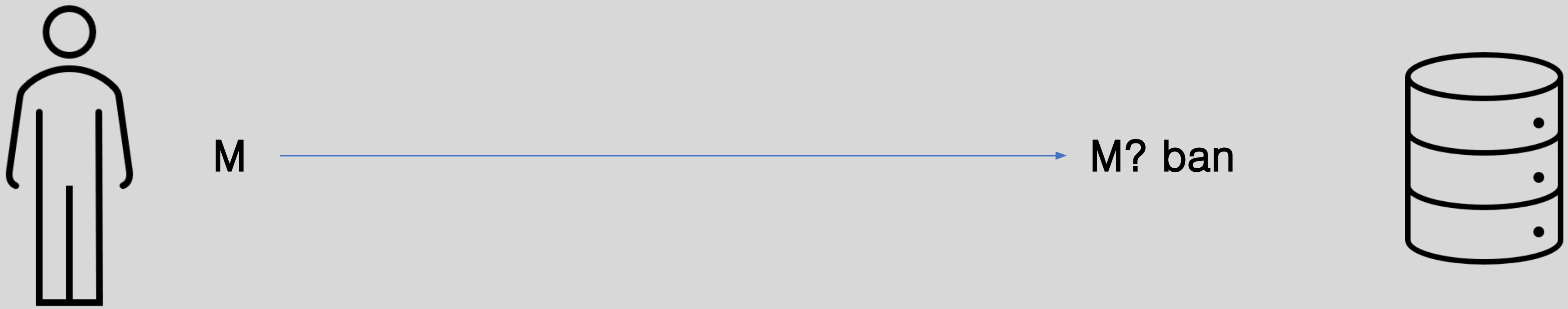
Blinding

- 전자서명이란?
  - 암복호화를 반대로 하면 전자서명



Blinding

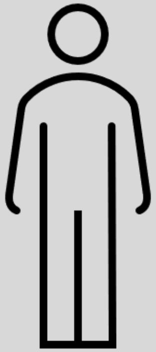
악의적인 공격자
wants to sign M



Blinding

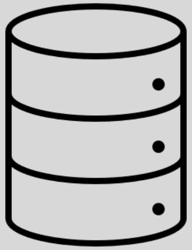
악의적인 공격자

wants to sign M



M’=r^{e}M mod N

S’=(M’)^d mod N



S=S’/r mod N

$$S = \frac{S'}{r} = \frac{M'^{d}}{r} = \frac{r^{ed}M^{d}}{r} = \frac{r^{k\varphi(N)+1}}{r}M^{d} = M^{d} \bmod N$$

Low Private Exponent

- 개인키 ⟨N, d⟩에서 $d < \frac{1}{3}N^{\frac{1}{4}}$ 이면 d를 복구할 수 있다.

- 보통 e가 크면 d가 작을 확률이 커짐
  - 복호화 시간을 줄이기 위해 d를 작게 만들 때 생기는 취약점

실제 공격 과정 – Wiener’s Attack

Example [edit]

This section **may be confusing or unclear to readers.** In particular, it assumes ed ≡ 1 (mod φ(N)), unlike the rest of the article, which uses (mod λ(N)) instead. Please help
There might be a discussion about this on the talk page. *(April 2022) (Learn how and when to remove this template message)*

Suppose that the public keys are $\langle N, e\rangle = \langle 90581, 17993\rangle$
The attack shall determine d.

By using Wiener's Theorem and continued fractions to approximate d, first we try to find the continued fractions expansion of $\frac{e}{N}$. Note that this algorithm finds fractions in their lowest terms. We know that

$$\frac{e}{N} = \frac{17993}{90581} = \cfrac{1}{5 + \cfrac{1}{29 + \cdots + \cfrac{1}{3}}} = [0, 5, 29, 4, 1, 3, 2, 4, 3]$$

According to the continued fractions expansion of $\frac{e}{N}$, all convergents $\frac{k}{d}$ are:

$$\frac{k}{d} = 0, \frac{1}{5}, \frac{29}{146}, \frac{117}{589}, \frac{146}{735}, \frac{555}{2794}, \frac{1256}{6323}, \frac{5579}{28086}, \frac{17993}{90581}$$

We can verify that the first convergent does not produce a factorization of N. However, the convergent $\frac{1}{5}$ yields

$$\varphi(N) = \frac{ed-1}{k} = \frac{17993 \times 5 - 1}{1} = 89964$$

Now, if we solve the equation

$$x^2 - ((N - \varphi(N)) + 1)\,x + N = 0$$
$$x^2 - ((90581 - 89964) + 1)\,x + 90581 = 0$$
$$x^2 - 618x + 90581 = 0$$

then we find the roots which are $x = 379; 239$. Therefore we have found the factorization

$$N = 90581 = 379 \times 239 = p \times q.$$

Notice that, for the modulus $N = 90581$, Wiener's Theorem will work if

$$d < \frac{N^{\frac{1}{4}}}{3} \approx 5.7828.$$

Wiener’s Attack 증명

오차의 한계 [편집]

어떤 무리수의 n번째 근사분수는, 그것을 분모와 분자가 서로소인 분수로 나타내었을 때의 분모보다 작은 분모를 가진 어떠한 유리수보다 주어진 무리수에 가까이 근접해 있다.

이 때의 오차의 한계는 M을 주어진 무리수, 각각 p_n과 q_n을 n번째 근사분수의 서로소인 분자와 분모라 할 때, 다음과 같은 식으로 주어진다.

$$\left| M - \frac{p_n}{q_n} \right| < \frac{1}{2{q_n}^2}$$

또한, 다음 식

$$\left| M - \frac{P}{Q} \right| < \frac{1}{2Q^2}$$

을 만족하는 가장 작은 정수 Q에 대하여, 적당한 자연수 k가 존재하여 $P = p_k$와 $Q = q_k$를 만족한다.

Wiener's Attack 증명

- $ed = 1\ mod\ \varphi(N) \Rightarrow ed - k\varphi(N) = 1$
- $\left|\frac{e}{\varphi(N)} - \frac{k}{d}\right| = \frac{1}{d\varphi(N)}$

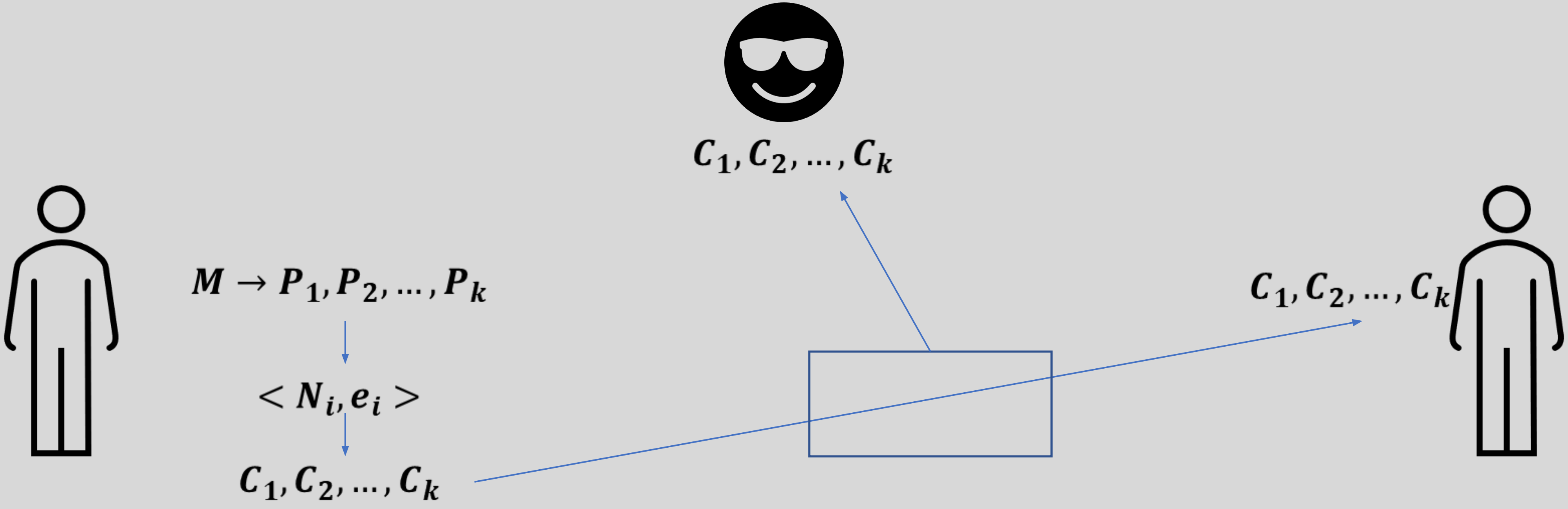
$$\varphi(N) = N - p - q + 1, p + q - 1 < 3\sqrt{N}, |N - \varphi(N)| < 3\sqrt{N}$$

- $\left|\frac{e}{N} - \frac{k}{d}\right| = \left|\frac{ed-k\varphi(N)-kN+k\varphi(N)}{Nd}\right| = \left|\frac{1-k(N-\varphi(N))}{Nd}\right| \leq \left|\frac{3k\sqrt{N}}{Nd}\right| = \frac{3k}{d\sqrt{N}}$

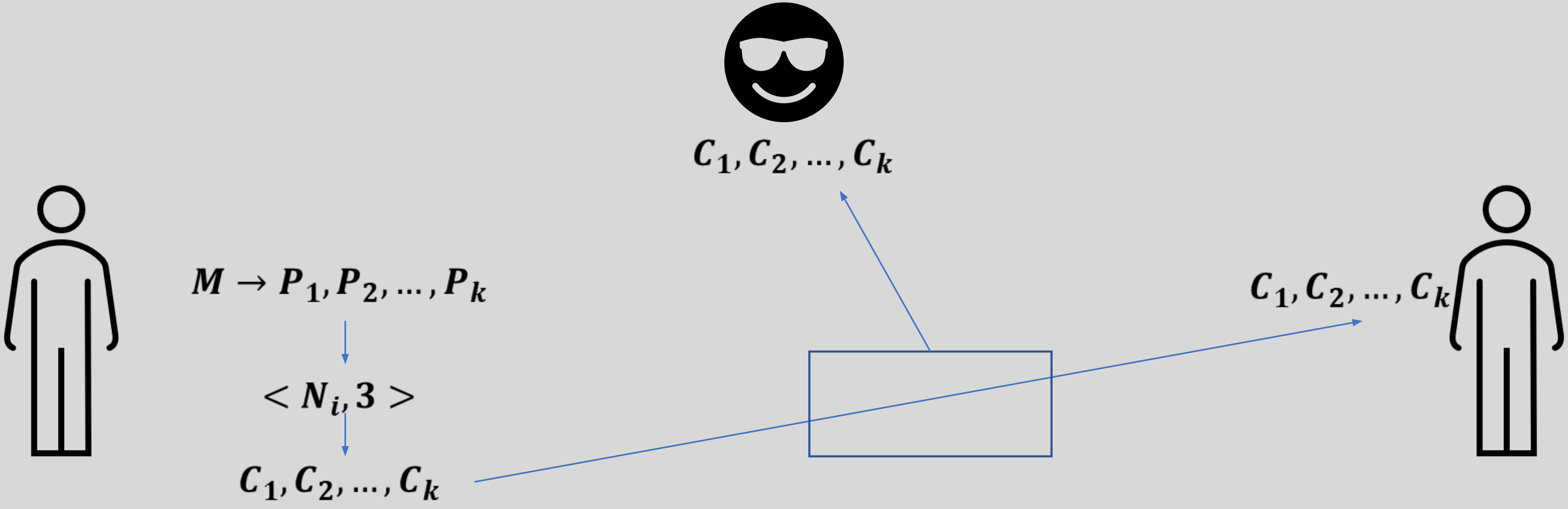
$$k\varphi(N) = ed - 1 < ed, k < d < \frac{1}{3}N^{\frac{1}{4}}$$

- $\left|\frac{e}{N} - \frac{k}{d}\right| \leq \frac{1}{d\sqrt[4]{N}} < \frac{1}{2d^2}$

Hastad’s Broadcast Attack



Hastad's Broadcast Attack



Hastad's Broadcast Attack

- $C_1 = M^3 \ mod \ N_1$
- $C_2 = M^3 \ mod \ N_2$
- $C_3 = M^3 \ mod \ N_3$

- for all i!=j, gcd(Ni, Nj)=1

중국인의 나머지 정리

- $M = 5, M^3 = 125$
- $N_1 = 7, N_2 = 11, N_3 = 13$
- $C_1 = 6, C_2 = 4, \quad C_3 = 8$
- $n_1 = 143, n_2 = 91, n_3 = 77$

- $143s_1 \equiv 3s_1 \equiv 1(mod\ 7)$
- $91s_1 \equiv 3s_1 \equiv 1(mod\ 11)$
- $77s_1 \equiv 12s_1 \equiv 1(mod\ 13)$

중국인의 나머지 정리

- $143s_1 \equiv 3s_1 \equiv 1(mod\ 7)$
- $91s_2 \equiv 3s_2 \equiv 1(mod\ 11)$
- $77s_3 \equiv 12s_3 \equiv 1(mod\ 13)$

- $s_1 = 5, s_2 = 4, s_3 = 12$
- $x \equiv a_1n_1s_1 + a_2n_2s_2 + a_3n_3s_3 \equiv 6 \cdot 143 \cdot 5 + 4 \cdot 91 \cdot 4 + 8 \cdot 77 \cdot 12 \equiv 125(mod\ 1001)$

질문

감사합니다.