고려대 학부생을 위한 암호 소개

이 은 정
Institute of Mathematical Sciences
Ewha Womans University

2013-12-10
Korea Univers
ity

암호(Cryptography)

- In Greek, *cryptos* means “secret, hidden”.
  - 정의(from Wiki) the practice and study of techniques for secure communication in the presence of third parties (called adversaries).
  - (from the book Applied Cryptography by Menezes) the study of mathematical techniques related to aspects of information security, such as confidentiality, data integrity and authentication

암호(Cryptography)

- In Greek, *cryptos* means “secret, hidden”.
  - 정의(from Wiki) the practice and study of techniques for se

암호 (Cryptography)
: 인터넷 통신 보호 서비스들을 위한 수학적 방법

  - (from the book Applied Cryptography by Menezes) the s tudy of mathematical techniques related to aspects of infor mation security, such as confidentiality, data integrity and a uthentication

암호의 사용 예


T money


KTV
공인인증서 저장하면 인터넷뱅킹 가능


DIPLOMATIC PASSPORT
REPUBLIC OF KOREA

Inbox
인증서
인증 경로
Web Slice Gallery
Important
Sent Mail
Drafts
Commercials
우리은행 | 개인고객
인터넷뱅킹
우리라이프
로그인정보관리
로그인
서명에 사용할 인증서 선택
우리은행
인증서 위치
하드 디스크
이동식 디스크
저장 토큰
보안 토큰
휴대폰
구분
사용자
만료일
발급자
인증서 보기
인증서 암호는 대소문자를 구분합니다.
인증서 찾기
인증서 암호
인증서 삭제
서명에 사용할 인증서를 선택하십시
확인
추천상품
서비스 활용 가이드
Hyang-Sook Lee
Spring 2013
ys
확인
TORRENT
BitTorrent
BitTorrent™

증권거래소 겨냥한 사이버 공격 증가세

안드로이드 앱, 필요할까?

페이스북 어플, 사용자 전화번호 무단 수집 문제 발생

○ 페이스북의 공식 안드로이드 앱이 사용자 동의 없이 단말기 전화번호를 무단 수집한 것으로 확인됨

– 미국의 보안회사 노턴(Norton)은 자사의 Norton Mobile Security 도구에 의해 페이스북 앱이 실행되는 것만으로도 단말기의 전화번호가 유출되는 것을 확인하였으며 이 같은 사실을 시만텍(Symantec)의 보안 블로그에 게시함

안드로이드 장비의 99%에 적용 가능한 취약점 발견

정상 앱을 원격조정용 악성 앱으로 둔갑시키는 APK Binder

○ 미국 보안업체 Symantec에 따르면, 정상 앱에 원격조정 기능을 추가시켜 "AndroRAT" 악성 앱으로 변환해주는 프로그램 "APK Binder"가 최근 37불, 한화 4만 2천원에 유통중인 것으로 알려짐

Cyber Sec

7/23	디지털 타임스	'똑똑해진' 자동차, 충격적 결함 있다 · 주요 자동차 업체들이 자동차에 통신기능을 도입하면서 개인정보가 유출되거나 해킹 당할 위험성이 높아짐 · 해킹과 관련한 자동차 업계의 보안 중요성은 더욱 커질 것으로 보이며, 이에 대비할 필요가 있음

〈 AndroRAT APK Binder 프로그램 판매 웹사이트 〉

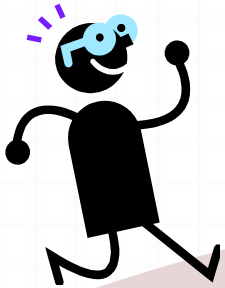
애플, Safa 않기로 결정

구글 글래스 숨겨진 WINK 기능 발견

○ 개인 정보보호의 문제는 스마트 시대(Always-connected tech age)의 가장 큰 문제로, 구글 글래스는 상대방의 동의 없이 촬영 가능한 문제가 있음

미국 주요 은행의 POS와 ATM을 목표로 하는 새로운 악성코드

사이버 공격으로부터의 보호

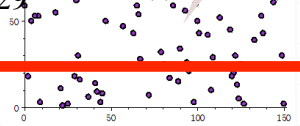


사용자의
안전한 사용

보안기술개발

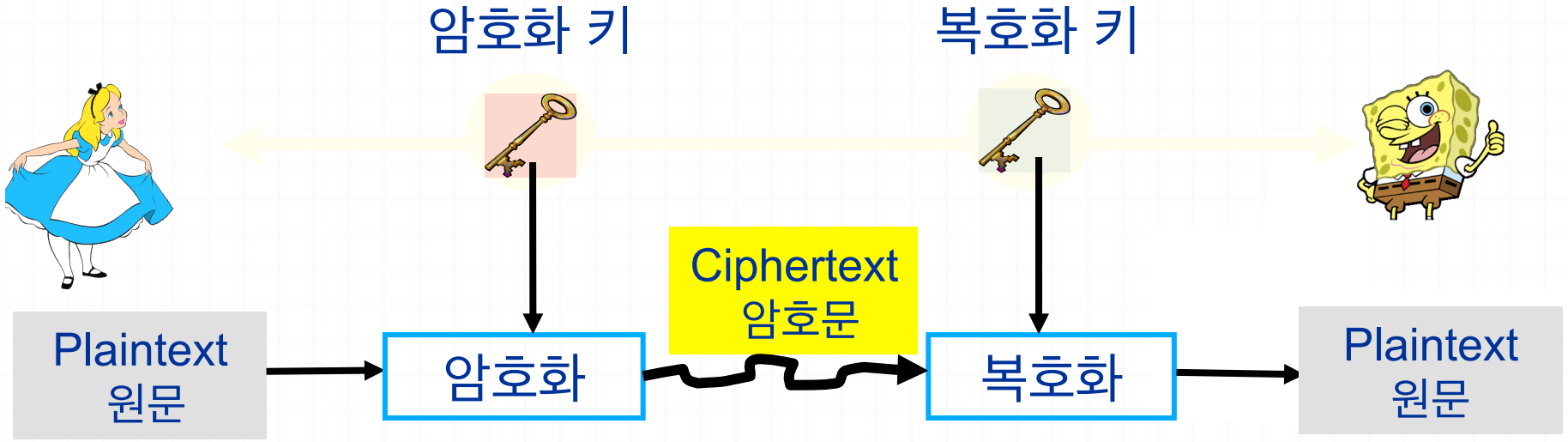
암호기술개발

7410010385009129
6168511028051948
8334363381235297
4797064073223842
2269665602
829



암호 시스템

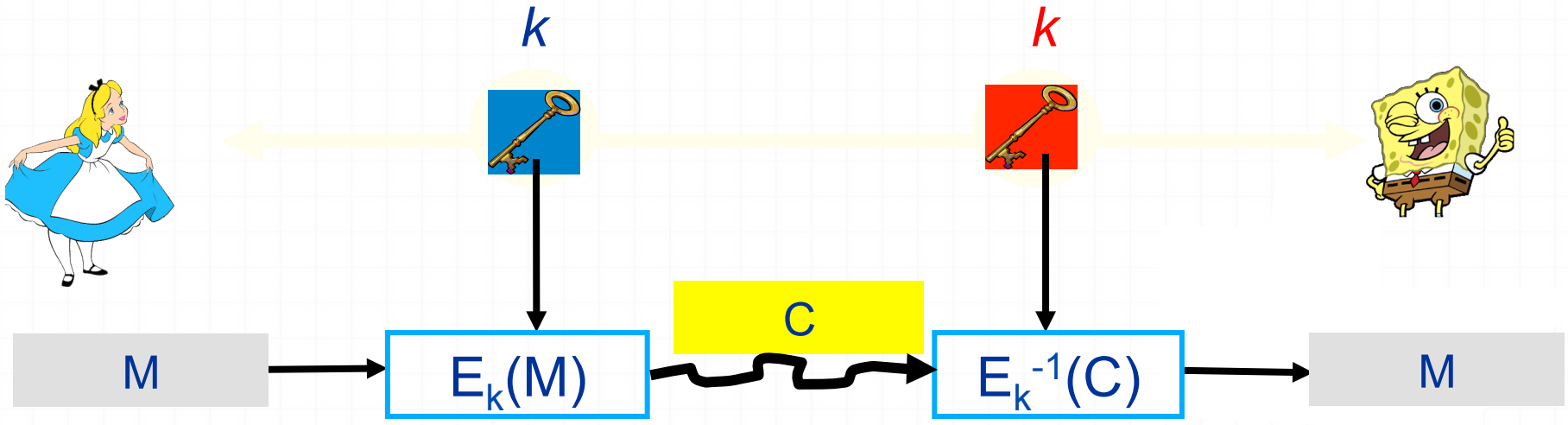
0 비밀통신(confidentiality)



다른 보안서비스들 : 전자서명, 키교환, 사용자 인증, 메시지 인증 등과 보안 요구조건에 따른 이들의 수많은 변형들

암호 시스템

0 비밀통신(secure communication): Encryption scheme



수학적 방법들

1. 쉬운 예
2. 약간 어려운 예
3. 어려운 예

쉬운? 어려운?

- 더하기
  - 20+13 을 26으로 나눈 나머지는?
  - 기호: $20+13 \bmod 26$
- 곱하기
  - 5^3 을 33로 나눈 나머지는?
  - 기호: $5^3 \bmod 33$
- 직선과 곡선
  - (-1,0)과 (0,1) 을 지나는 직선과 $y^2 = x^3+1$의 교점을 구하라

대수 구조 (group)

- 더하기
  - 20+13 을 26으로 나눈 나머지는?
  - 기호: 20+13 mod 26
  - Z : 정수 집합
  - Z/26Z :={0,1,2,…,25}
  - Z/26Z 는 $+_{26}$ (modulo 26 addition)에
    - - 닫혀있다. (closed)
    - - 항등원이 있다. (identity)
    - - 역수가 있다. (inverse)
- 곱하기
  - 5^3 을 33로 나눈 나머지는?
  - 기호: 5^3 mod 33
  - $(Z/33Z)^x$:={1,2,4,5,7,8,10,13,14,16,17,19,20,23,25,26,28,29,31,32}
  - $((Z/33Z)^x, x_{21}$ (modulo 33 mult.)) group이다.

$(Z/26Z, +_{26})$
군(group) 이다.

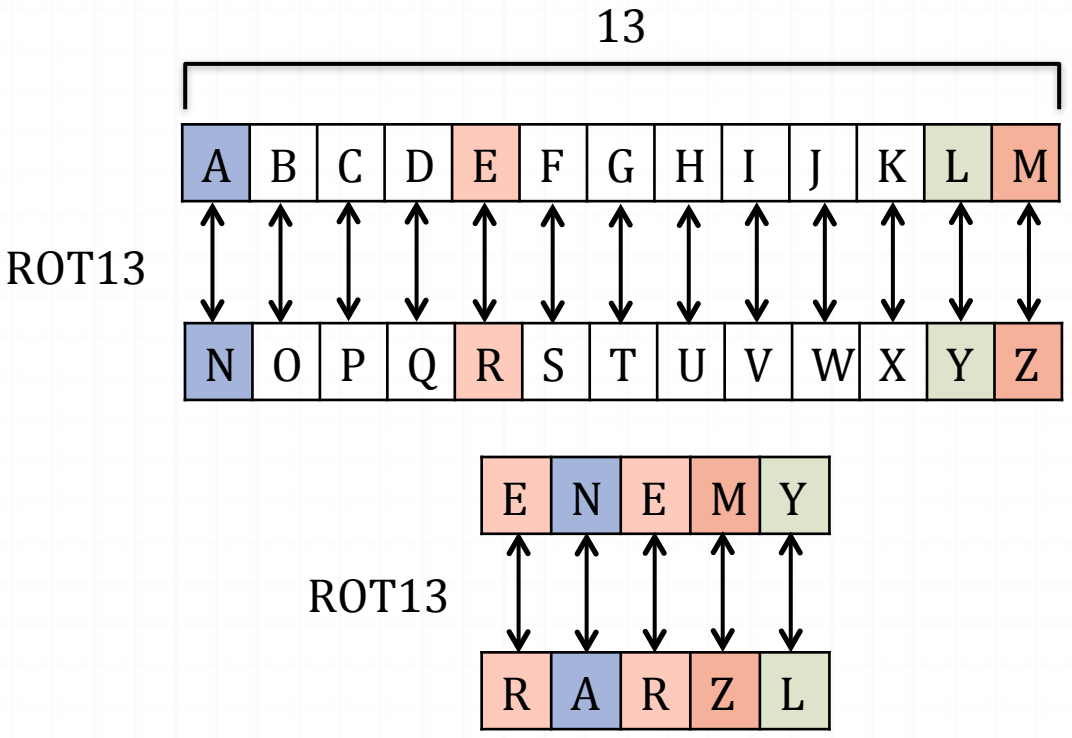
쉬운 예 : $(Z/26Z, +_{26})$

원문
e n e m y
f a l l i n g
b a c k
b r e a k
t h r o u g h
i m m i n e n t
l u c i u s

암호문
r a r z l s n
y y v a t 0 n
p x o e r n x
g u e b h t
u v z z w a
r a g y h p v
h f

쉬운 예 : $(Z/26Z, +_{26})$

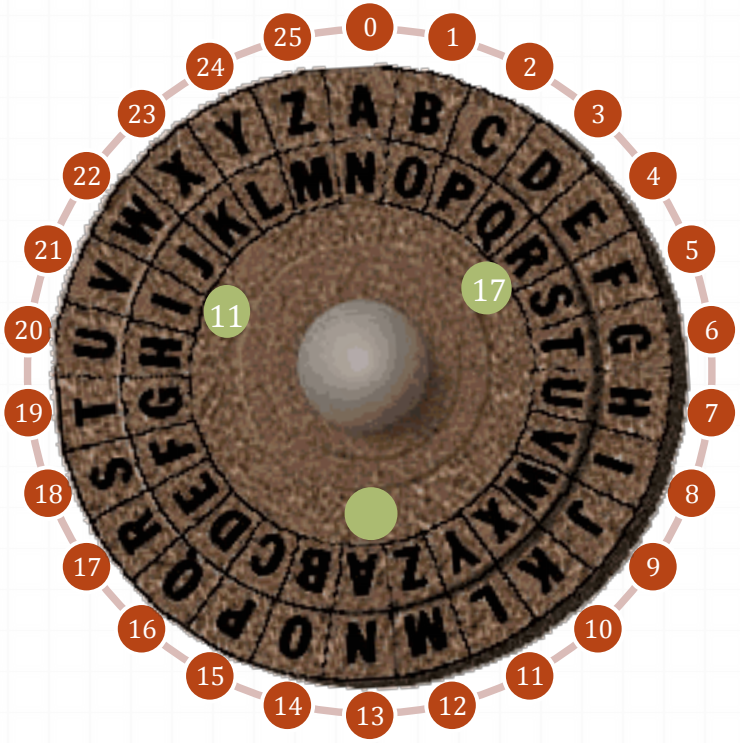
- Substitution cipher
  - 각 알파벳을 다른 알파벳으로 대치



쉬운 예 : $(Z/26Z, +_{26})$

원문:
e n e m y
…

원문(숫자로)
4 13 4 12 24
…

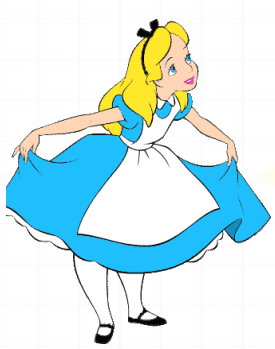


암호문:
r a r z l
…

암호문(숫자로)
17 0 17 25 11
…

암호화 : 4 + 13 mod 26= 17
13 + 13 mod 26= 0
…

쉬운 예 : $(Z/26Z, +_{26})$



k=13

k=13

$\{0,1,...,25\}^*$

4 13 4 12 24
5 0 11 11 8 1
3 6 1 0 2 10 1
17 4 0 10 19
7 17 14 20 6
7 8 12 12 8 1
3 3 13 19 11
20 2 8 20 18

M+k mod 26

17 0 17 25 1
1 18 13 24 24
21 0 19 14 13
15 23 14 4 17
13 23 6 20 4 1
7 19 20 21 25
25 22 0 17 0 6
24 7 15 21 7 5

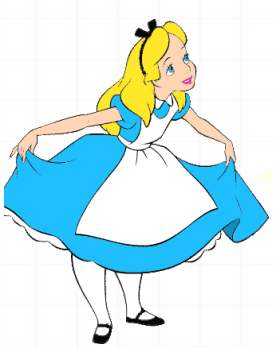
C-k mod 26

$\{0,1,...,25\}^*$

4 13 4 12 24
5 0 11 11 8 1
3 6 1 0 2 10 1
17 4 0 10 19
7 17 14 20 6
7 8 12 12 8 1
3 3 13 19 11
20 2 8 20 18

대칭키 암호 시스템

대칭키 암호 시스템*(symmetric key encryption)*의 예



k=13

k=13

=

$\{0,1,\ldots,25\}^*$

4 13 4 12 24
5 0 11 11 8 1
3 6 1 0 2 10 1
17 4 0 10 19
7 17 14 20 6
7 8 12 12 8 1
3 3 13 19 11
20 2 8 20 18

M+k mod 26

C-k mod 26

S K B V L F V

13 23 6 20 4 1
7 19 20 21 25
25 22 0 17 0 6
24 7 15 21 7 5

$\{0,1,\ldots,25\}^*$

4 13 4 12 24
5 0 11 11 8 1
3 6 1 0 2 10 1
17 4 0 10 19
7 17 14 20 6
7 8 12 12 8 1
3 3 13 19 11
20 2 8 20 18

점검포인트: 효율적인가? 즉, 암,복호화 쉬운가?
안전한가? 즉, k를 구하기 어려운가?

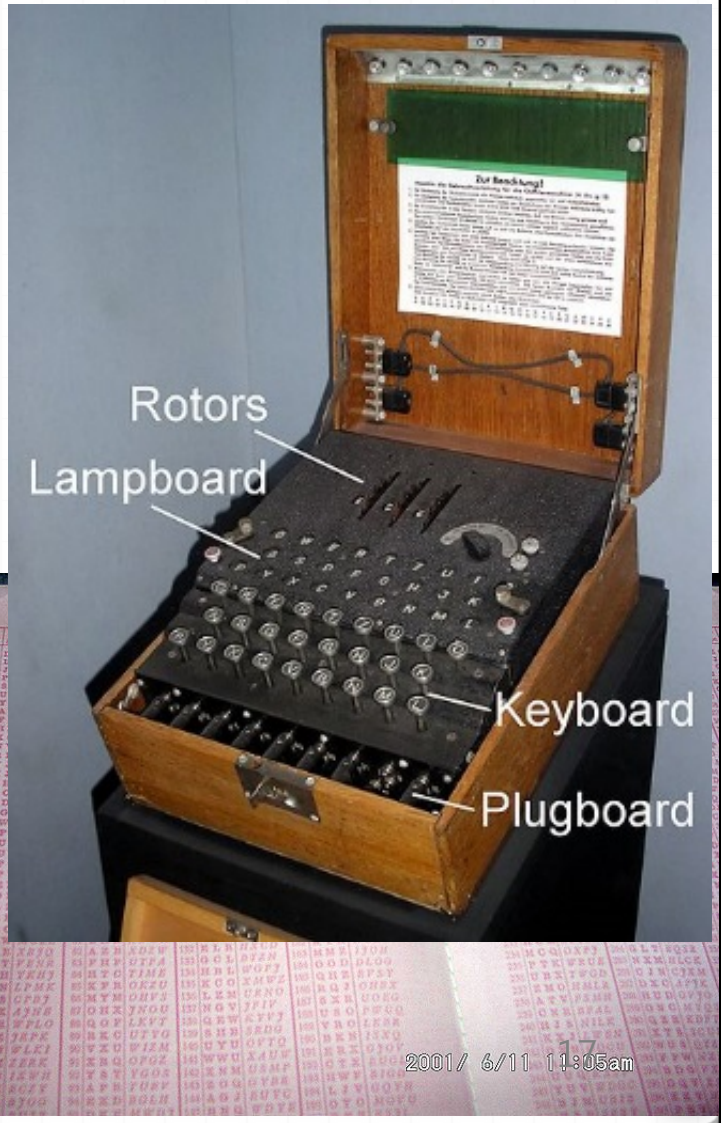
Substitution cipher

- Substitution cipher
  - 각 알파벳을 다른 알파벳으로 대치

A	B	C	D	E	F	G	H	I	J	K	L	M
N	E	C	P	T	U	A	B	W	Z	D	F	L

Rotation Table

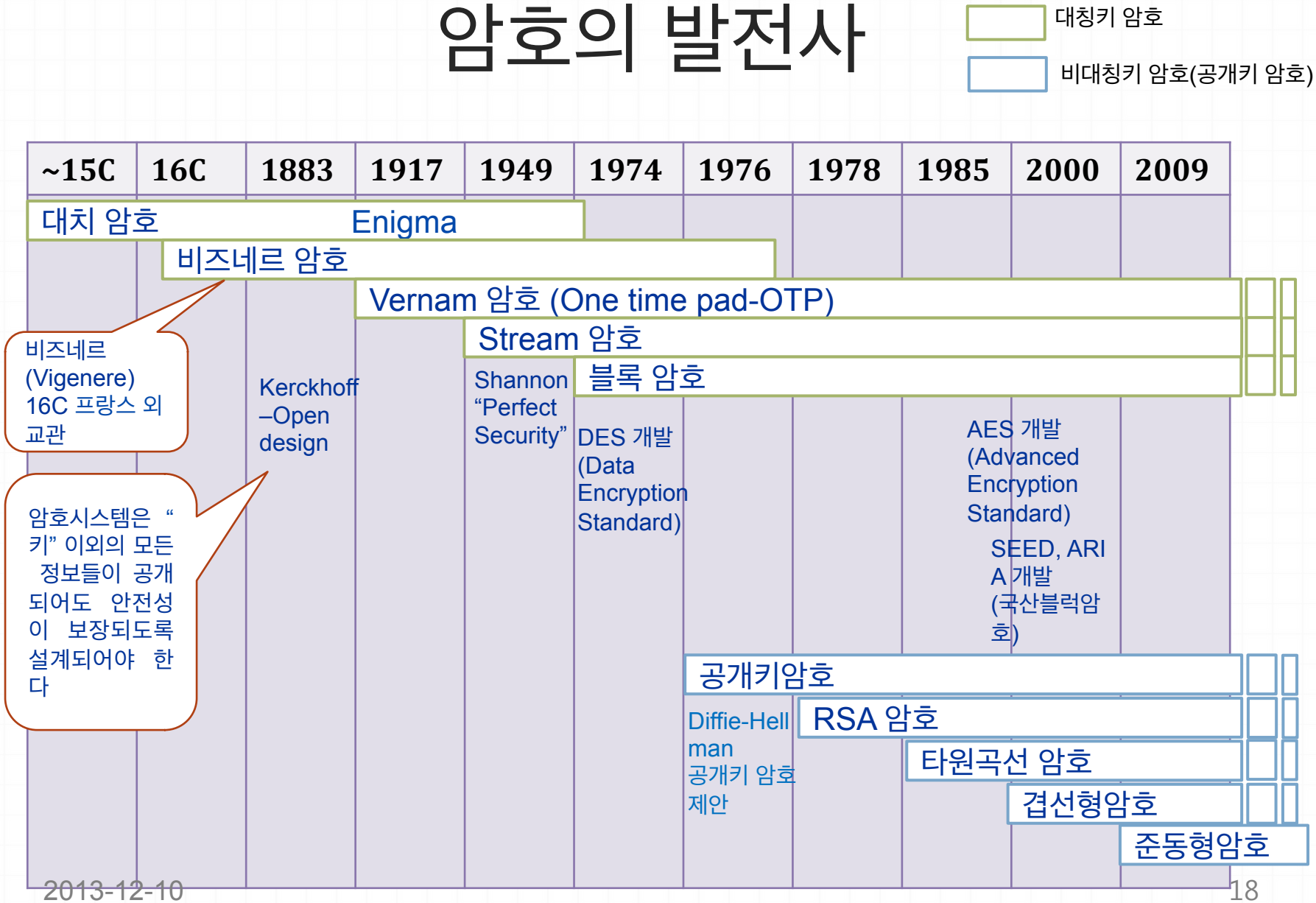
E	N	E	M	Y
T	G	T	L	Q



점검포인트: 효율적인가?
안전한가?

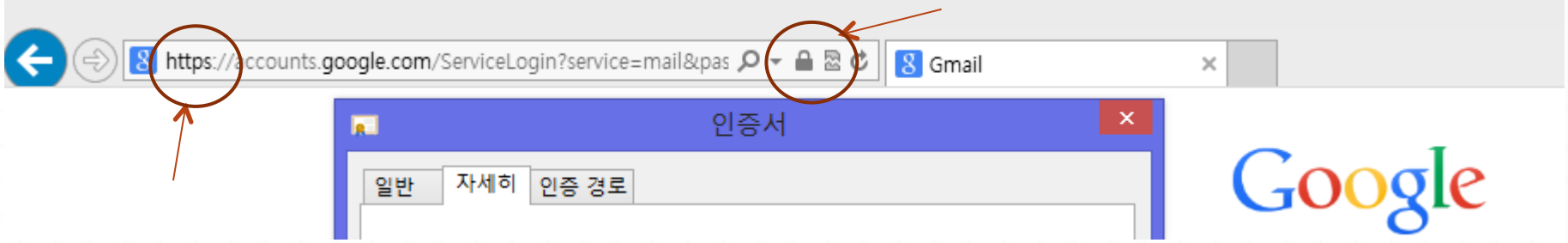
$26! \sim 2^{88}$

암호의 발전사


대칭키 암호
비대칭키 암호(공개키 암호)
~15C
16C
1883
1917
1949
1974
1976
1978
1985
2000
2009
대치 암호
Enigma
비즈네르 암호
Vernam 암호 (One time pad-OTP)
Stream 암호
블록 암호
비즈네르 (Vigenere) 16C 프랑스 외교관
Kerckhoff –Open design
Shannon "Perfect Security"
DES 개발 (Data Encryption Standard)
AES 개발 (Advanced Encryption Standard)
SEED, ARIA 개발 (국산블럭암호)
암호시스템은 "키" 이외의 모든 정보들이 공개되어도 안전성이 보장되도록 설계되어야 한다
공개키암호
Diffie-Hellman 공개키 암호 제안
RSA 암호
타원곡선 암호
겹선형암호
준동형암호

대칭키 암호 사용 예

- SSL(Secure Socket Layer)
  - 웹 표준 암호화 통신으로서 웹서버와 웹브라우저 사이에 모든 정보를 암호화 해주는 방식이다.
  - SSL 통신은 http가 아닌 https라는 통신채널을 사용하며, 모든 웹서버와 웹브라우저가 SSL을 지원한다.
  - '모든 정보를 암호화'
    - 전송되는 모든 정보를 대칭키 암호알고리듬으로 암호화 (AES, 3DES, ARCFOUR, Camellia, RC2, IDEA, SEED, NULL)



키 분배 및 키관리 문제

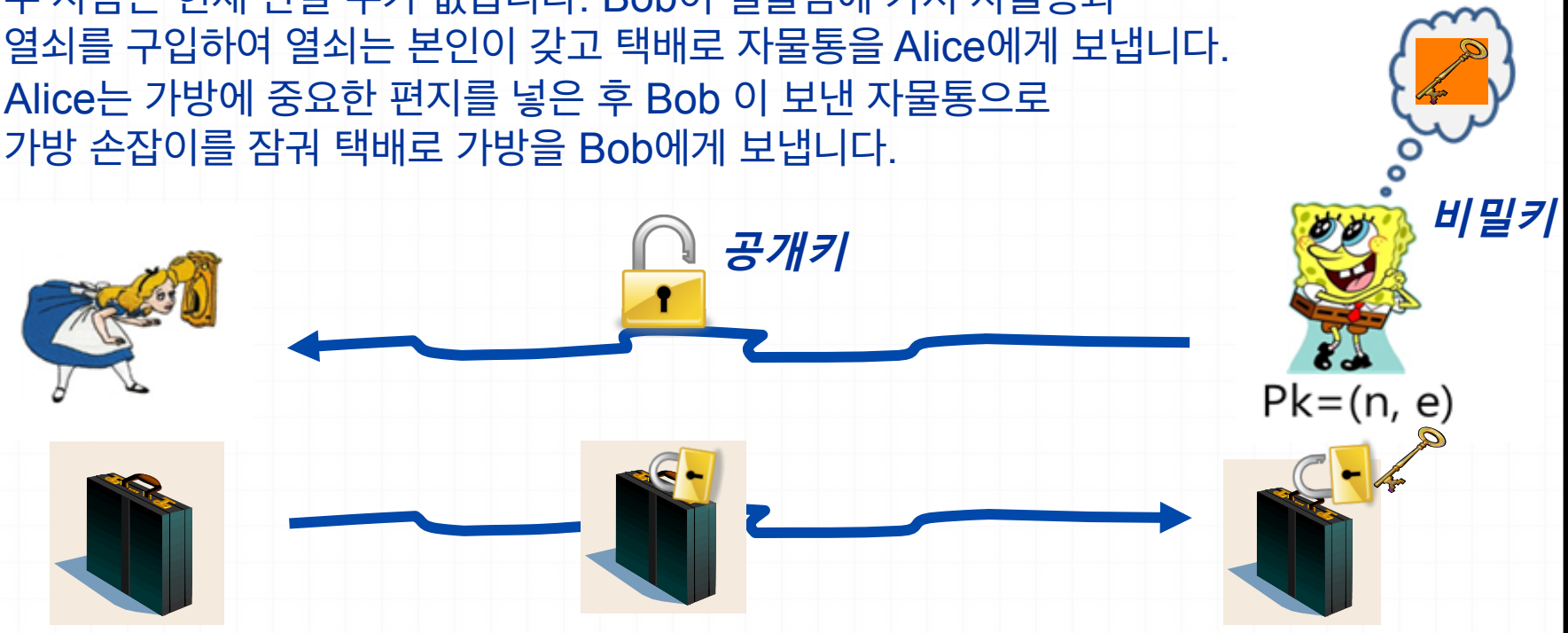
만나지 않고  **를 어떻게 분배 할까?**

N명의 사람들이 모두 서로 안전하게 대칭키암호를 사용하기 위해서는
- 각자 몇 개의 비밀키를 가지고 있어야 하는가?
- 필요한 비밀키의 총 개수는 적어도 몇 개인가?

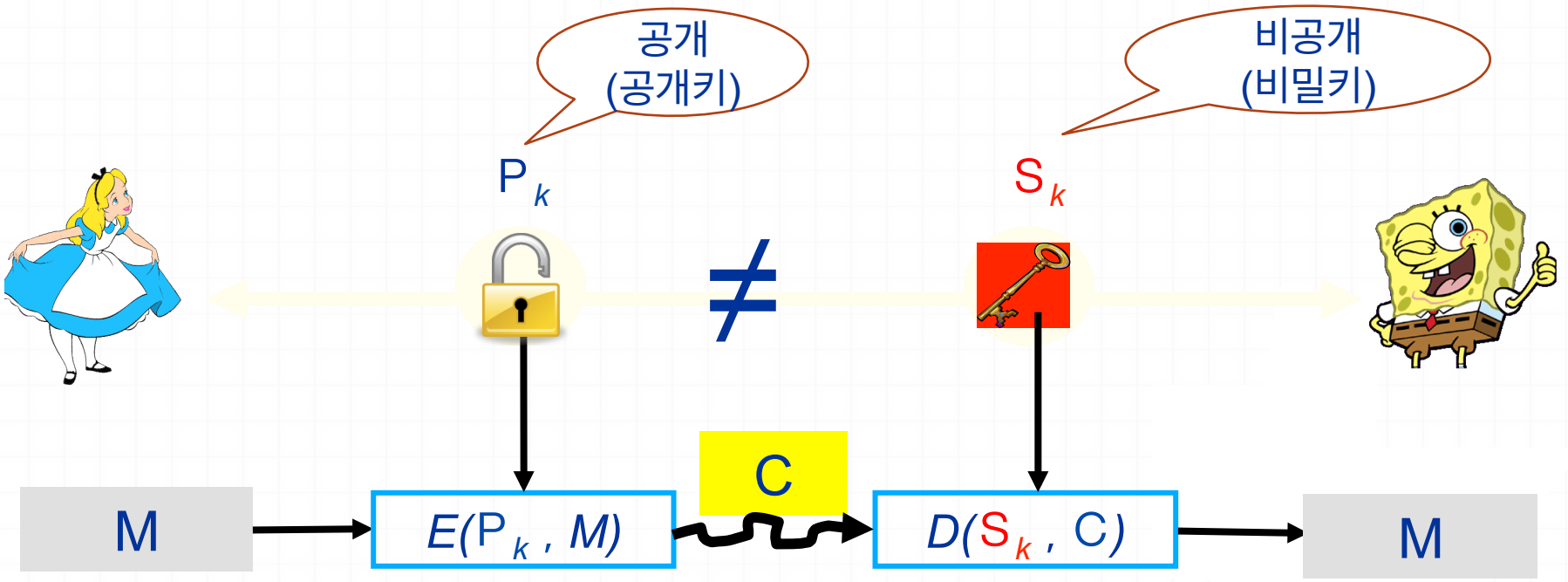
공개키 암호 시스템


Diffie-Hellman 1976

Alice 와 Bob은 원거리 통신을 하며 거래를 해오고 있습니다.
중요한 정보를Alice가 Bob에게 전달하려고 하는데,
두 사람은 현재 만날 수가 없습니다. Bob이 철물점에 가서 자물통과
열쇠를 구입하여 열쇠는 본인이 갖고 택배로 자물통을 Alice에게 보냅니다.
Alice는 가방에 중요한 편지를 넣은 후 Bob 이 보낸 자물통으로
가방 손잡이를 잠궈 택배로 가방을 Bob에게 보냅니다.

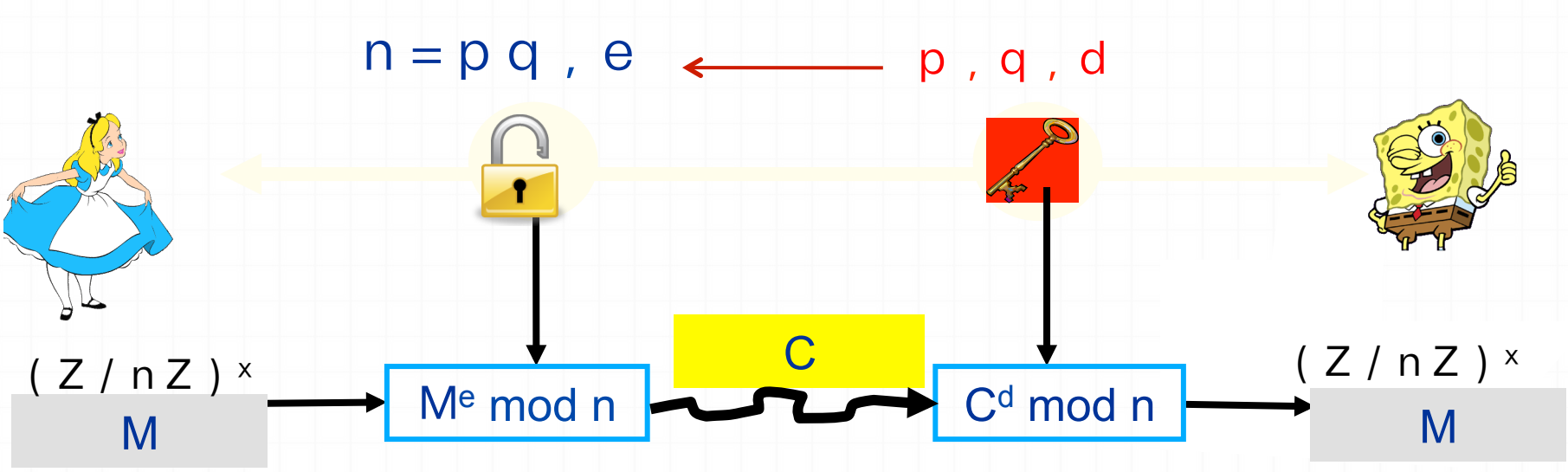


공개키 암호 시스템(1976)

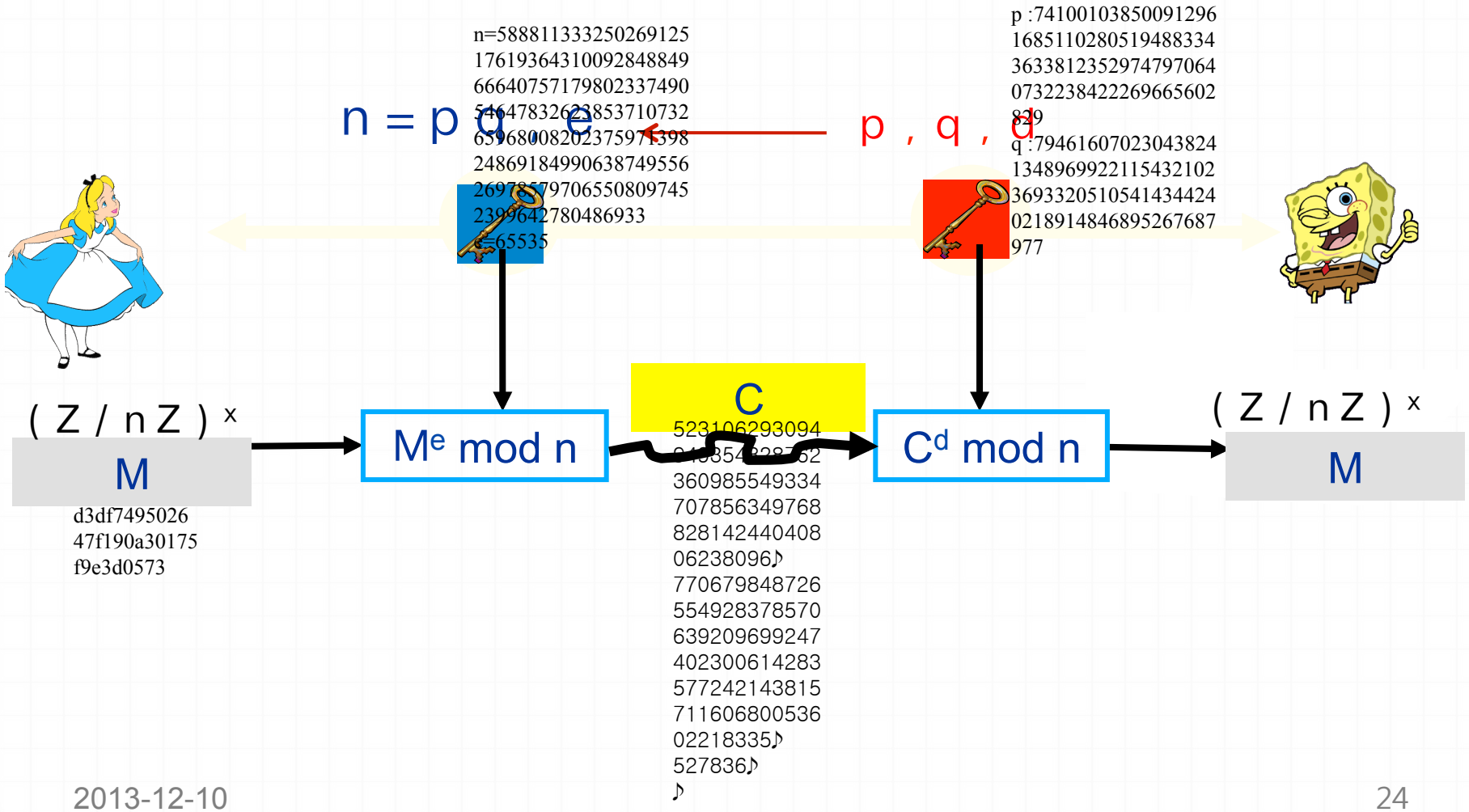


약간 어려운 예$((Z/nZ)^{\times}$,

RSA 1978



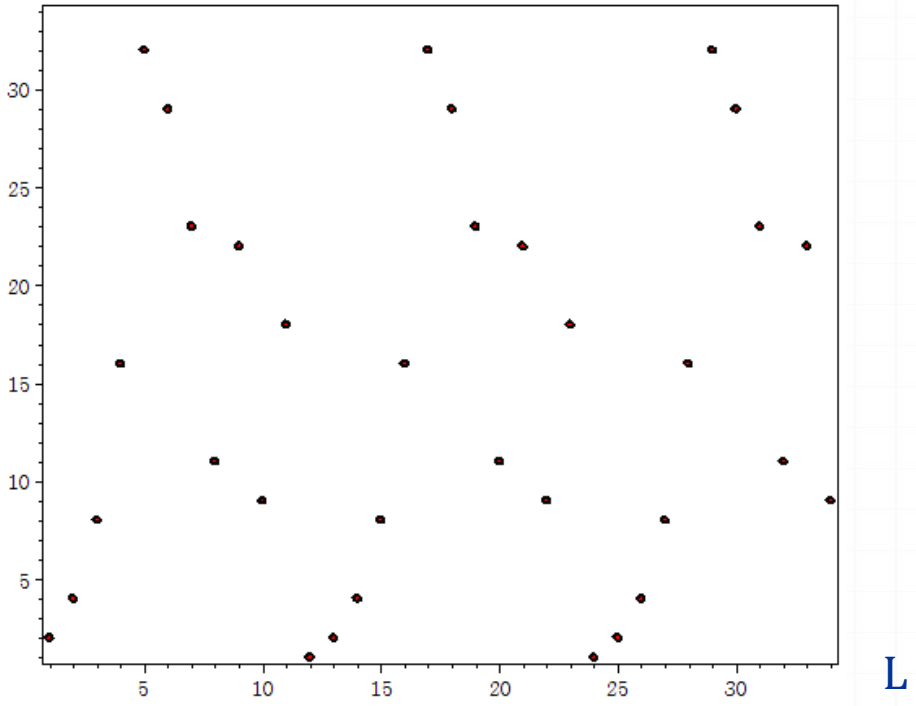
약간 어려운 예$((Z/nZ)^{\times}, \times_n)$



Fermat-Euler 정리(1736)

오른쪽 그래프:
n = 35
m ∈ {2,3,4,6,8,9,10,11,…,34}
에 대하여
$Y = m^L \bmod n$
$L \in \{2,3,4,5,6,7,\ldots,34\}$
X 축은 L 표시
Y 축은 $m^L \bmod n$ 표시

$m^L \bmod n,\ m \in \{2,3,4,6,8,9,10,11,\ldots,34\}$



Fermat-Euler 정리
$L = \varphi(n)$ 이면
모든 가능한 m 에 대해
$m^L \bmod n = 1$ 이다.

RSA correctness

암호화

$c = m^e \bmod n$

복호화

$m' = c^d \bmod n$

m' = m ? (복호화조건):

모든 평문 m에 대해서

$m' = c^d \bmod n$

$= m^{ed} \bmod n = m$

이어야 한다.

⇔ 즉,

$m^{ed-1} \bmod n = 1$

이 필요하다.

Fermat-Euler정리에 의해 $\varphi(n)$이 ed-1를 나누면 성립

RSA

n(=pq),e

p,q,d

e x d = 1
mod (p-1)(q-1)

복호화: $c^d \bmod n$

암호화
$C=M^e \bmod n$

원문 M
{ n보다 작고
n과 서로소인 정수 }

암호문 C
{ n보다 작고
n과 서로소인 정수 }

점검포인트: 효율적인가?
안전한가?

RSA 안전성

n(=pq),e

소인수분해문제

p,q,d

e x d = 1
mod (p-1)(q-1)

$c^d \bmod n$: 트랩도어(d)를 가지면 쉬운

암호화

$C=M^e \bmod n$

원문 M

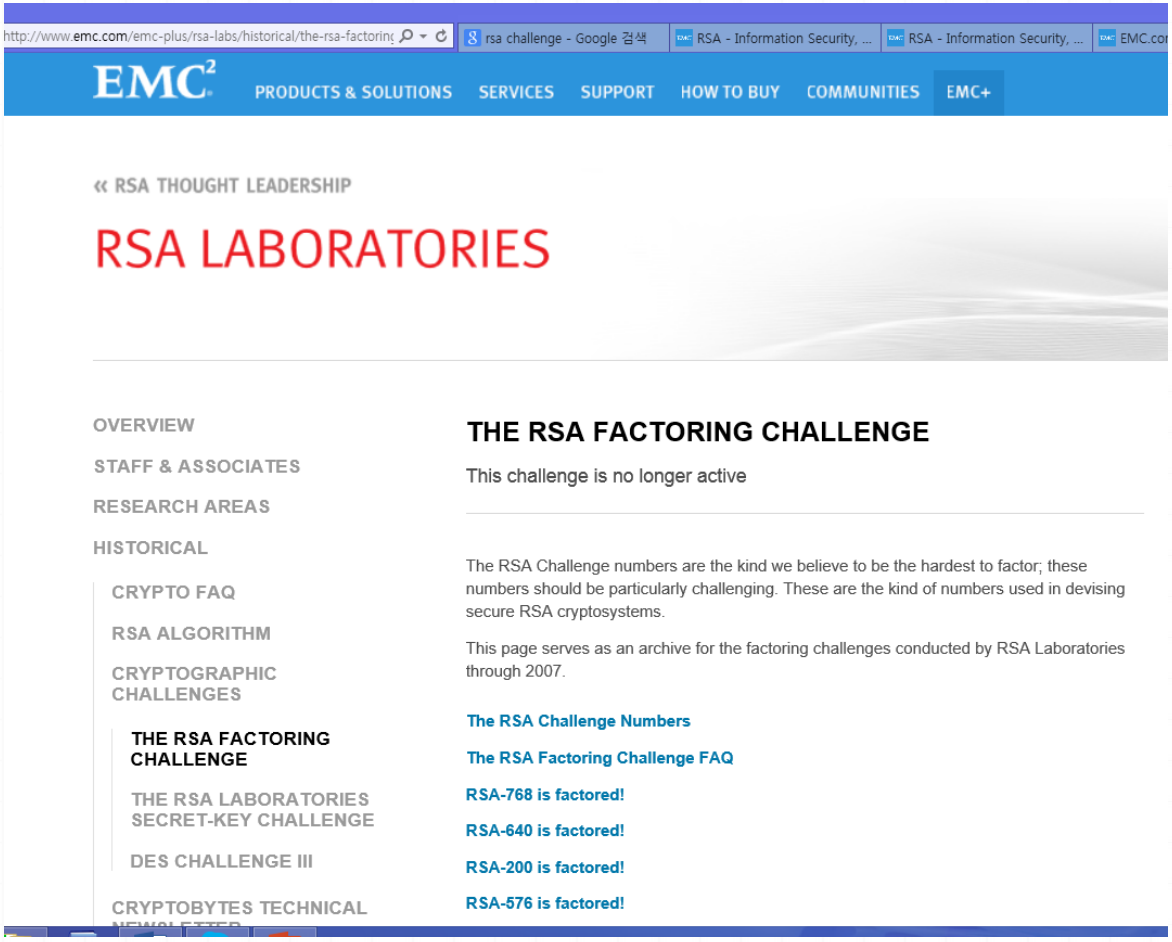
{ n보다 작고
n과 서로소인 정수 }

암호문 C

{ n보다 작고
n과 서로소인 정수 }

RSA problem
Input: C,e,n
Output:M

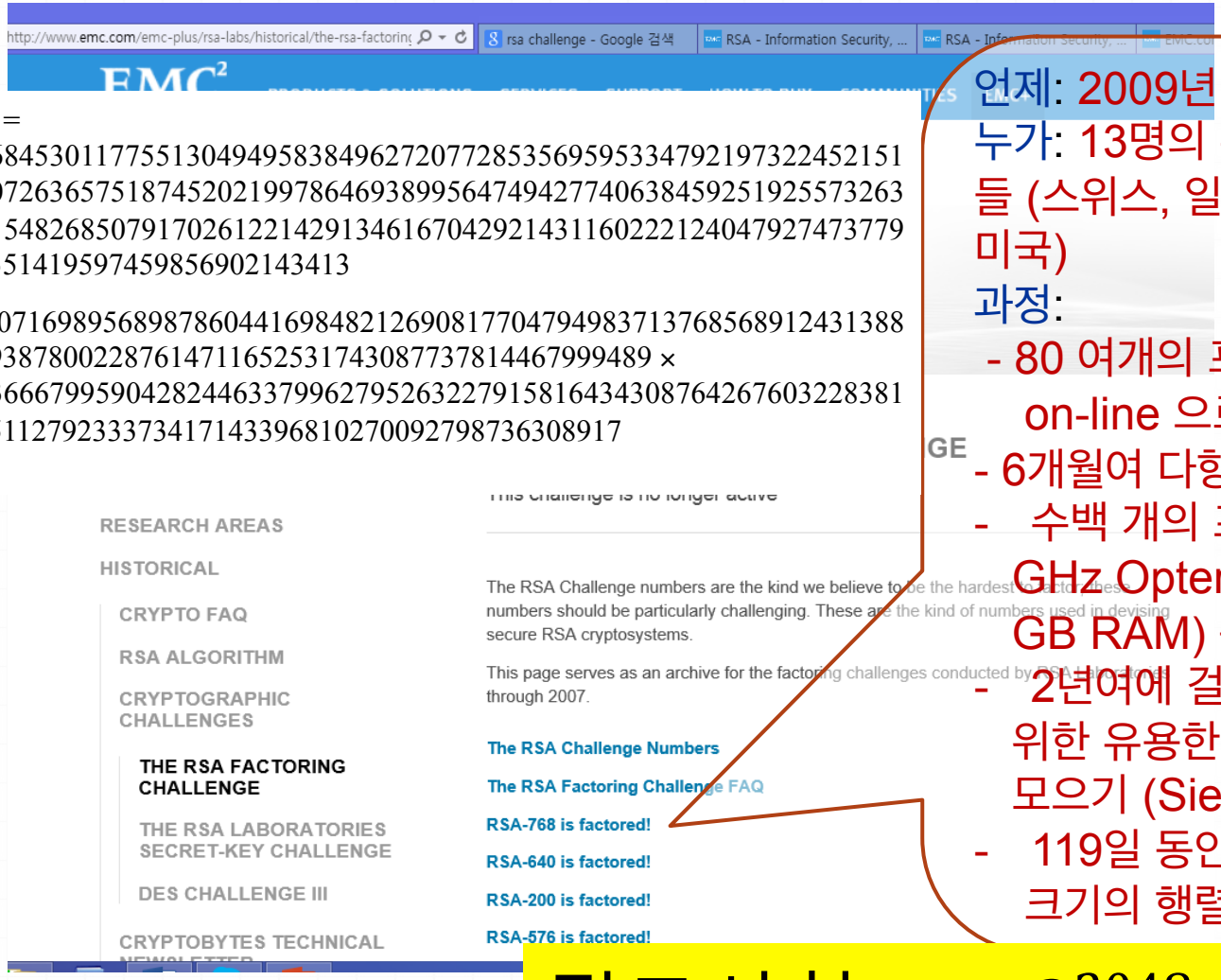
RSA challenge



Factorization

RSA-768 =
123018668453011775513049495838496272077285356959533479219732245215172640050726365751874520219978646938995647494277406384592519255732630345373154826850791702612214291346167042921431160222124047927473779408066535141959745985690214341 3

= 33478071698956898786044169848212690817704794983713768568912431388982883793878002287614711652531743087737814467999489 × 367460436667995904282446337996279526322791581643430876426760322838157396665112792333734171433968102700927987363089 17



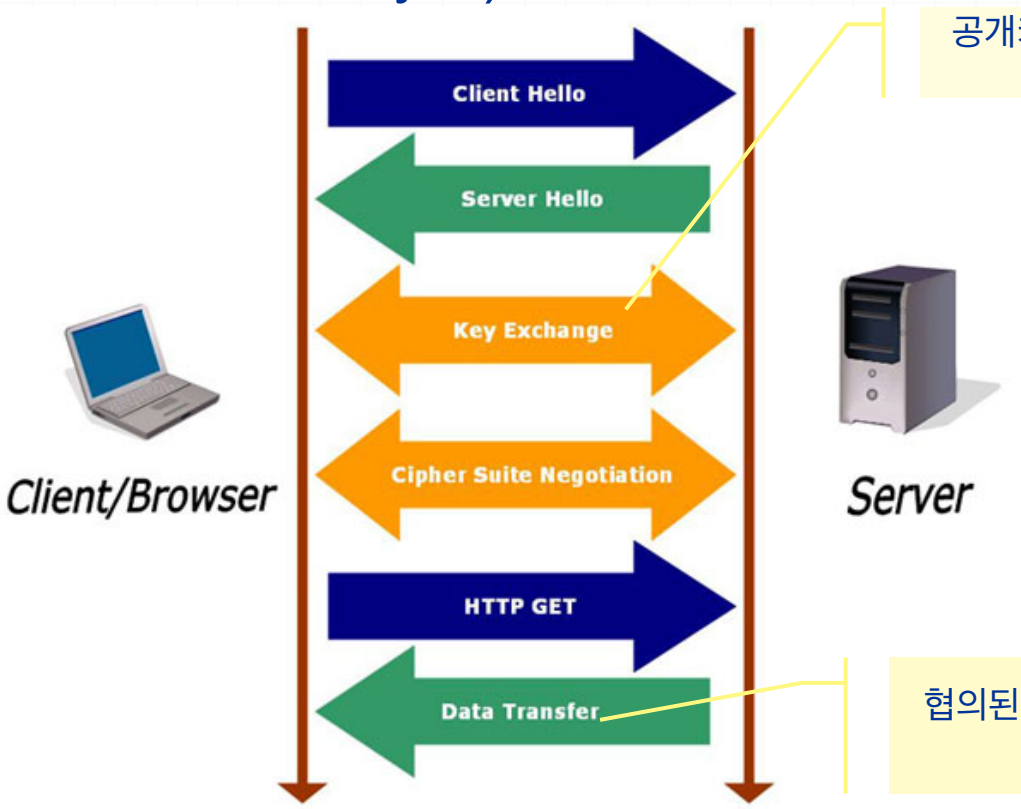
언제: 2009년 12월 12일 성공
누가: 13명의 수학자, 엔지니어들 (스위스, 일본, 독일, 프랑스, 미국)
과정:
- 80 여개의 프로세서를 on-line 으로 연결.
- 6개월여 다항식 고르기
- 수백 개의 프로세서(2.2 GHz Opteron core with 2 GB RAM) 동원.
- 2년여에 걸친 본 계산을 위한 유용한 데이터 모으기 (Sieving 과정)
- 119일 동안 208,065,007 크기의 행렬관련 계산

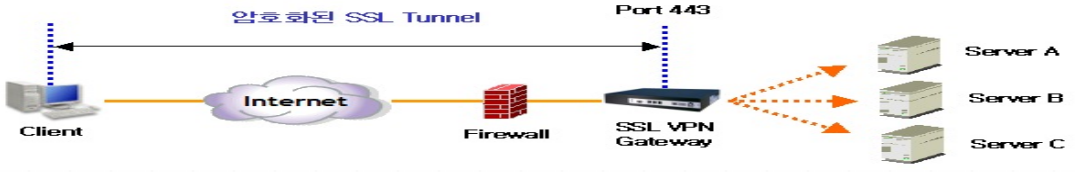
권고사항: $n > 2^{2048}$

At Crypto 2013 Rump session

RSA사용 (SSL)

0 SSL(Secure Socket Layer)

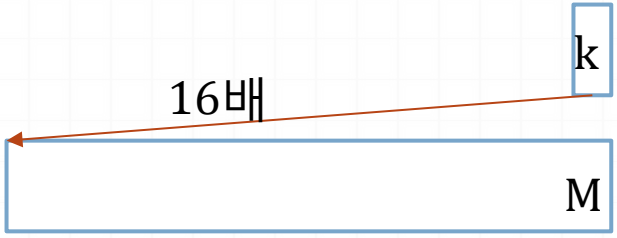




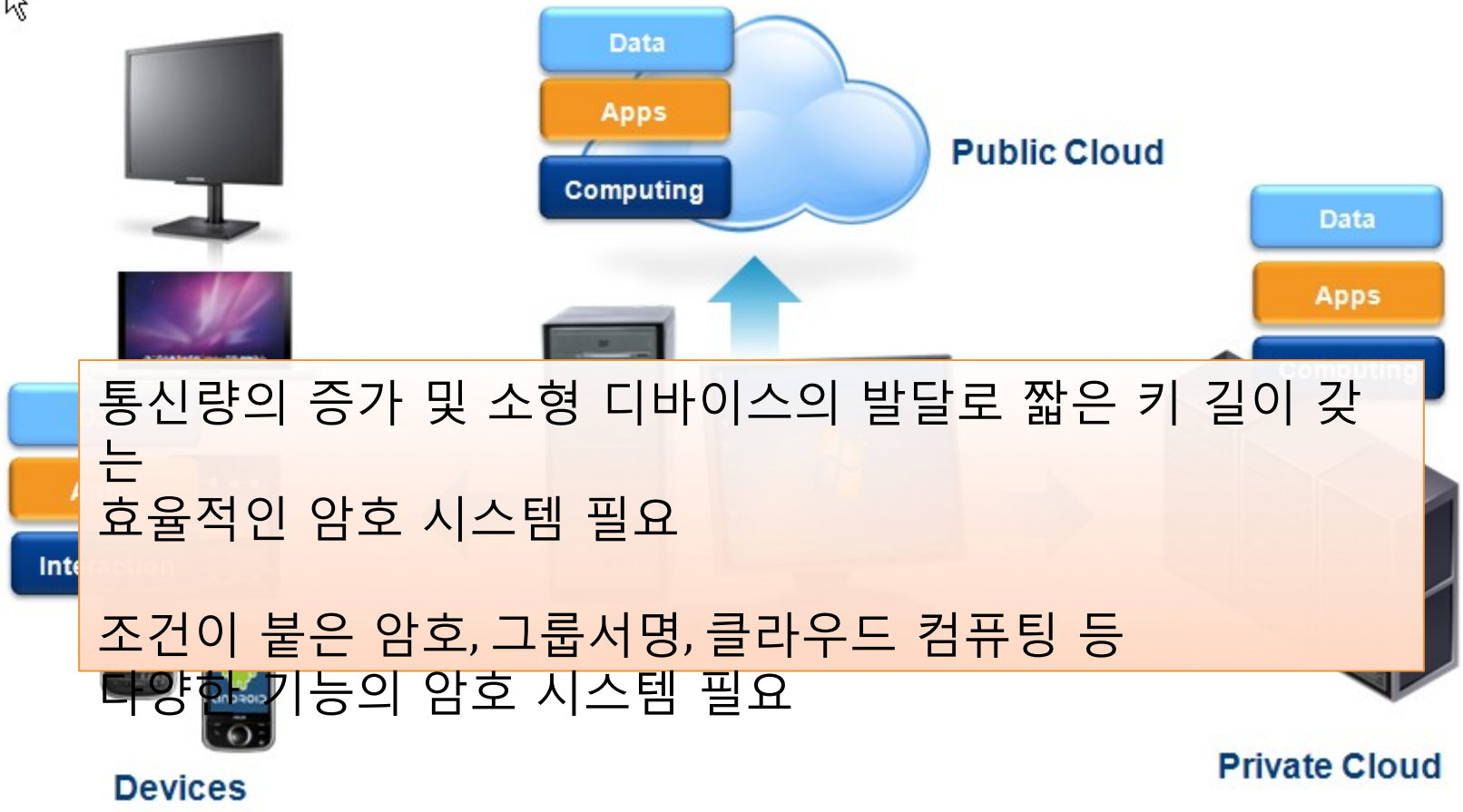
RSA 사용 RSA변형 – <RSA-OAEP>

Optimal assymetric encryption padding

- SSL 암호화
  - AES-128 사용
  - AES 키 k ~ 2^{128}
- SSL 키교환
  - RSA 사용 : n > 2^{2048}
  - C = k^e mod n
  - e=3,…,15 이면 ?
- Coppersmith (1996)
  - 두 암호문 c,c'이 m-m'=k (작은수) 의 관계에 있을 때 m을 알아내는 것은 쉽다.



현재,미래-통신환경의 변화



통신량의 증가 및 소형 디바이스의 발달로 짧은 키 길이 갖는
효율적인 암호 시스템 필요

조건이 붙은 암호, 그룹서명, 클라우드 컴퓨팅 등
다양한 기능의 암호 시스템 필요

어려운 예

ECC : Elliptic Curve Cryptosystem (타원곡선 암호)

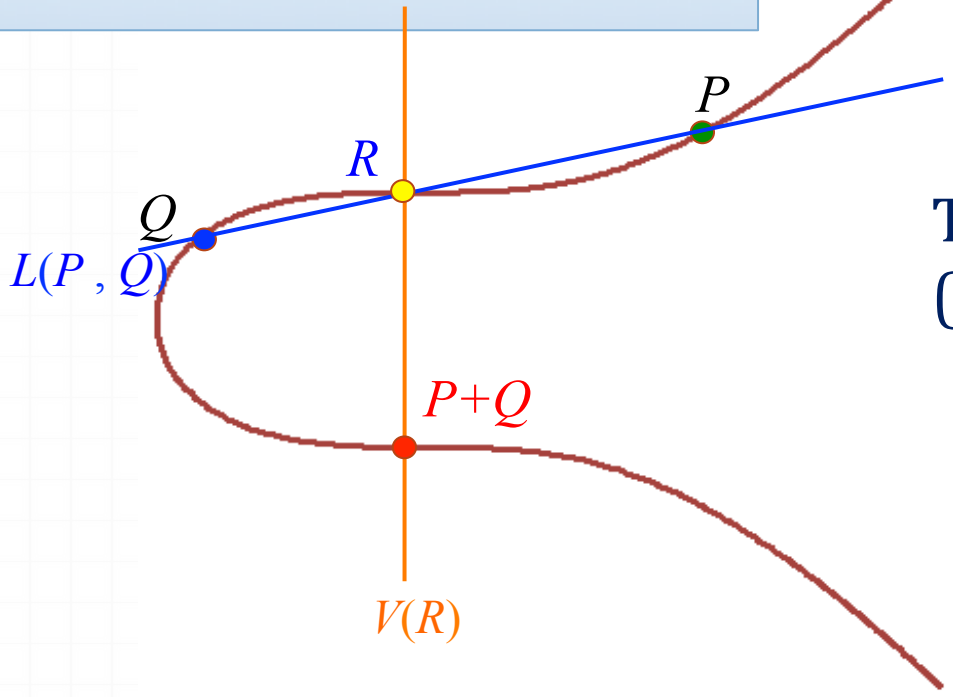
타원곡선 위의 점들의 더하기 연산 ***P+Q***

$L(P, Q) \cap E = \{P, Q, R\}$

$V(R) \cap E = \{R, \ \mathbf{P+Q}\ , O\}$

$E: Y^2 = X^3 + 3 \mod p$

p 는 큰소수



Theorem

$(E\ , +)$ 는 group

타원곡선 암호 (1985)

Y = xP
= P+P+...+
P

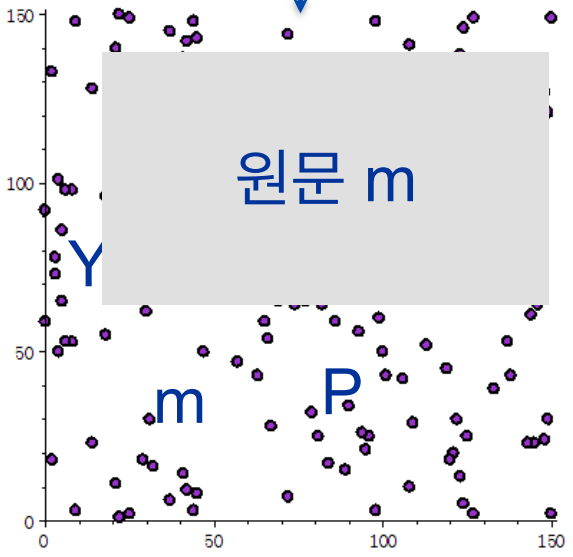
x
정수

이산대수 문제

RSA의 1/10 키 크기

m= - xU + V

트랩도어 x를 가지면 쉬운

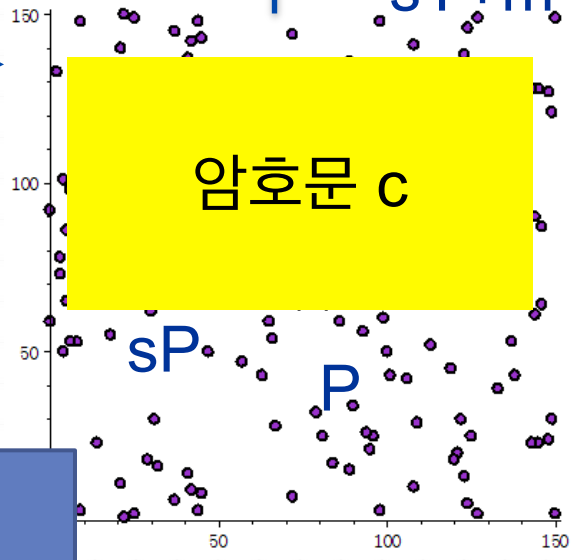


암호화

(U,V)=(sP, sY+m)

복호화

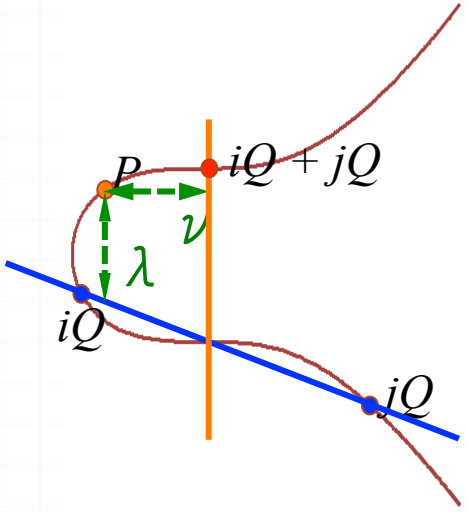
CDH 문제

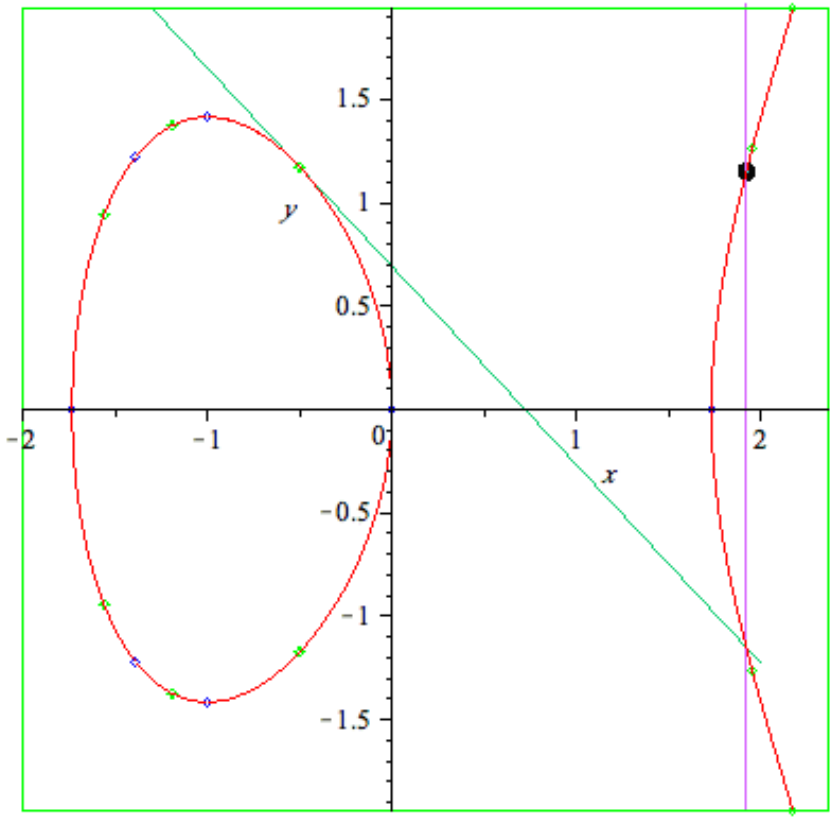


점검포인트: 효율적인가?
안전한가?

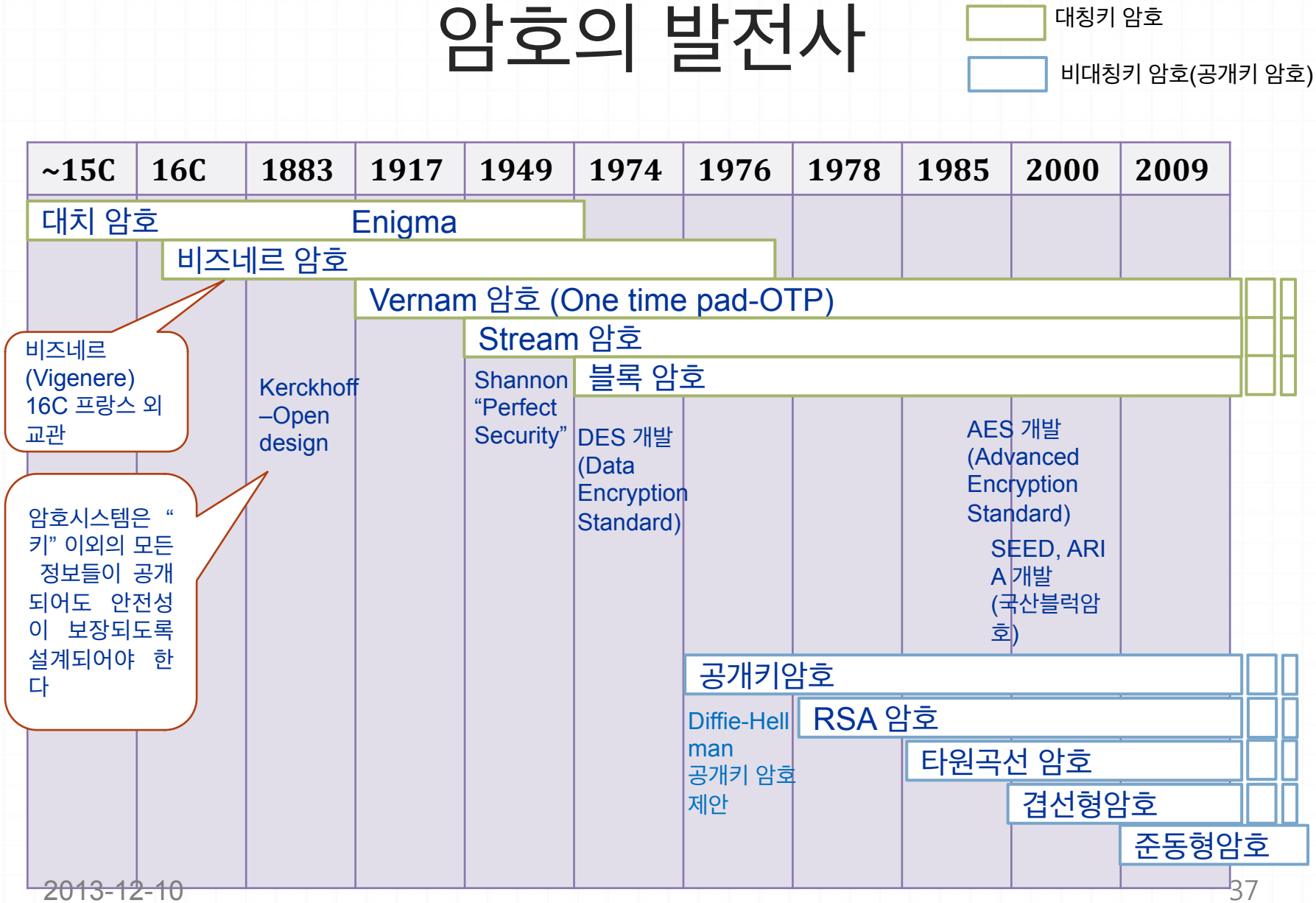
타원곡선-겹선형 함수 암호

- 삼자간 키교환 등 다양한 기능성 제공
- 계산 과정: λ / v 를 반복하여 계산

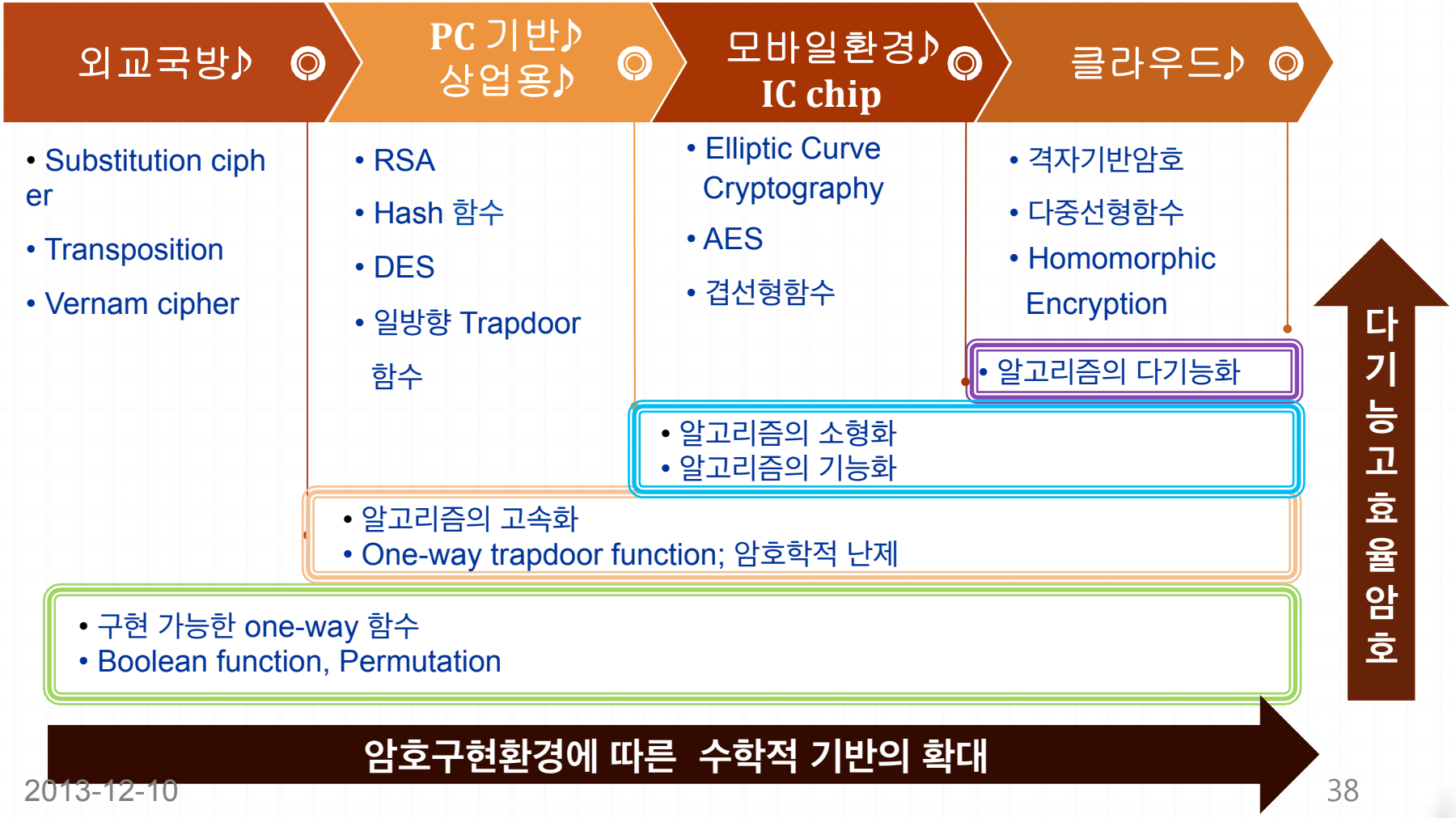




암호의 발전사


대칭키 암호
비대칭키 암호(공개키 암호)
~15C
16C
1883
1917
1949
1974
1976
1978
1985
2000
2009
대치 암호
Enigma
비즈네르 암호
Vernam 암호 (One time pad-OTP)
Stream 암호
블록 암호
비즈네르 (Vigenere) 16C 프랑스 외교관
Kerckhoff –Open design
Shannon "Perfect Security"
DES 개발 (Data Encryption Standard)
AES 개발 (Advanced Encryption Standard)
SEED, ARIA 개발 (국산블럭암호)
암호시스템은 "키" 이외의 모든 정보들이 공개되어도 안전성이 보장되도록 설계되어야 한다
공개키암호
Diffie-Hellman 공개키 암호 제안
RSA 암호
타원곡선 암호
겹선형암호
준동형암호

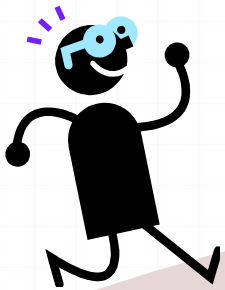
통신환경변화와 암호


외교국방♪
PC 기반♪ 상업용♪
모바일환경♪ IC chip
클라우드♪
• Substitution cipher
• Transposition
• Vernam cipher
• RSA
• Hash 함수
• DES
• 일방향 Trapdoor 함수
• Elliptic Curve Cryptography
• AES
• 겹선형함수
• 격자기반암호
• 다중선형함수
• Homomorphic Encryption
• 알고리즘의 다기능화
• 알고리즘의 소형화
• 알고리즘의 기능화
• 알고리즘의 고속화
• One-way trapdoor function; 암호학적 난제
• 구현 가능한 one-way 함수
• Boolean function, Permutation
다기능고효율암호
암호구현환경에 따른 수학적 기반의 확대

요약

- 대치 암호
  - 고대부터 1,2차 세계대전 군사용
  - 대칭키 암호의 기본
- 대칭키 암호(symmetric key encryption)
  - 3DES, AES(미국표준), SEED,ARIA(한국) 등
  - SSL 에서 데이터 암호 시 사용
  - 현재 최소 128 비트 권장
- RSA
  - Z/nZ 중 n과 서로소인 정수가 메시지, modulo 곱의 연산
  - 키의 안전성: 소인수분해 어려움
  - 메시지 안전성: RSA problem
  - 현재 2048비트 이상의 n 권장
  - 이외에도 안전한 사용을 위하여 여러가지 공격들 파악해야
- 안전성에 대한 이야기는 많이 못함

편리함과 안전함을 위하여



사용자의 안전한 사용

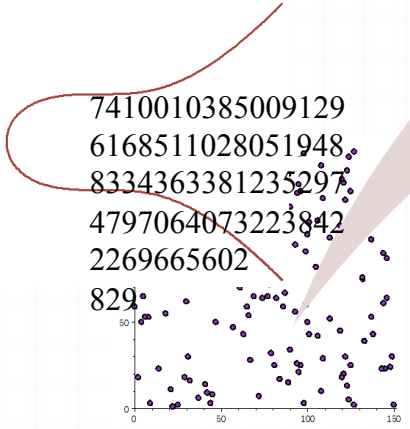
편리함만을 강조하지 않고 보안 지침들 잘 지키기

보안기술개발

암호스킴에 대한 이해를 바탕으로 보안 제품 개발

암호기술개발

수학적 프리미티브 연구를 통하여 다양한 기능의 안전한 암호 개발



Thank you