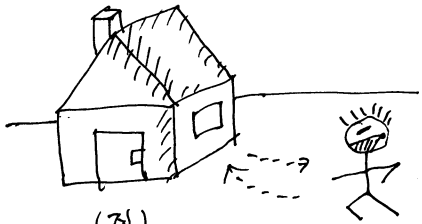
☒ 암호학 강의 노트 (양자 이론)

1) 암호란 무엇인가? (Cryptography)

- 질문) 암호란 무엇이고 보안과의 차이는 무엇인가?
  (Cryptography) (Security)

↓

예제) 도둑(강도)로 부터 집을 안전하게 지키려면 어떻게 해야 하는가?

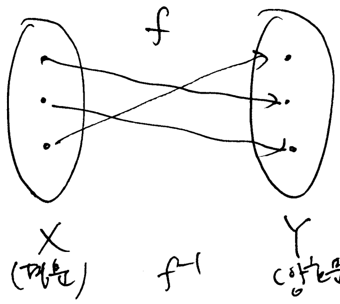


⇒ 문이나 열쇠로 닫고, 귀중품은 금고에 넣어 둔다. (기타 등등)

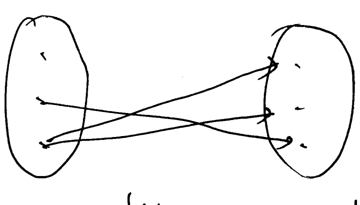
(암호 = 안전한 열쇠나 금고 만드는 것
(보안 = 열쇠나 금고 이외에서 집을 지키는 일

(ㄱ) 함수란 무엇인가?

> 함수(function) = (X, Y, f)
> - X = 도메인, Y = 이미지,
> - f = X→Y 가는 매핑. y=f(x)로 표기함

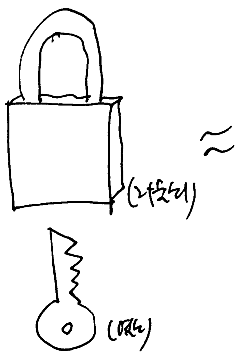


- 함수 x∈X가 두개 이상의 y로 매핑되면 함수가 아니다.

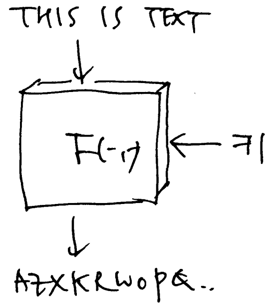


함수가 아니다 (why?)

- ⓑ) 물리적인 열쇠나 암호(암호기법)의 차이는 무엇인가?



≈



- 여기서 암호는 보안과 달리 정확한 [illegible] 필요하다.

> - 암호(Cryptography)는 기밀성, 무결성, 인증 등과 같은 정보보안의 목적을 달성하기 위한 수학적 테크닉(기술) 방법을 연구하는 학문.

(= 기법...)

- 그렇다면 컴퓨터(디지털 세계)에서 열쇠는 무엇인가? (컴퓨터에 해당하는 것)

↓

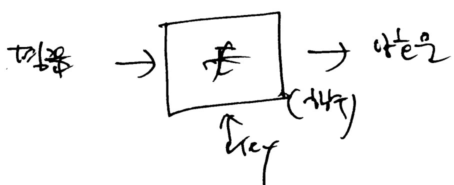
- 물리적인 열쇠는 컴퓨터에서는 함수(function)로 변환된다.

↓

why?

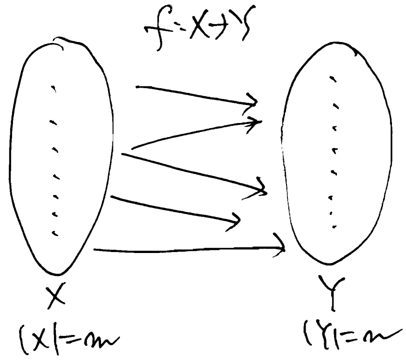
- 컴퓨터는 0이나 1의 디지털 데이터를 다루기 때문에, 모든 데이터(평문)는 다른 데이터(암호문)이 되도록 하는 함수(과정)로 변환해서 처리하는 것이다.

⇓

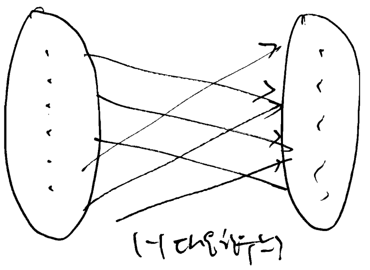


- 함수의 갯수 그리고 키

- 위 세기의 X에서 세기의 Y로 가는 함수는 얼마나 존재하는가?



$n * n * \cdots n = n^n$ (n개)



$n*(n-1)* \cdots *1 = n!$

- 가장 이상적인 (안전한) 함수는 역에서 선택된 것이 (모든 함수의 집합 F (X→Y)로 선택할 수 있는 것이다.

- 즉, 키로써 $f \in F$ 로 모든 가능한 함수 $n^n = 2^{n2^n}$ 가지의 키가 존재하기 때문에 이런 함수가 있으면 아주 안전하게 된다.

⇓

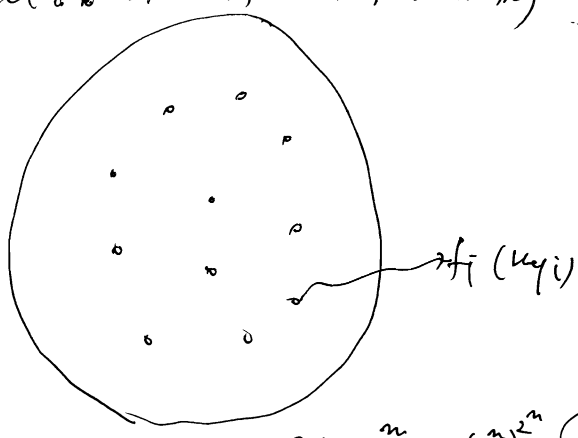
- 하지만 현실적으로는 불가능하다. 이유는 n^n $(=2^{n2^n})$ 가지의 키를 유일하게 지정하기 위해서는 $\log_2(2^{n2^n}) = n \cdot 2^n$ 개 비트의 비밀 키가 필요하다.

⇒ 세기 조금만 커져도 기하급수적으로 증가하여 키길이가 너무 커진다. (ㅜ)

⇒ 키길이는 줄여야 사용가능하다. 너무 크지 않도록

2015/3/30 ②

- 모든 함수의 집합 $\{f: X \to Y\}$ X에서 Y로 가는 (n^n)



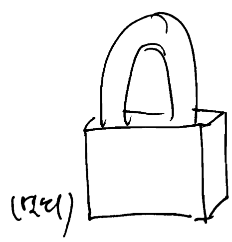
F, $|F| = n^n = (2^n)^{2^n} = 2^{n2^n}$

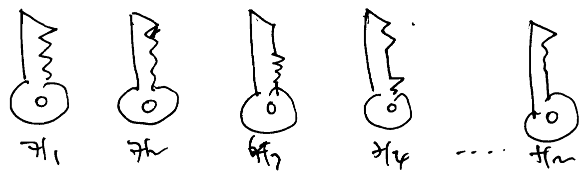
- 여기서 열쇠의 키에 해당하는 암호기법의 키는 n^n가지 함수 매핑중에 하나를 지정하는 역할을 한다 (index)

→ 따라서 암호의 키가 주어지면 하나의 X→Y로 가는 매핑이 유일하게 결정된다!

\+ 1-2) 안전한 열쇠란 vs 안전한 암호란?

- 열쇠가 안전하기 위한 조건은 무엇인가?

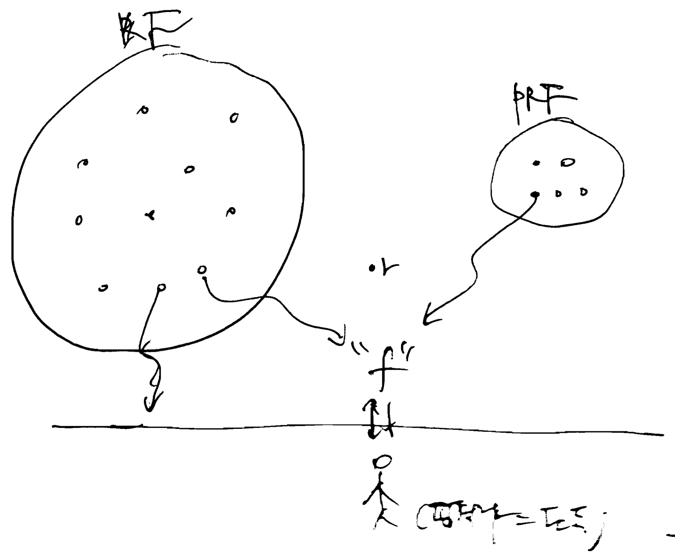




① 정해진 키는 유일해야 한다 (왜?)

② 가능한 키의 가짓수가 많아야 한다 (왜?)

- 랜덤 함수, 유사 랜덤 함수
- 예를 들어 모든 함수의 집합 F 에서 임의로 f 하나를 선택하여 f 사용하는 경우를 랜덤 함수라고 한다. (여기서 |F| = 2^{n2^n} 개로 한정)
- 유사 랜덤 함수는 F 집합의 아주 작은 일부(2^n) 함수로만 이루어진 함수의 집합이고, PRF ⊆ F 그러나 f_1 ∈ PRF, f_2 ∈ PRF 되어도 공격자(도둑)는 어떤 것이든 구분하지 못한다



- 공격자의 능력이 제한되지 않는다면 공격자는 F, PRF 쉽게 구분이 가능하다. (f 함수의 모든 x 에 대해 질의하여 비교해 보면 된다)

↓

어떻게 공격자 능력 제한해야 하는가?

(공격자는 시간과 자원으로 제한한다)

||

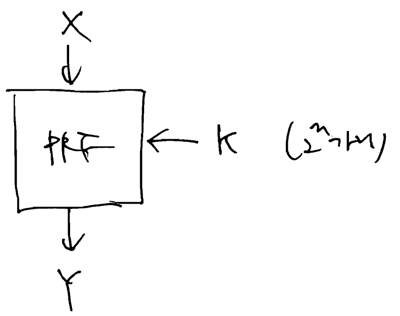
공격자에게는 무한시간, 무한대의 컴퓨터 자원이 아닌 제한된 시간 (다항식) 다항시간에 걸리는 것만 허용된다

↓

이유는?

- 현실에서의 공격자는 효율적이어야 하기 때문이다 (~~도둑~~ 도둑은 제한된 시간에 훔쳐야 하고, 무한(대의) 자원은 가지지 못한다)

- PRF = X × K → Y

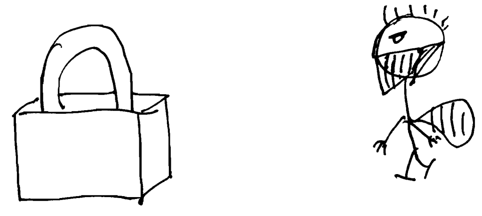


- PRF 함수는 전체 2^{n2^n} 가지의 모든 함수 F 중에서 오직 2^n 개만 사용이 가능하나, 공격자는 이를 구분하지 못한다 (눈

⇒ Q) F 와 PRF는 언제 다르게 보이지 않는 것인가?

(-3) 공격자는 누구인가? (도둑)

- Q) 우리가 일상생활에서 사용하는 열쇠는 모든 도둑에게 안전할까?



↓

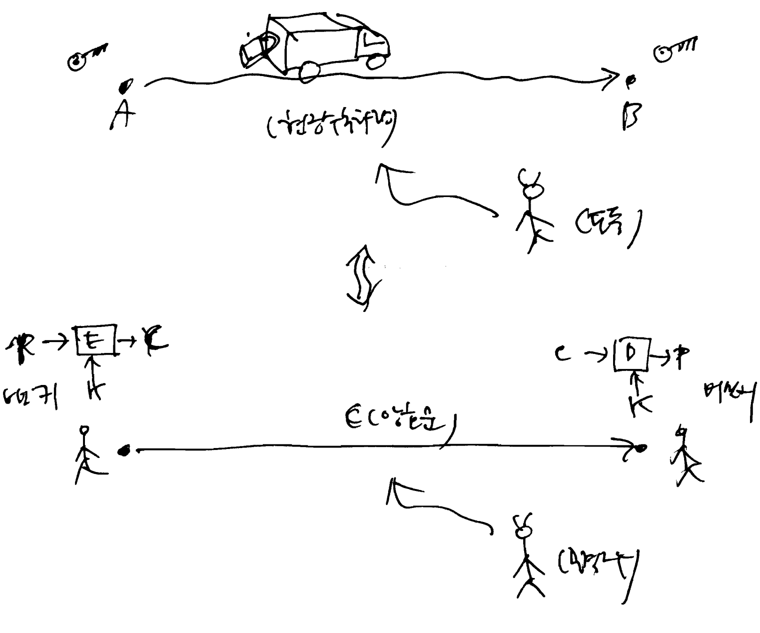
- 우리가 사용하는 열쇠는 좀도둑에게는 안전하나, 전문도둑에게는 취약할 수 있다. 이유는? (열쇠 복사할 수도 있고, 훔칠 때 .. 다양한 도구를 이용해서 열쇠 무력화시킬 수 있다)

⇓

∴ 열쇠는 모든 공격자에게 안전한 것이 아니라, 일정 능력이 제한된 도둑(좀도둑)에게만 안전

⇒ 공격자의 능력 제한해야 한다.

— 예제) 현금수송차 vs 대칭키 암호

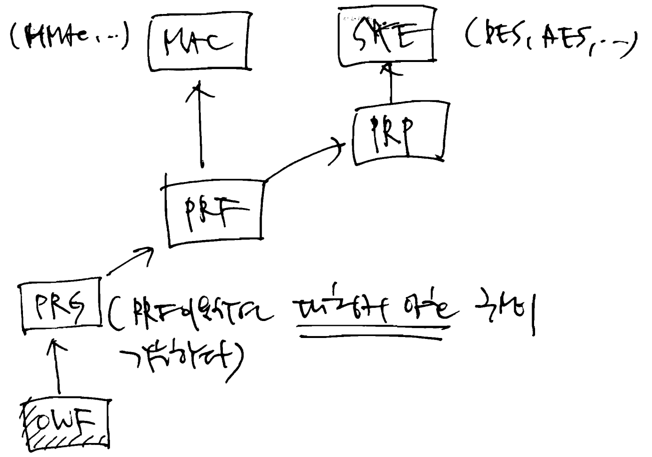


— 공격자는 비밀키 알지 못하기 때문에 가능한 PRF 함수의 갯수 중에서 하나를 추측해야 하기 때문에 어렵다.
([illegible])

— 그래서 암호는 키이외의 사항이 공개되더라도 안전하게 설계해야 한다.

1-4) PRF가 의미하는 바는

— PRF는 이론적인 대상이나 암호도구(도구..) 만드는 데 기초한다.



(PRF이 있어야 대칭키 암호 구현이 가능하다)

— Q) 앞에서 암호기법은 함수이고 안전한 암호는 PRF라고 하였다. 그러면 그러한 함수의 역이 존재할 수 있을까. 어떻게 f 계산하는 것과 f^{-1} 계산하는 것이 다를 수 있는가!

— A) "수학적인 트릭"가 필요하다. (단순하지 않다)

↓

RSA (RSA, 1978)

$PK = [N, e]$

$SK = [p, q, d]$ where $N = p \cdot q$, $e \cdot d \equiv 1 \bmod \phi(N)$

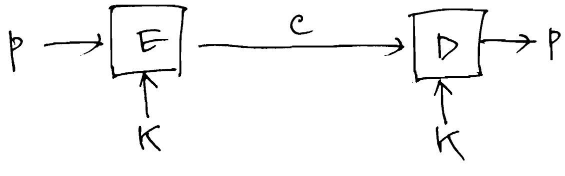
$C = M^e \bmod N$

$M = C^d \bmod N$.

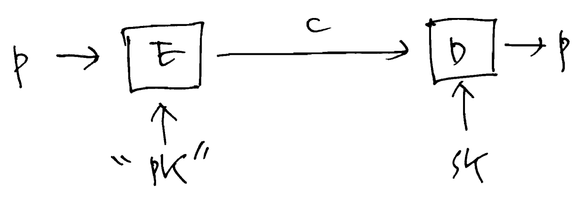
$$(M^e)^d \equiv M^{e \cdot d} \equiv M^{1 \bmod \phi(N)} \equiv M \bmod N.$$

2) 대칭키 암호 및 그 한계들

— 암호학이 하나의 학문으로 발돋움하게 된 계기는 1976년 공개키 암호 개념이 등장하면서이다. (Diffie-Hellman)



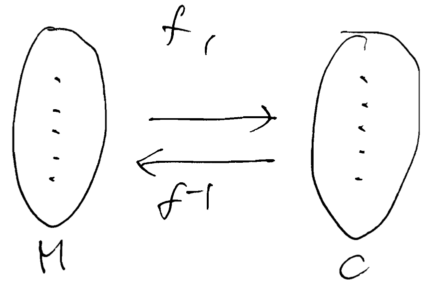
(기존의 암호 = 대칭키 암호)



(새로운 암호 = 공개키 암호) PK는 공개, PK는 모두에게 공개됨

2015/3/31 ⑤

— RSA 암호방식은 함수로 다시 설명해보면,

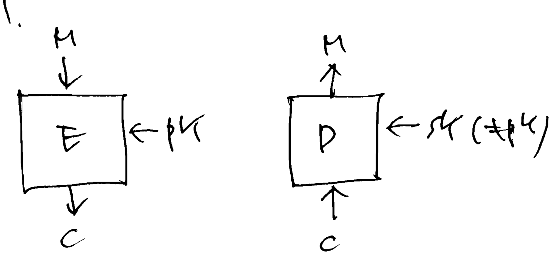


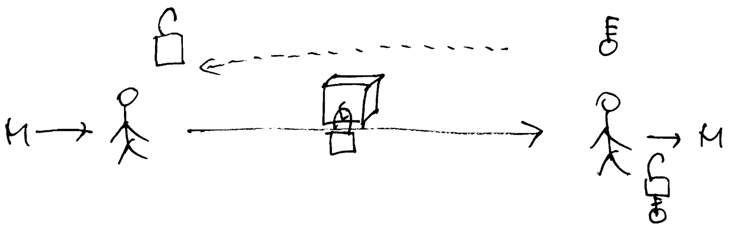
$$f(x) = x^e \bmod N$$

$$f^{-1}(y) = y^d \bmod N.$$

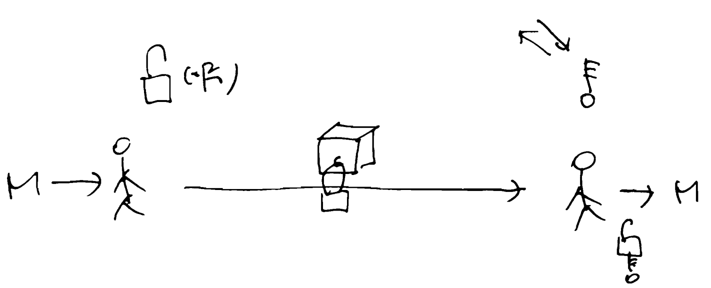
↓

— 이와같이 비대칭 함수를 TDF (트랩도어 함수) 라고한다.





(공개키 암호, 자물쇠(공개키) 먼저 가져와야 된다)

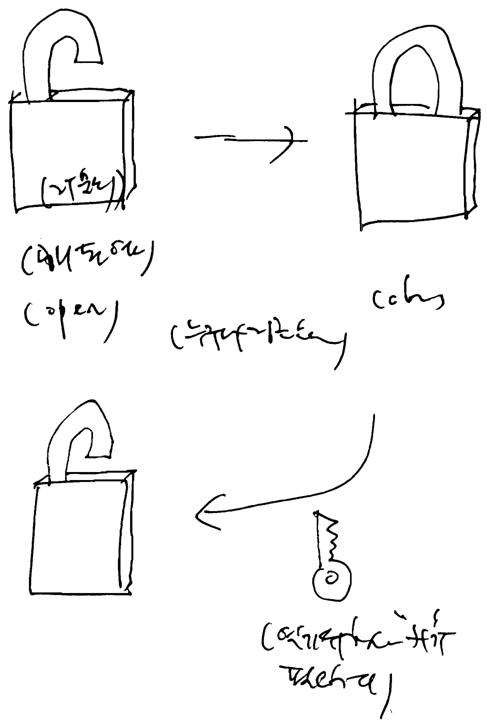


(아이디 기반암호, 자물쇠(이름) 가져와야한다)

⇓

Wow : (2001년에야 이 난제가 해결됨)

— 열쇠와 비교하면 TDF는 누구나 잠글수는 있지만 열어야하는 키가 필요한 형태다



⇒ (자물쇠 = 공개키, 열쇠 = 비밀키)

2-1) 아이디 기반 암호 (IBE)

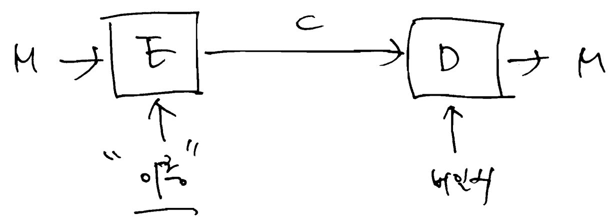
— 문제: 기존 공개키 암호(PKE) 경우 암호를 수행하기전 수신자의 공개키(자물쇠)를 보내야한다. 공개키 없이도 암호할 수는 없는가?

↓

임의 사용자의 이름이 공개키가 될수는 없는가!

⇓

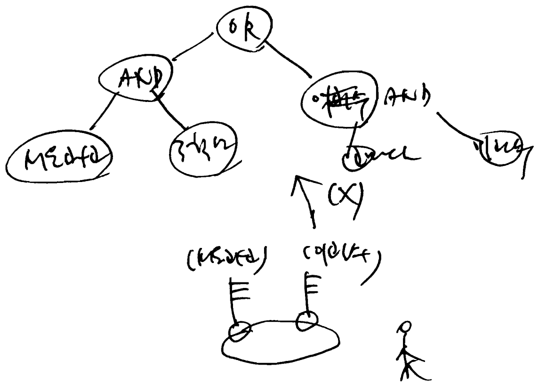
"있다." (IBE개념 (2001, BF제안)

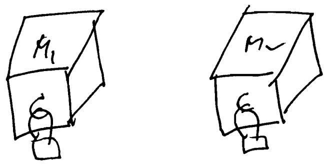


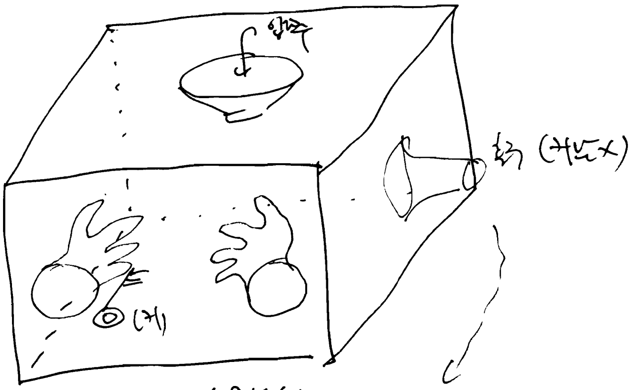
2-2) 속성기반 암호 (ABE)

- 내 개인키에 여러가지 속성을 넣을 수 있는 암호 방식이다. (Waters 등)

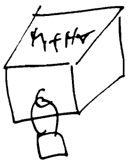
이 암호문은 (("서울대" AND "3학년") or ("이영수" AND "[illegible]"))







- (키를 따르는 사용방식)

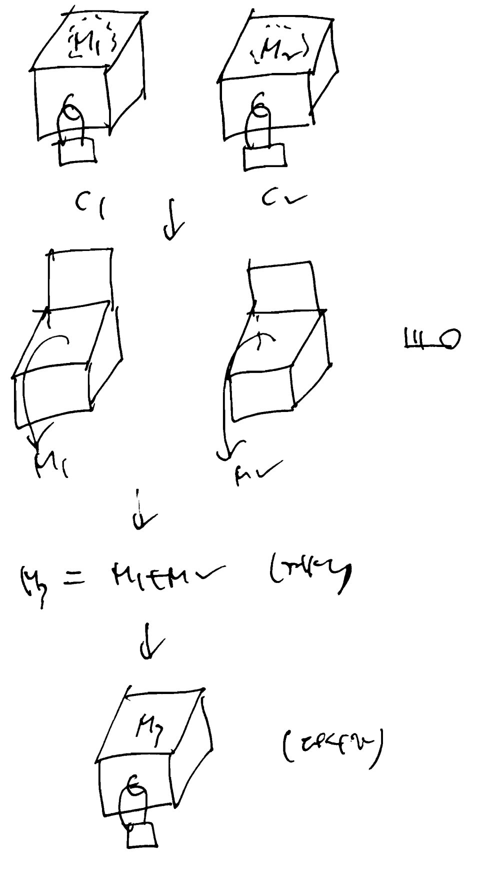


- 복잡한 수학적 구조(격자 등)를 이용해서 해결함.

2-3) 최근 암호학계 이슈들 (동형암호, 난독화) ⑥

- 최근 암호학계에서 흥미로운 일들이 벌어지고 있음. (동형암호, 난독화)

- 첫번째 이슈는 "동형암호"이다. 동형암호는 암호문을 복호하지 않고도 암호문에 필요한 연산을 계산하는 것이다.

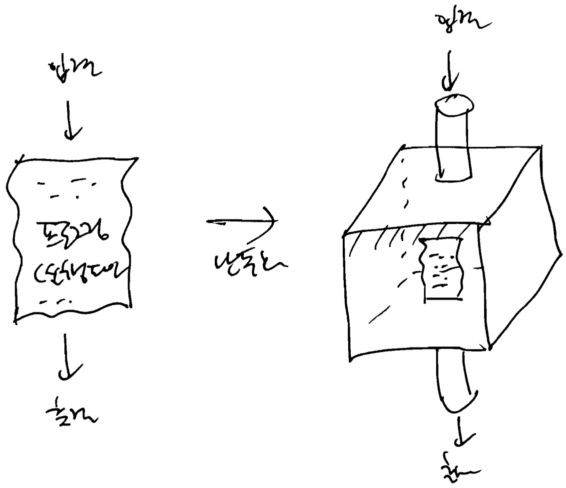


- 그래서 덧셈(AND)과 곱셈(OR) 연산 없이도 동작하는 것을 수학적으로 찾는가? (이게 가능하면 = 동형암호)

- 이건 암호학계의 30년된 난제.

- 2009년 스탠포드 대학의 Gentry (IBM) 박사가 [illegible] 해결을 수학적 (!!!)

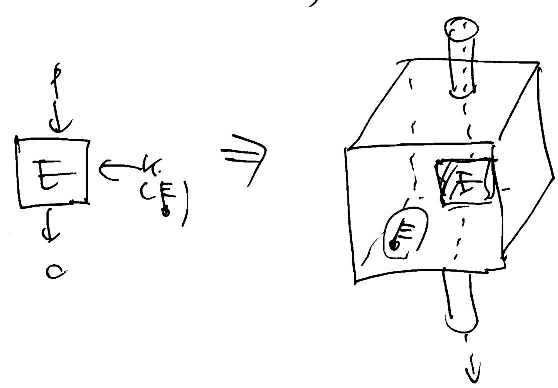
— 프로그램 난독화: 난독화는 기존의 프로그램의 입력과 출력은 제외한 다른 정보를 볼 수 없는 프로그램이다.



— 프로그램 소스코드는 숨겨져도 기계어로 컴파일되더라
⇒ 역공학에 의해 정보가 노출됨.

— 내부에 한 번에 숨겨져서 무엇이 일어나는지 모르도록 (블랙-박스)

— 난독화가 존재한다면 암호가 아주 쉬워진다 (대칭 → 공개)



— 난독화된 블랙-박스 내부에 E(키 포함) 연산(암호) 같이 넣어두면 된다.

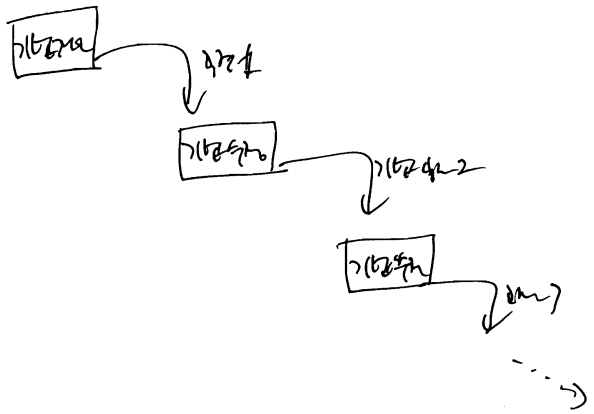
— 난독화된 블랙박스 공개하더라도 내부의 비밀키 (연산) 정보는 모르게 된다.

⇒ "암호화의 혁명"

3) 증명 가능한 안전성

— 이 암호기법이 안전하다는 것은 어떻게 보장할 수 있는가?

— 이론의 안전성 보장 방법은 다음과 같다 (환원적 안전성 보장방법)



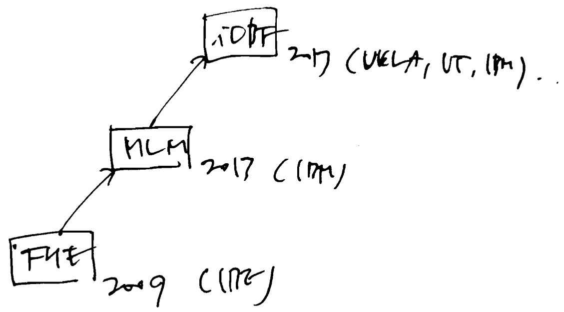
— 이 방법은 사람의 능력이 나타나지 않은 문제는 제외된 암호기법이 안전함을 보장한다.

⇒ 이) 앞으로도 영원히 어려운가 할 수 있는가? (앞으로도 이 문제를 풀지 못하는 보장은 어떻게 할 수 있는가?)

— 블랙-박스 형태로 숨기는 난독화는 불가능!

— 하지만 조금 약한 형태의 난독화는 가능하다 (2013년도!!)

— 이를 활용한 응용 많은 연구가 이루어질 수 있다!!!



- 가장 이상적인 방법은 공격자가 (기관은) 아무리 노력해도 기법을 깨뜨릴 수 없는 확률이 낮음을 수학적으로 증명하는 것이다.

↓

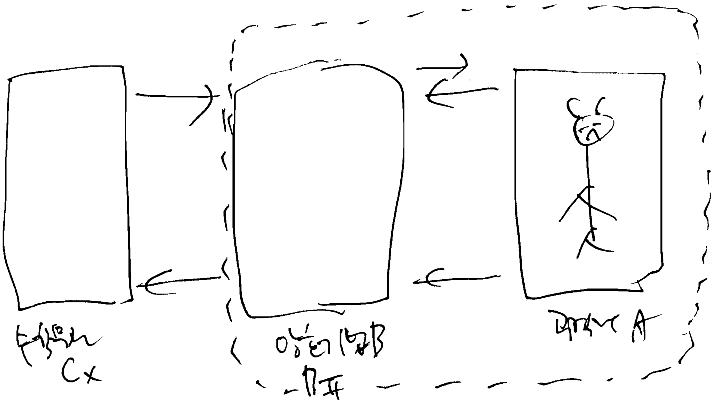
문제점.

- 이러한 확률적인 증명이 가능한 기법은 현실적으로 사용되기 어렵다 (OTP)
- 이유는 비용이나 길이가 너무 크거나, 다른 방법의 조작을 할 수도 있다.

↓

- 비록 확률적인 증명은 아니나, 다른 방법으로 증명할 수 (수학적) 없는가?
- 증명이 어려운 이유는 아직 밝혀지지 않은 무한한 가지의 모든 공격에 대해서 (어떠한 방법도) 안전함을 증명하는 것이 필요하다.

⇒ 이는 어떻게 수학적으로 다룰까?



- 만일 공격자 A가 암호기법을 깨뜨릴 수 있다면, Bπ 알고리즘은 A를 내부 알고리즘으로 이용하여 수학문제 X를 푸는 알고리즘으로 변환된다.
- 그러나 수학문제 X를 푸는 알고리즘은 존재하지 않는다 (아직까지 없다). 따라서 이는 수학문제가 어렵다는 것에 모순이다

⇒ 따라서 공격자 A는 없어야 한다 ⊛

무한한 경우에 대한 수학적 증명 방법

① 수학적 귀납법

- 각각의 경우가 순차적 연결되는 가정하에 차례대로 i+1 성립함을 보여서 모든 i에 대하여 성립함을 보인다.

↓

- 모든 공격은 연결되어 있지 않으므로 적용이 어렵다

⇓

"fail"

② 모순 이용한 증명

- 가정에 어긋난 상황이 모순 발생함을 유도해서 증명
- 즉,

↓

- 즉 만일 공격자가 존재한다면 가정이 어긋나 가정(?)... 모순을 유도함 (귀류법)

⇓

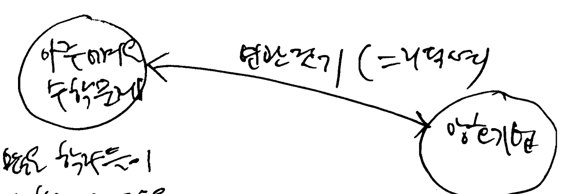
"succ"

+ 즉 "귀류법을 이용한 증명"

= 현대 암호 (1980년대이후)의 가장 중요한 성취 중에 하나는 암호기법의 안전성을 증명하는 방법을 소개한 것이다 (귀류법을 이용한 증명 ⇔ 모순이용한 증명)

↓

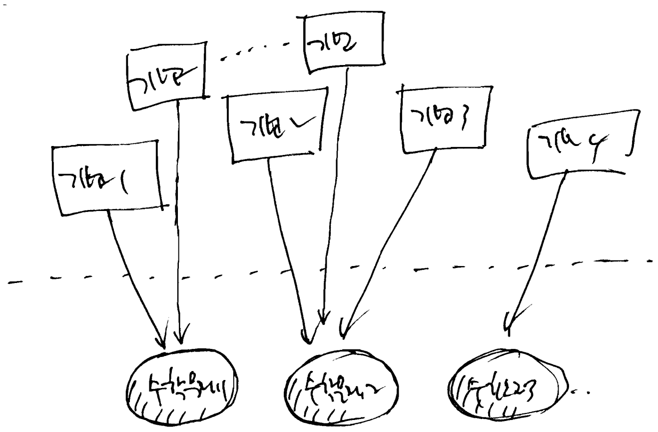
- 이 귀류법 증명이란 무엇인가?



- 많은 학자들이 연구해도 답을 발견하지 못하고 해결되지 않은 "어려운 문제"
- 예) N=p·q → 인수분해

- 암호기법
- 안전성은 어려운 수학문제에 의존하는 거다!

— 귀납적 증명의 장점과 단점 (사례1)



— 개별적으로 암호기법에 대한 연구 노력은 부합하는 대신 넓게 쓰이는 범위의 중요한 수학문제도 풀수있게 된다.

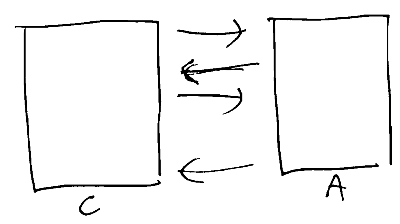
— 하지만 귀납적 증명 과정은 기법이 안전하다는 수학적 증명이 아니다 (왜?)

⇒ 수학문제가 어려우면 기법이 안전하다.
즉, 수학문제가 쉬우면 기법도 깨진다.

— 6) 암호기법이 안전함을 귀납적으로 증명 대신에 환원적으로 암호기법이 깨지는 경우가 없음을 (보일 수) 있는가?

↓

있다. 이유는?



— 증명 수행하기 위해서는 안전성 모델 정의해야한다. (공격자가 취할 수 있는 행동, 공격 목표).

— 또한 환원에서 공격자가 암호를 깨뜨리는 능력으로 어떤 수학적 문제를 풀 수 있어야 가능하다

— 하지만 증명이 틀리면 안된다. 이유는 오류가 많기 때문에.... (예)?

— 6) 그렇다면 수학문제(가정)이 어렵다는 것은 어떻게 보일수 있는가? 증명할수 있는가?

↓

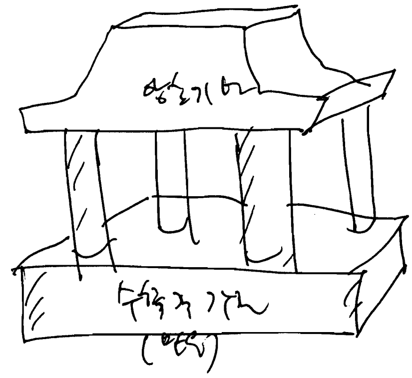
· 수학문제가 어렵다는 수학적 증명은 찾을 수 있다면 좋으나 아직 우리의 지식이 부족해서 증명하지 못한다

· 단지 오랜기간 동안 많은 수학자들이 노력했으나 해결하지 못했기 때문에 어렵다

- 수학문제(가정들) 마치 과학적 공리처럼 믿어야 한다

⇒ 가정을 믿는 방법에서, 기법의 안전성이 보장된다...
(약간이라도 증명없이 믿음이 필요하다.)

— 7) 그렇다면 암호는 사상누각이 아닌가?
(가정이 안전하려면 단지 믿어야 하고, 수학적 증명이 없기 때문에..)



— 수학적 가정에 대한 믿음이 무너지면 (깨지면) 모든 암호기법이 흔들릴수 있다.

↓

언뜻 불안한듯 보이지만
더 좋은 방법은 찾지 못했다 !!!