U-571과 Enigma

암호와 수학

차례

- 재미있는 암호 이야기
- 필요한 수학 ; 잉여산, 합동식
- Fermat 와 Euler
- RSA 공개키 암호
- Trapdoor Problem (쥐덫 문제)
- 이산로그 문제 (DLP)

U-571

- 그들은 왜 침몰하는 배(잠수함)에 올라갔을까 ??
- 목숨을 걸고..... (실제 영국 해군 여러 명 사망)
- 안전한 암호의 제조와 상대 암호의 해독이 전쟁의 승패를 가름
- 오늘날에는 ??

암호와 음어

- 음어 : “어제와 같은 시간 같은 장소에서 만나자”

- 암호 : 최초의 암호다운 암호는 로마의 Julius Caesar 시대
  - Substitution ; 문자들의 역할 바꾸기
  - Transposition ; 문자열의 순서 바꾸기

Subsitution 암호의 보기

평문	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
암호문	y	v	w	p	n	r	z	t	q	g	u	m	c	f	x	i	j	a	k	e	b	h	l	o	d	s

- 가능한 substitution 방법 ; 26!-가지
- $26! = 약\ 4 * 10^{26}$
  $= 403,291,461,126,605,635,584,000,000$

영문자의 사용빈도

a	8.04 %	n	7.09 %
b	1.54 %	o	7.60 %
c	3.06 %	p	2.00 %
d	3.99 %	q	0.11 %
e	12.51 %	r	6.12 %
f	2.30 %	s	6.54 %
g	1.96 %	t	9.25 %
h	5.49 %	u	2.71 %
i	7.26 %	v	0.99 %
j	0.16 %	w	1.92 %
k	0.67 %	x	0.19 %
l	4.14 %	y	1.73 %
m	2.53 %	z	0.09 %

Subsitution 암호의 보기

- 암호문 :

  etnan xfwn lyk y ryetna qf ebwkxf ltx kyqp etqk
  yphqwn qk rxa dxb kxf dxb pxfe lykt dxbaknmr
  lnmm kx dxba rnne kcnmm mqun tnmm qr qf vnp
  lqet y zqam unni dxba ktxnk xf

- 빈도 : n ; 12.1 %
  x ; 10.6 %
  k ; 9.1 %
  q ; 7.6 %

영문자의 사용빈도

a	8.04 %	n	7.09 %
b	1.54 %	o	7.60 %
c	3.06 %	p	2.00 %
d	3.99 %	q	0.11 %
e	12.51 %	r	6.12 %
f	2.30 %	s	6.54 %
g	1.96 %	t	9.25 %
h	5.49 %	u	2.71 %
i	7.26 %	v	0.99 %
j	0.16 %	w	1.92 %
k	0.67 %	x	0.19 %
l	4.14 %	y	1.73 %
m	2.53 %	z	0.09 %

n	e ?	12.1 %
x	t ?	10.6 %
k		9.1 %
q		7.6 %
m	l?	6.8 %
t		6.1 %
y	a?, i?	5.3 %
e		5.3 %
f		4.6 %

???

etnan xfwn lyk y ryetna qf ebwkxf ltx kyqp etqk
e e t e a a a e t t a

yphqwn qk rxa dxb kxf dxb pxfe lykt dxbaknmr
a e t t t t t a t e

lnmm kx dxba rnne kcnmm mqun tnmm qr qf vnp
e t t ee e e e e

lqet y zqam unni dxba ktxnk xf
a ee t te t

영문자의 사용빈도

- 가장 빈번하게 짝지워지는 철자 ;
  th > he > an > in > er, is, in, on, ou, ...
- 가장 빈번하게 사용되는 단어 ;
  the > of > and > to > a > in > .....

- 암호문에서는 ;
  xf > xb > et > tn > na, qk, qf, ...
- etn 3번

- 따라서, etn = the 로 가정
  etnan = there 로 가정
  ryetna = father 로 가정 (gather 로 가정 실패 후)
  q, x = o, i 로 가정

q=o, x=i ??!

etnan xfwn lyk y ryetna qf ebwkxf ltx kyqp etqk
there i e a a father o t i h ao tho

yphqwn qk rxa dxb kxf dxb pxfe lykt dxbaknmr
a o e o fir i i i i t a h i r e f

lnmm kx dxba rnne kcnmm mqun tnmm qr qf vnp
e i i r feet e o e he of o e

lqet y zqam unni dxba ktxnk xf
oth a or ee i r hie i

q=i, x=o ?!!

- etnan xfwn lyk y ryetna qf ebwkxf ltx kyqp etqk
  there o e a a father i t o ho ai thi

  yphqwn qk rxa dxb kxf dxb pxfe lykt dxbaknmr
  a i e i for o o o ot ah o r e f

  lnmm kx dxba rnne kcnmm mqun tnmm qr qf vnp
  e o o r feet e i e he if i e

  lqet y zqam unni dxba ktxnk xf
  ith a ir ee o r hoe o

- 따라서, k=s, l=w, p=d

OK !!!

- etnan xfwn lyk y ryetna qf ebwkxf ltx kyqp etqk
  there o e was a father i t so who sai this

  yphqwn qk rxa dxb kxf dxb pxfe lykt dxbaknmr
  a i e is for o so o o t wash o rse f

  lnmm kx dxba rnne kcnmm mqun tnmm qr qf vnp
  we so o r feet s e o e he if i e

  lqet y zqam unni dxba ktxnk xf
  with a ir ee o r shoes o

- 따라서, f=n, d=y, b=u, m=l

성공 !!!

etnan xfwn lyk y ryetna qf ebwkxf ltx kyqp etqk
there on_e was a father in t_ _son who sai_ this

yphqwn qk rxa dxb kxf dxb pxfe lykt dxbaknmr
a_ _i_e is for you son you _ont wash yourself

lnmm kx dxba rnne kcnmm mqun tnmm qr qf vnp
well so your feet s_ell li_e hell if in _e_

lqet y zqam unni dxba ktxnk xf
with a _irl _ee_ your shoes on

Subsitution + Transposition

- Subsitution 암호문 2 :

  etnanxfwnlykyryetnaqfebwkxfltxkyqpetqk

  yphqwnqkrxadxbkxfdxbpxfelyktdxbaknmr

- Subsitution 암호문 3 :

  etna nxfw nlyk yrye tnaq febw kxfl txky qpet

  qkyp hqwn qkrx adxb kxfd xbpx fely ktdx bakn

- Subsitution + Transposition 암호문 :

  aten wxnf klny eryy qnta wefb lxkf yxtk tpqe

  pkqy nqhw xkqr bdax dxkf xbxp yefl xtkd nabk

독일의 Enigma

- 제2차 세계대전 중 사용
- 4개의 substitution wheel
  - 문자의 사용빈도를 은폐하기 위해
  - 한 문자를 입력할 때마다 4개의 바퀴가 돌아가면서 substitution 규칙을 바꿈
- 매 8시간마다
  - 8개의 바퀴 중 4개를 선택하는 방법과
  - 끼우는 순서와 바퀴들의 초기 위치 변경
- "반사바퀴" .....

Bletchley Team

- 제2차 세계대전 때 영국의 암호해독반
- 런던 교외 Bletchley Park에 본부
- 많을 때는 10,000명의 직원
- 1970-1980년대 많은(?) 비밀문서 공개……

Alan Turing

- Bletchley Team의 연구원 A. Turing
- 결국은 시간과의 싸움 (8시간마다 새 subsitution 규칙……)
- Bombe, Collosus 등의 장비로 Enigma 해독 반자동화
  - 최초의 컴퓨터?
- 컴퓨터의 원리 발명 ; “Turing Machine”
- 컴퓨터의 등장과 발전 : 암호의 개념 자체를 바꿈

암호의 개념

영희

평문

암호화 과정

암호문

복호화 과정

평문

철수

盜士님

암호의 개념

- 메시지는 결국 숫자 (10진법, 2진법, ……)
  - Block 으로 나눌 수 있음
- 단어를 숫자로 substitute 할 수도 (코드북)
  - 주로 제1차 세계대전
- Enigma의 비밀키는 substitution 규칙

현대 암호

- **아예 암호화/복호화 방법(알고리즘) 공개**
  - 컴퓨터의 발달로 엄청난 computing power
  - 알고리즘 자체의 비밀에 의존할 수 없기 때문
- **비밀키(secret key)를 모르면 해독할 수 없도록 설계**
- **암호화의 필요성**
  - 무선 통신, 인터넷 등은 마음만 먹으면 "공격" 가능
- *혹 "나는 아무도 해독 못할 암호를 만들 수 있다....." ??*

현대 암호의 응용

- 군사, 외교 : 비밀 문서, 비밀 통신
- 은행 업무 : 인터넷 뱅킹, 은행간 거래
- 전자 화폐 : 인증, 위조(변조) 방지, 부인 방지
- 전자 투표 : 투표자 인증, 이중투표 방지, 비밀 유지 등
- 문서 보안 : 비밀 유지, 위조(변조) 방지
- 이동 통신 : 비밀 유지, 회원자격 확인

현대암호의 분류

대칭키 암호체계 Symmetric-Key Cryptosystem	블록 암호 (Block Cipher)	DES, AES, SEED ...
	스트림 암호 (Stream Cipher)	RC4, SEAL, ...
공개키 암호체계 Public-Key Cryptosystem	RSA (소인수 분해의 어려움) ECC (타원곡선 위에서의 이산로그 문제) XTR, NTRU, NICE, BGC, MOR, ...	

대칭키와 공개키 암호 체계

- 대칭키 암호 체계
  - U-571 : 그들은 왜 목숨을 걸고 암호화 규칙을 빼앗았을까?
  - 암호화 할 수 있으면 복호화도 할 수 있다.
- 공개키 암호 체계
  - 암호화 할 수 있어도 복호화는 할 수 없다.

대칭키 암호체계

암호화 키 : k

비밀키

=

사전에 공유

복호화 키 : k

비밀키

영희

평문

암호화 과정

f_k

암호문

복호화 과정

f_k^{-1}

평문

철수

Block Cipher와 Stream Cipher

- **Block Cipher : Subsitution + Transposition 의 결정판**
  - DES (Data Encryption Standard)
  - AES (Advanced Encryption Standard)

- **Stream Cipher :**
  - 예를 들어, 평문을 2진법 수로 생각할 때,
  - 비밀키는 평문 전체 길이와 같은 2진법 난수(random number)
  - 보기 : 평문 = 11010011
    비밀키 = 10111111
    암호문 = 01111100

  - 영화에 보면……

공개키 암호체계

암호화 키 : e

수신자의 공개키

≠

복호화 키 : d

수신자의 비밀키

영희

평문

암호화 과정

f_e

암호문

복호화 과정

g_d

평문

철수

17세기 파리 사교계의 두 ★

- Pierre de Fermat
  (1601 – 1665)

취미 ; 수학(정수론)

직업 ; 정치가(외교관)

$a^p \equiv a \pmod{p}$

$x^n + y^n = z^n \quad (n>2)$

- B. Pascal
  (1623 – 1662)

기하학
확률론
유체역학
철학
신학

“인간은 생각하는 갈대!”

Fermat's Little Theorem

- p 는 소수이고, gcd(a,p)=1 이면, $a^{p-1} \equiv 1 \pmod{p}$
- p 가 소수이면, $a^{p} \equiv a \pmod{p}$
- 증명 : ……
- Fermat 나 Euler 는 응용수학에는 무관심했지만……

Euler φ -함수

- 정의

  φ(n) = (n 보다 작은 자연수 중 n 과 서로 소인 것의 개수)

- 예; φ(6) = 2 (∵ { 1, ~~2~~, ~~3~~, ~~4~~, 5, ~~6~~ })

- 성질

  p 가 소수일 때, φ(p) = p-1

  a, b 가 서로 소일 때, φ(ab) = φ(a) φ(b)

  ∴ p≠q 가 소수이면, φ(pq) = φ(p) φ(q) = (p-1)(q-1)

Euler의 일반화

- a 와 N 이 서로 소일 때, 즉 gcd (a,N)=1 이면,

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

- 증명 : .....
- 보기 : $7^2 \equiv 1 \pmod{6}$
- Fermat's Little Theorem 은 N 이 소수인 경우

오일러 정리의 결과

- $p \neq q$ 는 소수, $N=pq$, $1 < e,d < N$,
  $ed \equiv 1 \pmod{\varphi(n)}$, $\gcd(x,N) = 1$ 이면,

$$x^{ed} \equiv x \pmod{n}$$

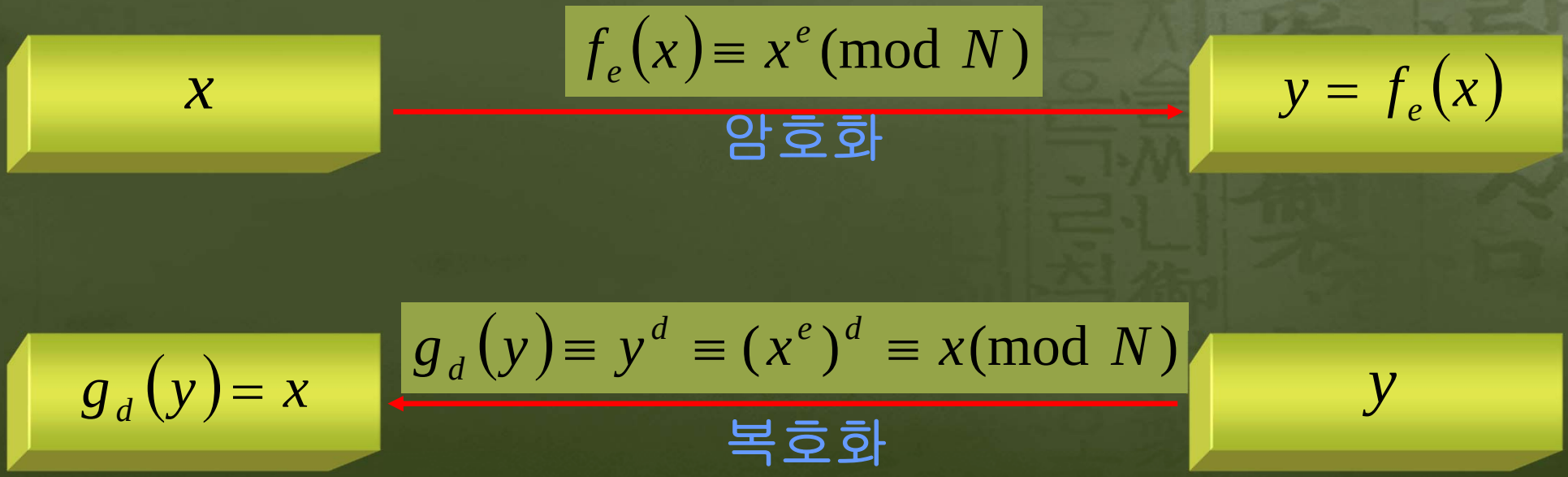
- 증명 : $\gcd(x,N) = 1$ 이므로, 오일러의 정리에 의하여

$$x^{ed} = x^{k\,\varphi(N)+1} = (x^{\varphi(N)})^k x \equiv 1^k x = x \pmod{N}$$

RSA 암호체계

- 1978년 Rivest, Shamir, Adleman에 의해 고안된 암호체계가 장 널리 쓰이는 공개키 암호체계

- 공개키 e 로 암호화하고, 비밀키 d 로 복호화한다.



p,q 소수, N=pq, $ed \equiv 1 \pmod{\varphi(N)}$

RSA 키 설정

- 단, $ed \equiv 1 \pmod{\varphi(N)}$, $\gcd(e,N)=1$

사람	공개키		비밀키	
	N	e	N = pq	d
A (영희)	N_A	e_A	$N_A = p_A q_A$	d_A
B (철수)	N_B	e_B	$N_B = p_B q_B$	d_B
.	.	.	.	.
.	.	.	.	.
.	.	.	.	.

누구나 안다

소유자만 안다

RSA의 안전성

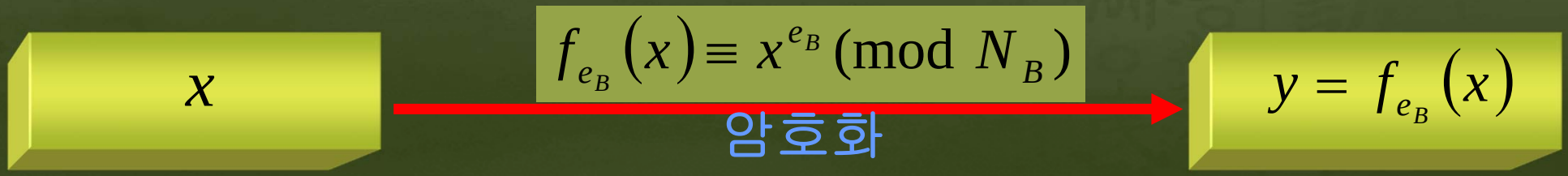
- 인수분해의 어려움에 의존

- 소수 $p, q \approx 2^{500}$, $N = pq \approx 2^{1000}$ 일 때,
  - p, q 알고 N 구하기 ; 1초
  - N 의 인수분해 ; (현재 기술로) 우주 역사보다 긴 시간 필요
    (100억년이나 1조년이나 오십보백보)

- p, q 알면, $\varphi(N) = (p-1)(q-1)$ 알 수 있고,
  - 이때 $d \equiv e^{\varphi(\varphi(n))-1} \pmod{\varphi(n)}$ 이므로, 비밀키 노출
    ($\because ed \equiv e^{\varphi(\varphi(n))} \equiv 1 \pmod{\varphi(n)}$)

RSA 암호화

- 상황
  - A 가 B 에게 메시지 x 를 암호화하여 보내고 싶을 때,
  - 단, $1 < x < N$
- 필요한 것 : 누구나 아는 B 의 공개키 (N_B, e_B)
  - $(x, N_B) \neq 1$ 일 확률은 $(p_B + q_B)/N_B \approx 2^{-499} = 0$ (!)
  - 따라서, $(x, N_B) = 1$
- B 에게 보내주는 것 : $x^{e_B} \pmod{N_B}$



$2^{-499} = 0$

- 만약 믿을 수 없다면, ...

- 로또 1등 확률을 (1조분의 1) = 10^{-12} 이라고 하면,
  - $10^{-12} = (10^3)^{-4} \approx (2^{10})^{-4} = 2^{-40}$
  - $10^3 = 1000 \approx 1024 = 2^{10}$

  - 두 주 연속 1등 당첨 확률은 $(2^{-40})^2 = 2^{-80}$
  - 12 주 연속 1등 당첨 확률은 $(2^{-40})^{12} = 2^{-480}$

큰 수의 지수 계산

- $N = pq \approx 2^{1000}$ 이고, $1 < x,e < N$ 일 때, $x^e \pmod N$ 계산?
- 보기 : x^{35409} ??
  - 무식한 방법 : x 를 35409 번 곱한다^^ ㅋㅋ
  - $35409_{10} = 1000101001010001_2$
  - $35409 = 2^{15}+2^{11}+2^9+2^6+2^4+1$
  - $(x^2)^2 = x^4 = x^{2^2}$, $(x^4)^2 = x^8 = x^{2^3}$, $(x^8)^2 = x^{16} = x^{2^4}$, ……
  - $x^{35409} = x^{2^{15}+2^{11}+2^9+2^6+2^4+1} = x^{2^{15}} x^{2^{11}} x^{2^9} x^{2^6} x^{2^4} x$

RSA 복호화

- 상황
  - B 가 A 에게서 받은 암호문 $y = x^{e_B}$ 를 복호화할 때,
- 필요한 것 : B 만 아는 비밀키 d_B
  - 단, $e_B d_B \equiv 1 \pmod{\varphi(N_B)}$
- 얻는 것 : $(x^{e_B})^{d_B} \equiv x \pmod{N_B}$

$g_{d_B}(y) = x$

$g_{d_B}(y) \equiv y^{d_B} \equiv (x^{e_B})^{d_B} \equiv x \pmod{N_B}$

복호화

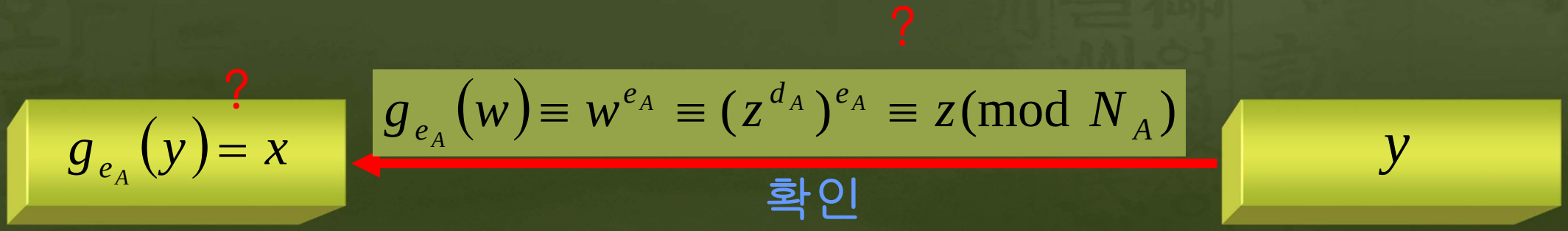
y

RSA 서명

- 상황
  - A 가 B 에게 메시지를 보내면서 자신임을 증명
  - 메시지 보낸 사실 부인 방지
- 필요한 것 : 서명 message z, A 만 알고 있는 A의 비밀키 d_A
- 보내주는 것 : (z^{dA}, x^{eB})
- B의 확인 과정 : A 의 공개키 e_A 이용

RSA 서명 확인

- 상황
  - B 가 A 에게서 받은 서명 $w = z^{d_A}$ 를 확인하고 싶을 때,
- 필요한 것 : 누구나 아는 A 의 공개키 (N_A, e_A)
- 확인 : $(z^{d_A})^{e_A} \equiv z \pmod{N_A}$?



Trapdoor (쥐덫) Problem

- 실마리(clue)를 알면 역함수를 쉽게 구할 수 있지만, Clue 를 모르면 역함수를 구하기 어려운 함수

- Trapdoor Problem 의 예
  - 소인수분해 문제 : RSA가 기반한 문제
  - 이산로그 문제(Discrete Logarithm Problem, DLP)
  - Diffie-Hellman 문제 등등

이산로그 문제 (DLP)

- 정의 : primitive element

P 가 소수일 때,
모든 y를 (단, $1 \le y \le p-1$)어떤 유일한 x에 (단, $1 \le x \le p-1$) 대하여
$y = g^x \pmod p$ 로 나타낼 수 있는 g가 (단, $1 \le g \le p-1$) 존재한다.

이런 g 를 primitive element (mod p) 라고 한다.

- 이산로그(discrete log) 문제의 정의

y와 primitive element g가 주어졌을 때,
$y \equiv g^x \pmod p$를 만족하는 x를 구하라.

$x \equiv \log_g y \pmod p$라고 쓰기도 한다.

Diffie-Hellman 문제

- DH 문제의 정의

  g 가 primitive element (mod p) 이고
  (a,b 둘 중 하나만 알고) g, g^a, g^b 를 알 때, g^{ab} 를 구하라

- DH 문제를 이용한 DH 키공유

  Alice : a 만 안다. g^a (mod p) 를 계산하여 Bob 에게 보낸다
  Bob : b 만 안다. g^b (mod p) 를 계산하여 Alice 에게 보낸다
  Alice : g^b 에 a 제곱을 하여 g^{ba} 를 얻는다
  Bob : g^a 에 b 제곱을 하여 $g^{ab} = g^{ab}$ 를 얻는다

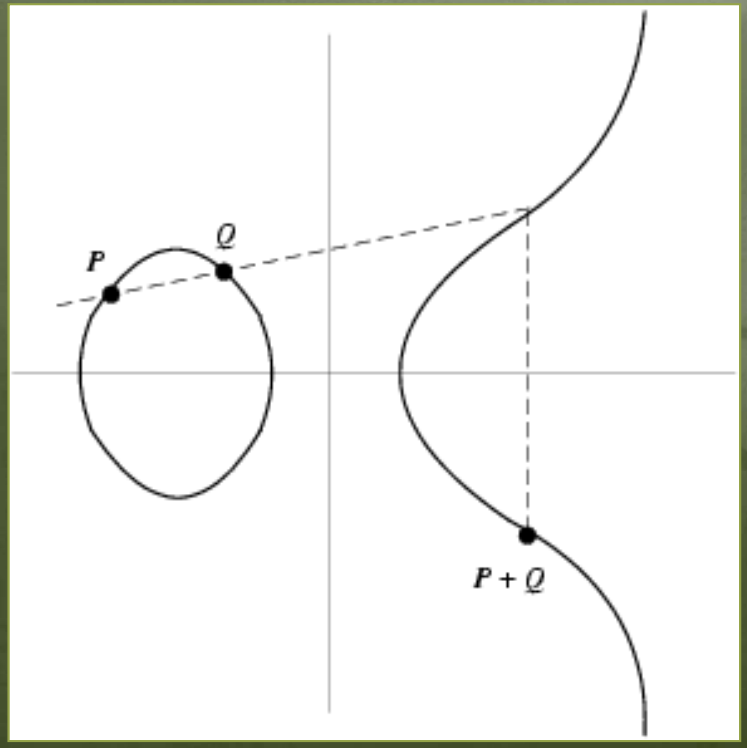
  Alice와 Bob은 같은 키(g^{ab} (mod p))를 공유하게 된다

타원곡선

- 타원곡선(Elliptic Curve)이란?
  $y^2=x^3+ax+b$ 꼴의 곡선

- mod p 타원곡선이란?
  $y^2 \equiv x^3+ax+b \pmod p$ 를 만족하는 점 (x, y)의 집합

- 타원곡선 암호
  - 타원곡선 위에서 기하학적으로 덧셈을 새롭게 정의할 수 있다
  - 새로운 연산에 관한 이산로그 문제를 이용하여 암호시스템을 만든다



타원곡선의 덧셈 P+Q

NSA

- National Security Agency (USA)
- 예산과 조직 비밀
  - CIA의 수십 배 예산 ??
  - 매년 수학 new Ph. D. 수십 명 채용 ??
- 수많은 영화의 소재……
- *알 카에다 ??*

압호의 대한독립 만세