韓國通信情報保護學會誌
第1卷, 第1號, 1991. 4

Cryptosystems의 기법과 동향분석

이 경 석*

1. 서 론

최근 컴퓨터와 통신기술의 발전으로 언제 어디서나 각종 데이터를 주로 받을 수 있게 되고, 빠른 속도로 정보화 사회로 변화되고 있는 요즘 종래의 특수분야에서 뿐만 아니라 개인이나 상업적 측면에서의 정보보호가 무엇보다도 중요하고 시급한 문제로 대두되고 있어 암호학의 연구가 활발히 진행되고 있다.

정보의 보호는 컴퓨터(H/W, S/W) 혹은 전산요원 및 관련시설 등의 정보외적인 요소에 의한 위험도 많지만, 전송되는 정보자체의 무단 탈취변형 및 불법이용 등에서 발생되는 문제가 더욱 심각할 수 있다. 이에 대하여 본고에서는 2장에서 암호학의 정의와 그 배경을 살펴보고, 3장에서 컴퓨터를 이용하기 이전의 암호화 기법에 대하여, 그리고 4장에서는 현대적인 암호기법인 conventional cryptosystems과 public-key cryptosystems에 대하여 서술하였고, 5장에서는 미국과 일본을 비롯한 국내 암호학 동향 등을 분석하고, 마지막으로 암호학의 연구방향을 제시하였다.

* 정회원, 산업연구원

2. 암호학 개요

2.1 정의

데이터의 보호를 위하여 암호화되지 않은 상태의 원문(plaintext, original message)을 암호문(ciphertext, cryptogram)으로 만드는 것을 암호화과정(encryption, encipherment)이라 하고, 그 반대과정인 암호문을 원문으로 변화시키는 것을 복호화과정(decryption, decipherment)이라 한다. 여기서 사용되는 암호화 키(key, cryptographic key)와 함께 이들을 암호시스템(cryptographic system, cryptosystem)이라 부른다(그림 1).

이러한 cryptosystems은 일반적으로 다음의 세가지 요건을 충족시켜야 한다. 첫째는 키에 의하여 암호화 및 복호화가 효과적으로 이루어지고, 둘째는 이용하기에 용이하여야 하며, 마지막으로 암호알고리즘 자체보다는 암호키에 의한 보안이 이루어져야 한다.

그리고 광의의 암호학(cryptology)은 원문을 보호하기 위하여 암호알고리즘을 연구개발하는 암호학(cryptography)과 숨겨진 원문을 찾기 위하여 암호화 과정과 암호문을 연구하는 암호해독학(cry-

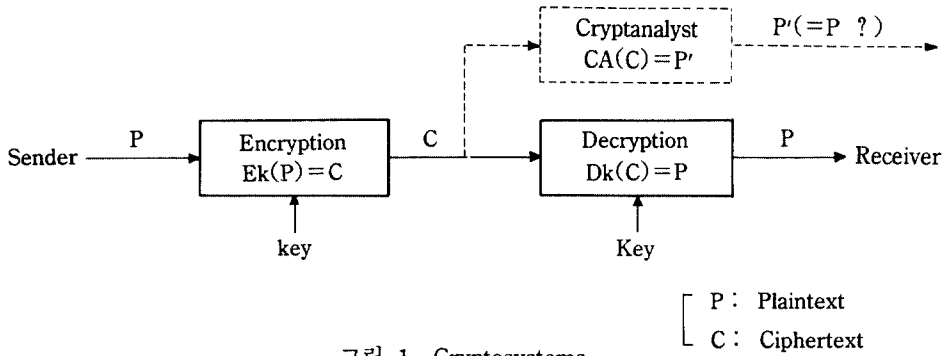

그림 1. Cryptosystems

ptanalysis)으로 구분된다.

암호학자(cryptographer)와 암호해독자(cryptanalyst) 모두 암호문에서 원문을 만들어 내지만 암호해독자는 부적법한 침입자 입장에서, 암호학자는 적법한 수신자의 입장에서 암호를 풀어낸다는 점이 다르다. 그러나 cryptography와 cryptanalysis의 영역은 명확히 구분하기 어려운 서로 연관된 분야로서 이러한 암호학(cryptology)의 연구는 전산학, 전자공학, 언어학, 통신공학, 수학(대수, 통계), … 등 여러 관련분야에서 이루어지고 있다.

2.2 배경

암호의 역사는 고대 중국이나 그리이스, 로마 아니 그 이전부터 인류의 역사와 함께 사용되어 왔다. 예를 들어, 로마시대의 시이저가 사용했던 시이저암호는 치환암호법(substitution cipher)이었으며, 그리이스의 스파르타가 "Scytale"을 이용하여 만든 전위암호법(transposition cipher) 등이 있다.

그리고 전신기(Morse, 1840) 및 라디오(Marconi, 1895) 등의 출현과 더불어 여러가지 근대적인 암호법이 많이 개발되었으나, 암호학의 가장 큰 발전계기가 된 것은 제 1 차 및 제 2 차 세계대전이었다. 그리고 컴퓨터와 통신기술의 발달이 현대 암호학 발전에 커다란 공헌을 하였다.

한편, L. S. Hill에 의하여 1929년 현대의 대수학적 암호학(algebraic cryptography)이 제안되었으며, 1949년 C. E. Shannon의 통신의 수학적 이론(The mathematical theory of communication)에 나오는 "Mixing transformation"은 IBM에서 만든 Lucifer 암호법에 응용되었다.

그리고 미 상무성 표준국(NBS : National Bureau of Standad)에 의해 암호화 표준기법으로 1977년 제정된 DES(Data Encryption Standard)는 Lucifer 암호에 근거를 둔 것이다. 또 다른 하나의 암호법은 1976년 Diffie와 Hellman에 의하여 고안된 Public-key 암호 알고리즘이다.

최근 정보교환에 있어서 안전문제가 중요한 문제로 대두되고 있어, 이젠 암호학이 군사나 외교적 측면뿐만 아니라 상업용으로 그 응용범위가 확대되어 가장 큰 분야로 정착되어가고 있다. 특히 컴퓨터 사용의 증가로 전산망을 이용한 정보교환이 활발히 이루어지고 있는 추세에 비추어, 암호학은 정보통신부문에서 중요한 요소중에 하나가 되었다.

3. 근대 암호 기법

오래전부터 비밀정보의 보호대책으로 암호화 기법을 이용하였는데, 이를 위하여는 미리 안전한 경로를 통하여 관련된 비밀사항이나 암호관련 키를 사람에 의하여 주고 받았으므로 자연히 정보전달에 여러 문제가 발생되었으며 시간이 오래 걸렸다.

이러한 전통적인 암호화 방법은 다음 과 같이 세가지로 구분할 수 있다.

3.1 전위암호법(Transposition cipher)

원문의 구성요소 자체를 변화시키지 않고 다음과 같이 그 요소들의 위치만 바꾸어 암호문을 만들기 때문에 "위치교환암호법"이라고도 한다.

1) 문자배열에 의한 방법

원문을 역순으로 배열하는 방법(i)과 두줄에 차례로 배열하여 일정한 숫자로 모으는 방법(ii) … 등이 있다.

(i) 원문 : TO ENCIPHER THE MESSAGE
암호문 : EGASS EMEHT REHPI CNEOT

(ii) 배열상태 : T E C P E T E E S G
O N I H R H M S A E
암호문 : TECPE TEESG ONIHR HMSAE

2) 키워드나 단순키에 의한 방법

정해진 매트릭스에 원문을 배열하되, 숫자를 단순키로 이용하는 방법(i)과 키워드의 알파벳 순서가 키로 사용되는 방법(ii) 등이 있다.

원문 : TO ENCIPHER THE MESSAGE

(i) 단순키(숫자) : 2 5 3 4 1

(ii) 키워드 : P L A I N
(키순서) (5 3 1 2 4)

배열 :

T	O	E	N	C
I	P	H	E	R
T	H	E	M	E
S	S	A	G	E

암호문 (i) : CREE TITS EHEA NEMG OPHS
(ii) : EHEA NEMG OPHS CREE TITS

3.2 치환암호법(Substitution cipher)

원문 구성요소의 순서는 변하지 않고 각 요소 자체가 다른 형태의 요소로 대치되는 방법으로 "대치암호법"이라고도 하며, 이 치환암호법은 다음과 같이 세가지로 나눌 수 있다.

1) Monoalphabetic substitution

원문과 암호문의 구성요소를 1 : 1로 대응시켜 치환하는 방법이다. 알파벳 순서를 n자리씩 차례로 이동시켜 만드는 Additive cipher(Caesar cipher), 특수 기호로 암호를 만드는 Pig-Pen cipher(Monoalphabetic with symbols) … 등이 있다. 이중에 Key를 첨가하고 알파벳을 재배치하여 만드는 "Keyword mixed sequence cipher"는 다음과 같다.

알파벳순서 : ABCDEFGHIJKLMNOPQRSTUVWXYZ
key : PLAXYTEN
재배열 : PLAXYTENBCDFGHIJKMOQRSUVWZ
원문 : KEYWORD
암호문 : DYWUIMX

2) Polyalphabetic substitution

암호화하기 위하여 다중 맵핑(multiple mapping) 방법을 사용하여 하나의 암호문자가 여러가지 원문문자로 전환이 가능한 방법이다. 여기에는 Vigenère square(표 1)를 이용한 Vigenère cipher,

표 1. Vigenère square

원문 ;	A B C D E …… S T U V W X Y Z
키 ; A	A B C D E …… S T U V W X Y Z
B	B C D E F …… T U V W X Y Z A
C	C D E F G …… U V W X Y Z A B
⋮	⋮ ⋮
X	X Y Z A B …… P Q R S T U V W
Y	Y Z A B C …… Q R S T U V W X
Z	Z A B C D …… R S T U V W X Y

알파벳 순서가 '표 1'의 역으로 전개되는 표를 이용한 Beaufort cipher … 등이 있다.

이런 방법에는 '표 1'를 이용하되 키의 반복을 피하기 위해 잡지나 소설 등의 특정 page, 특정부분에서 키의 시작을 지정하는 'Running-Key cipher"도 있는데, 여기서 그 키(running-key)가 "Newsweek"지 1991년 4월 1일, 17 page, 첫째 문장부터 시작된다면 그 결과는 다음과 같다.

원문 : C R Y P T O G R A P H Y A N D…
Running-key : W E S T W A N T S T O C O U N…
암호문 : Y V Q I P Q T K S I V A O H Q…

3) Polygraphic(Polygram) substitution

원문의 구성요소를 1 : 1로 치환하는 것이 아니라 n : n으로 치환하는 방법이다. polygram에서 n=2일 때 26×26=676개의 digraps를 이용한 Digraphic cipher, 메트릭스 key와 "modulo 26"을 이용한 Hill cipher,… 등이 있다. 이중에 알파벳(I=J)을 5×5 메트릭스안에 배열하고, 다음의 4가지 규칙에 의하여 원문 P1, P2를 암호문 C1, C2로 만드는 "Playfair cipher"는 다음과 같다.

- P1, P2가 사각형의 양쪽 코너에 있을 때, C1은 P2줄의 코너에서 C2는 P1줄의 코너에서 구한다.
- P1, P2가 같은 줄일 때는, C1, C2는 P1, P2 바로 오른쪽 문자를 취한다.
- P1, P2가 같은 행일 때는, C1, C2는 P1, P2 바로 밑에 문자를 취한다.
- P1, P2가 동일 문자인 경우는, P1과 P2사이에 "X"를 삽입하고, Pi가 홀수로 끝날 때는 "X"를 뒤에 첨가하여(*) 위의 원칙을 적용한다.

D	B	M	W	I
C	O	X	G	E
Q	Y	R	F	S
Z	A	K	T	P
L	U	H	N	V

원문 : HILL CIPHERX
LXL *
암호문 : MV CH DQ EV XV KR

3.3 합성암호법(Product cipher)

치환암호법(Substitution cipher)과 전위암호법(Transposition cipher)을 결합하여 암호의 강도를 높이기 위한 방법으로서 제1차 세계대전 당시 독일군이 사용하던 ADFGVX Product cipher … 등이 여기에 속한다.

이 ADFGVX cipher는 6×6 매트릭스에 알파벳 26자와 숫자(0, 1, 2, 3, …, 9)를 배열하고(표 2), 원문을 ADFGVX table(6×6)에 의하여 치환방법으로 1차 암호문을 만든 다음, 키(DEUTSCH)의 알파벳 순서에 의하여 전위방법으로 최종 암호문을 다음과 같이 만들어 낸다.

표 2. ADFGVX table

(i)

	A	D	F	G	V	X
A	K	Z	W	R	1	F
D	9	B	6	C	L	5
F	Q	7	J	P	G	X
G	E	V	Y	3	A	N
V	8	O	D	H	0	2
X	U	4	I	S	T	M

원문 : P R O D U C T C I P H E R S

(ii) 1차 암호문 : FG AG VD VF XA DG XV
DG XF FG VG GA AG XG

(iii) 키 : D E U T S C H
(키순서) 2 3 7 6 5 1 4

F	G	A	G	V	D	V
F	X	A	D	G	X	V
D	G	X	F	F	G	V
G	G	A	A	G	X	G

(iv) 최종 암호문 : DXGX FFDG GXGG VVVG
VGFG GDFA AAXA

4. 현대 암호 기법

전신기와 라디오의 출현 및 두 차례의 세계대전은 암호기법이 원시적인 상태에서 벗어나 많은 발전을 이룩하는 계기가 되었으나, 최근 사용하고 있는 알고리즘은 1970년대부터 시작되었다고 볼 수 있다. 즉 컴퓨터와 고속통신망 이용에 근대적인 암호기법들은 부적합하여 컴퓨터를 이용한 새롭고 난이도가 높은 알고리즘들이 연구개발되어 사용되고 있다.

현대의 암호기법은 주로 계산의 난이도를 응용한 것들이며, 데이터의 불법 탈취를 방지하는 "비밀유지"와 데이터의 무단변형이 이루어지지 못하게 하는 "정확성 확인"이라는 두가지 측면에서의 기본 목적이 있다.

컴퓨터 통신에서의 암호화 과정과 키관리에 관한 현대적인 암호 알고리즘에는 비밀키(secret-key, single-key, conventional)시스템과 공개키(public-key, two-key) 시스템 등이 있다. 이들 시스템의 주요 차이점은 KEY의 사용에 있는데, 비밀키 시스템은 암호화나 복호화에 오직 하나의 키를 사용하여 symmetric 알고리즘이라 하며, 공개키 시스템은 공개된 암호화 키와 복호화를 위한 비밀키가 서로 다르기 때문에 asymmetric 알고리즘이라고 한다.

이러한 종류의 현대 암호 알고리즘은 1976년 Diffie와 Hellman에 의해 제안된 공개키 시스템과, 1977년 미국 정부에 의해 표준으로 지정된 DES와 같은 비밀키 시스템 등이 있다.

4.1 비밀 키(secret-key) 시스템

암호화, 복호화에 동일한 비밀키를 이용하며 고대의 암호기법과 구별하기 위해 single-key 시스템이라고도 한다. 그러므로 비밀키 시스템에서는 송수신자가 미리 안전한 경로를 통해 키를 공유한 후 그 키에 의하여 정보교환이 시작된다.

비밀키 알고리즘에서 암호화, 복호화에 쓰이는 비밀키 k와 역함수 관계인 function F, ($Fk \cdot Fk^{-1} = 1$),가 있을 때, 원문을 P, 암호문을 C라고 한다면; 암호화 과정은 $Fk(P) = C$이고, 복호화 과정은 $Fk^{-1}(C) = Fk^{-1}(Fk(P)) = P$가 된다.

1) DES(Data Encryption Standard)

미국 상무성 표준국(NBS: National Bureau Standards)에서 정부표준 암호시스템으로 IBM에서 만든 DES(Data Encryption Standard)를 1977년 확정하였다. 그리고 그후 이 알고리즘을 ANSI (American National Standards Institute)에서 1980년에, ISO(International Standards Organization)에서 1983년에 각각 표준안으로 채택되었다.

DES는 IBM의 Tuchman 등이 만든 Lucifer cipher를 기초로 한 block product cipher이며, 64 bits의 원문 data가 56bits(48bits)의 16가지 키에 의하여 16회의 암호계산 단계를 거쳐 64bits의 암호문이 작성되는 방법이다.

- 알고리즘
  - 64bits의 block data가 초기 permutation(Initial Permutation ; IP)을 거쳐 좌우 32bits씩 나누어져 16회의 암호계산을 마친 후 64bits로 모아진다.
  - 매회마다 다른 64bits의 키가 48bits로 되어 사용되며, 16단계를 거친 64bits에 최종 permutation(Inverse Initial Permutation ; IP^{-1}) 과정이 수행되면 64bits의 암호문이 작성된다

- 암호화 과정
  - 첫단계를 제외한 모든 단계에서 바로 전단계의 결과인 64bits를 각 단계마다 서로 다른 16개의

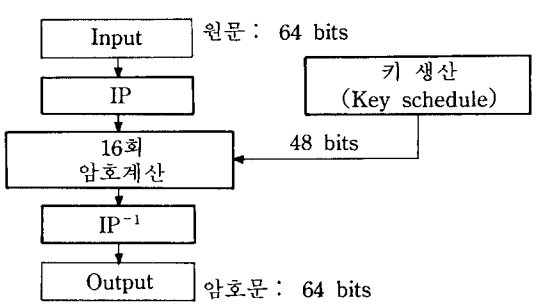

그림 2. DES 알고리즘

키(64bits→48bits)에 적용시킨다.

◦ 64bits의 원문 data를 초기 permutation(IP) 후에 32bits씩 나누어 좌우(L, R)에 배정한다.

◦ 32bits의 L과 Cipher function f(R, K) 결과의 modulo 2 계산에 의해 32bits가 다음 단계의 R′(= L ⊕ f(R, K))에 저장한다.

◦ R의 32bits는 변동없이 다음 단계의 L′에 저장되며, 이런 식으로 16단계를 거쳐 나온 결과가 최종 permutation 과정(IP^{-1})이 끝나면 암호 64bits가 된다(그림 3).

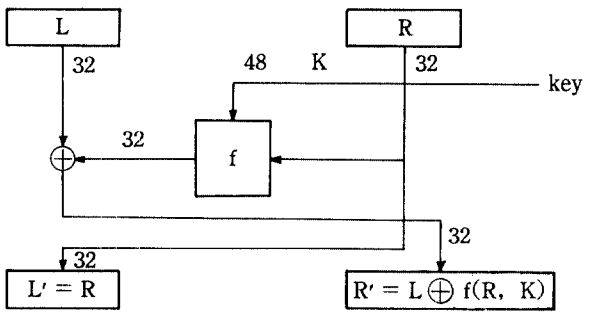

그림 3. 한단계의 암호계산

– Cipher function f(R, K)

◦ 32bits R이 Expansion box(E-box)에 의해 48 bits로 확장되고, 48bits의 key K와 함께 modulo 2 계산에 의해 중간결과인 48bits가 나온다.

◦ 이 48bits가 8개의 Substitution box(S-box)에 의하여 32bits가 생산되고, Permutation-box (P-box)에 의해 32bits 결과가 나오면 32bits L과 modulo 2에 의하여 R′가 만들어 진다(그림 4).

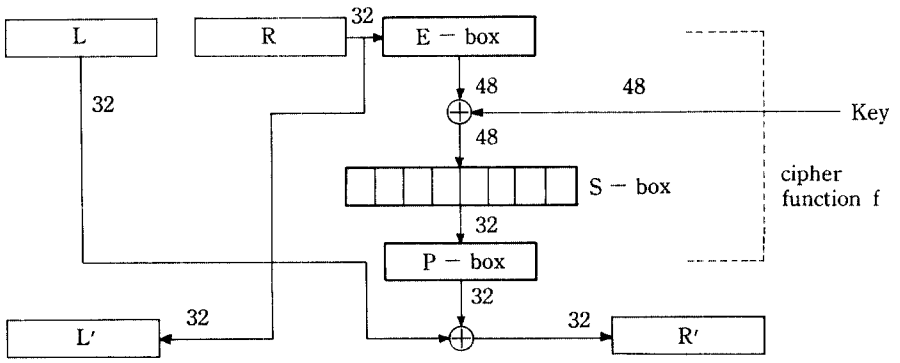

그림 4. Cipher function f

– 키 생산(key schedule)

◦ 64bits의 key에서 8개의 parity bits를 제외한 56bits가 Permuted choice 1(PC−1)에 의하여 만들어지고, 좌우(C, D) 28bits씩 분류된다.

◦ Table of key schedule shifts에 의해 키의 위치가 변한다.

◦ Permuted choice 2(PC−2)에 의해 56bits가 48bits로 만들어져 cipher function f에 적용된

다(그림 5).

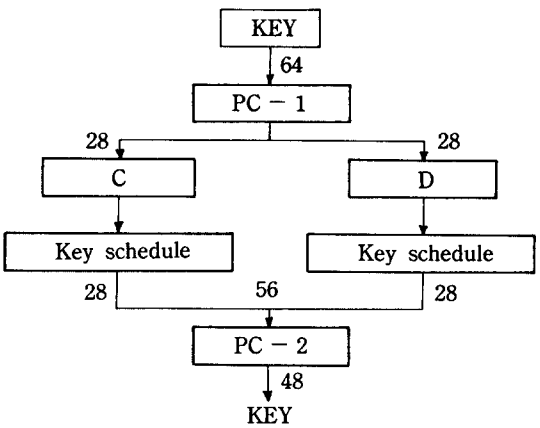

그림 5. 키 생산 과정

− 복호화 과정

- 암호화 과정과 동일하나, 암호화시 사용된 key가 역순서로(16th key→1st key, 15th key →2nd key,…) 적용되고, key schedule shifts의 방향이 왼쪽에서 오른쪽으로 적용된다.
- 64bits의 암호문이 최종 permutation(IP^{-1})을 거쳐 32bits씩 좌우로 나누어진다.
- 암호화의 역순으로 모든 것이 이루어진 후, IP를 거쳐 원문 64bits가 생성된다.

4.2 공개 키(public-key) 시스템

공개키 시스템에서는 정보의 전송 전에 비밀키의 교환이 필요없이 암호화 키(encryption key)를 누구나 사용할 수 있도록 공개하고, 복호화 키(decryption key)의 보안을 유지하는 기법을 쓰고 있어 asymmetric 알고리즘이라고 한다.

이러한 공개키 시스템 개념의 4가지 기본성질은 다음과 같다. 암호화 과정을 E, 복호화 과정을 D, 암호문을 C, 원문을 M, 그리고 키를 k라고 할 때 ;

- 모든 key k에 대하여, Ek와 Dk는 역함수 관계가 성립한다($Ek \cdot Dk = 1$).
  $Ek(M) = C$이면, $Dk(C) = Dk(Ek(M)) = Ek \cdot Dk(M) = M$이다.
- 모든 키 k는 M에 대하여, Ek(M)과 Dk(M)의 계산이 용이하다.
- 거의 모든 키에 대하여, 암호화 키 Ek만 아는 상태에서 복호화 키 Dk를 계산해 내는 것은 실현불가능하다.
- 모든 키 k에 대하여, Ek와 Dk가 역으로 적용될 수 있다(Dk로 암호화 하고 Ek로 복호화가 가능하다).
  $Dk(M) = C'$이면, $Ek(C') = Ek(Dk(M)) = Ek \cdot Dk(M) = M$이다.

여기서 셋째의 성질에 의하여 암호화 키를 공개할 수 있고, 첫째, 둘째, 셋째의 성질을 만족할 때 "trapdoor one-way function"이라 하며, 네가지 성질 모두를 만족시킬 때 "trapdoor one-way permutation for signature"라 한다.

1) RSA(Rivest, Shamir and Adleman)시스템

Diffie와 Hellman의 공개키 알고리즘(1976)에 대한 첫번째 실현방법이 MIT의 Rivest, Shamir 그리고 Adleman 세사람에 의하여 1978년 개발되었다(그림 6). 이 암호시스템에서는 두개의 큰 소수 p, q에서 곱 n을 구하여 암호화에 사용되는데, 이 시스템의 안전도는 n을 소인수분해하여 p와 q를 산해 내는 난이도에 달려있다.

− 키 선정 방법

- 공개 암호키 e와 비공개 복호키 d는 모두 양의 정수로 되야 한다.
- 2개의 큰 소수 p, q를 구한다.
- 2소수 p, q의 곱 $n = p \cdot q$를 계산한다.
- 공개 키로 사용할 큰 수 e를 선정하는데, Euler 함수 $\phi(n)$과 e의 최대공약수가 1이 되어야 한다. 그리고 e는 "max(p, q)+1"과 "n−1" 사이의 수이어야 한다.
  $\phi(n) = (p-1)(q-1)$, $GCD(\phi(n), e) = 1$
- Euclid 이론에 의하여 "d"를 구하고 비밀키로 사용한다.
  $d \equiv e^{-1} \bmod \phi(n)$

− 암호화, 복호화 방법

- 원문을 암호화하기 위하여 숫자(A=01, B=

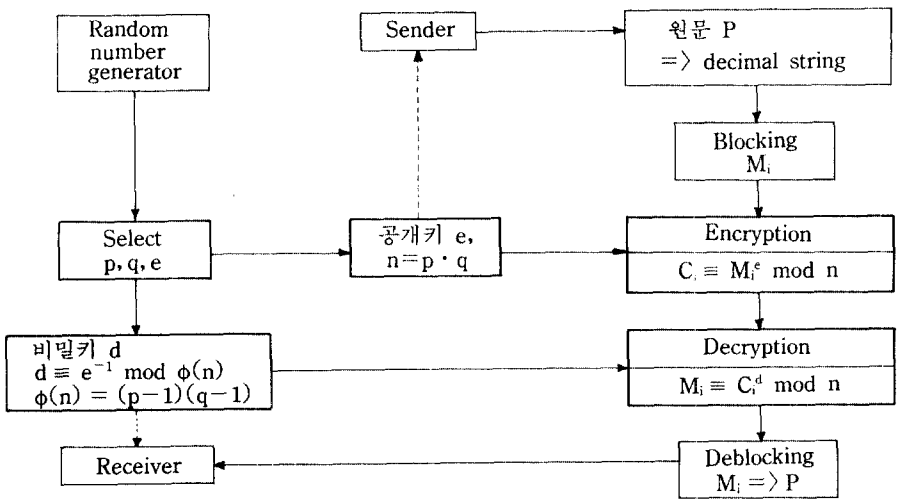

그림 6. RSA Cryptosystem

02, ⋯, Z=26)로 변환시키고 Blocking하되 그 값 M_i가 n−1을 넘지 않도록 하여야 한다.

- M_i를 e로 암호화하여 암호문 C_i를 만든다.

  $C_i \equiv M_i^e \bmod n$

- 수신자는 비공개 복호키 d로 원문의 전단계인 M_i를 구한다.

  $M_i \equiv C_i^d \bmod n$

- M을 deblocking하고 숫자에 해당문자를 일치시켜 원문 P를 찾아낸다.

  M_i =〉 P

2) MH(Merkle and Hellman)시스템

1978년 Merkle과 Hellman에 의하여 knapsack 문제가 최초로 공개키 암호기법에 적용되었다. Knapsack 벡타 $A'=(a'_1, a'_2, \cdots, a'_n)$와 2진수인 비밀벡타 $X=(\chi_1, \chi_2, \cdots, \chi_n)$가 있으면 ($\chi_i$="0" or "1"), $S=A' \cdot X=\sum_{i=1}^{n} a'_i\chi_i$에서 knapsack 문제는 S와 A'가 주어졌을 때 벡타 X를 구하는 것으로서 이러한 knapsack 방법은 R.M.Karp(1972)의 개념에서 비롯됐다.

공개키 알고리즘에서는 A'가 공개키가 되고 원문 X가 암호문 S로 바뀌는 것이다. 이때 벡타 A'는 반드시 "$a'_i > a'_1 + a'_2, \cdots, a'_{(i-1)}$"의 조건을 만족시켜야만 X의 값을 쉽게 구할 수 있으며, 이 때의 벡타를 superincreasing vector라고 한다.

단순히 superincreasing vector A'를 이용한 knapsack-based 암호시스템은 누구나 쉽게 해독할 수 있기 때문에 Merkle과 Hellman에 의하여 trapdoor knapsack 암호가 개발되었다. 즉 superincreasing 성질을 가진 simple(easy) knapsack vector A'를 key (trapdoor)가 없이는 풀기가 거의 불가능한 trapdoor knapsack vector A로 변화시켜서 암호기법에 적용한 것이 MH 시스템이다(그림 7).

– key 선정 방법

- Superincreasing simple vector $A' = (a'_1, a'_2, \cdots, a'_n)$를 선택한다.
- 매우 큰 정수 m, w를 다음의 조건이 만족하도록 구한다.

  $GCD(m, w) = 1, \quad w < m,$

  $w \cdot w^{-1} \equiv 1 \bmod m$

  $m > \sum_{i=1}^{n} a'_i$

- simple knapsack vector A'에서 trapdoor knapsack vector $A=(a_1, a_2, \cdots, a_n)$를 구한다.

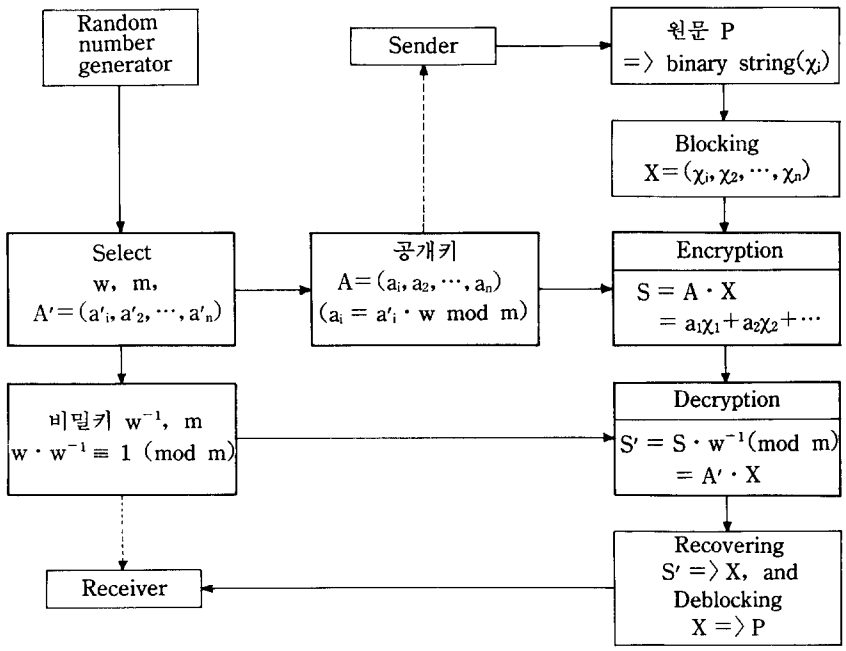

그림 7. MH Cryptosystem

$$A = A' \cdot w \pmod m$$

◦ 이 trapdoor vector A를 공개키로 사용하고 simple vector A′와 m 및 w^{-1}를 비밀키로 이용한다.

— 암호화, 복호화 방법

◦ 암호화 과정은 원문 P를 이진수 block X=(χ_1, χ_2, ⋯, χ_n)로 변환시켜 trapdoor vector A로 암호를 만든다.

$$S = A \cdot X = a_1\chi_1 + a_2\chi_2 + \cdots a_n\chi_n = \sum_{i=1}^{n} a_i\chi_i$$

◦ trapdoor 정보인 w^{-1}과 m을 알고 있는 이용자만이 원문을 얻을 수 있다.

$$S' = w^{-1} \cdot S \pmod m$$

5. 암호학의 동향분석

미국에서 70년대초에 암호표준안을 준비하고 public-key 알고리즘이 중반기인 1976년에 개발되므로서, 관련분야의 연구개발이 활기를 띄기 시작하여 세계 각국에서 이 암호학에 관심을 갖게 된 것은 80년대초 부터라고 할 수 있다.

최근 정보화 사회의 도래에 힘입어 여러분야에서 암호학에 대한 중요성을 인식하여 활발한 연구개발이 이루어지고 있다. 이와 관련하여 미국, 일본을 비롯한 국내외 암호기법의 표준화 및 기술개발… 등 관련분야의 동향을 다음과 같이 조사 분석하였다.

5.1 미국

1977년 미국 정부의 표준 암호 알고리즘으로 제정된 DES에 관하여 여러 분야에서 보안책을 포함한 관련기법 및 다양한 표준들이 다음의 5개 기관에 의해서 주로 많이 만들어지고 있다.

1) ABA(American Bankers Association)

은행과 연관된 금융에 대한 암호표준만을 주로 개발하고 있다. 즉, ATM(Automatic Teller Machine), POS(Point-of-Sale) 단말기 이용시 사용자의 ID(PIN : Personal Identification Numbers) 처리기법 등에 DES를 적용하였다.

그리고 매일 수천억 달러의 EFT(Electronic Fund Transfers) 처리와 CHIPS(Clearing House Interbank Payments System) 등의 모든 처리도 DES에 의하여 보안이 이루어지고 있으며, 모든 금융 데이터의 보안유지는 반드시 DES를 사용하도록 ABA에서 권고하고 있다.

2) ANSI(American National Standards Institute)

ANSI 산하에 정보처리시스템을 관장하는 ASC (Accredited Standards Committee) X3와 금융서비스에 관여하는 ASC X9 등에서 DES를 중심으로 많은 표준을 만들고 있다. 그리고 ASC X3는 CBEMA(Computer and Business Equipment Manufactures Association)에서, ASC X9은 ABA (American Bankers Association)에서 관련업무를 총괄하고 있다.

한편, X3T1 subcommittee에서는 DES를 DEA (Data Encryption Algorithm)로 표준화를 했고 (ANSI X3.92), Operation 표준의 DEA Modes를 제정하였다(ANSI X3.106). 그리고 X9A3(Financial Institution Retail Security)에서는 DES를 이용하여 PINs의 보안과 관리를 위한 표준을 개발하였다(ANSI X9.19). 또 X9E9(Financial Institution Wholesale Security)에서는 DES를 응용하여 키 관리(ANSI X9.17)와 메세지 인증(ANSI X9.9)을 위한 표준을 발표하였다.

3) NBS(National Bureau of Standads)

Brooks법(Public Law 89-306)과 컴퓨터 보안법 (Computer Security Act : 1987)에 의하여 NBS의 ICST(Institute for Computer Science and Technology)가 주도하여 암호학의 응용을 포함한 각종 ADP(Automatic Data Processing)자료의 보호와 컴퓨터 보안을 위한 표준화가 이루어지고 있다.

그리고 NBS는 DES(FIPS #46)를 비롯하여 Guidelines for Implementing and Using the NBS DES (FIPS #74), DES Modes of Operation(FIPS #81), Password Usage(FIPS #112), Computer Data Authentication(FIPS #113) … 등을 발표하였으며 암호학 관련분야의 표준화 연구를 계속하고 있다.

4) GSA(General Services Administration)

GSA는 NCS(National Communication System)의 telecommunication 표준화를 주도하였으나, 1987년 제정된 Computer Security법에 의해 NBS에 컴퓨터와 telecommunication 등에 관련된 표준화 작업을 인계하였다.

NCS에서는 데이터 통신의 데이터 링크층과 물리적인 측면에서의 DES 이용, DES를 이용한 일반전자장비 그리고 팩시밀리장비의 표준화 등이 이루어졌으며, 1987년말까지 NSA(National Security Agency)에서 관여하였다.

5) ISO(International Organization for Standardization)

데이터 보호에 관한 표준화사업에 ISO가 많은 관여를 하여 DES를 DEA 1(Data Encryption Algorithm-1)이라는 국제표준으로 1986년에 확정하였다. 그리고 ISO의 TC-68/SC-2/WG2에서는 금융에 관한 암호표준화 작업중에서 키 관리와 메세지 인증에 관한 표준을 제정하였으며, TC-97/SC-21/WG1에서는 보안관련 architecture에 관한 표준화 작업을 하고 있다.

최근 ISO groups에서는 디지틀 서명, 키 분배 및 데이터의 안전성 등 network security에 관련된 표준화작업을 하고 있다.

5.2 일본

1984년부터 일본에서는 본격적인 암호학 연구가 수행되고 있으며, 1990년 5월까지 암호학과 정보보안에 대한 7번의 심포지움과 4번의 workshop이 84년과 86년부터 개최되어 암호학 연구개발이 활성화되고 있다.

이러한 암호관련 회의를 통하여 통신공학과 전산과학 분야에서 DES와 public-key 시스템 … 등에

대하여 많은 논문이 발표되었다. 통신망의 전국적인 확산과 더불어 통신보안에 관련된 암호기법의 연구로 일본에서의 현대 암호학이 출현하게 되었다.

이와 함께 CIS Group(Cryptography and Information Security Research Group)과 EIC(Institute of Electronics, Information and Communication Engineers of Japan)내의 관련 Group 등에 의하여 다음과 같은 심포지움과 workshop 등이 개최되고 있다.

1) SCIS 84

1983년에 CIS Group이 결성되어 일본에서의 본격적인 암호학 연구가 시작되었으며, 이 Group에서 제 1 회 SCIS(Symposium on Cryptography and Information Security) 84를 주관하였다.

여기에서는 암호시스템 및 표준화 동향, 새로운 공개키 시스템 등을 주제로 11개의 논문이 발표되었으며, 정보보안과 암호학에 관한 중요성 등이 토의되었다.

2) SCIS 85

두번째 심포지움 SCIS 85에서 발표된 11개의 논문 중 소수를 구하는 Solovay-Strassen 방법이 일본 암호학 연구진들에 큰 관심사가 되었다.

그리고 요코하마 대학과 도쿄대학에 의해 공개키 시스템 연구에 큰 영향을 끼친 "Obscure Representation"이라는 새로운 개념이 발표되었다. 한편 EIC는 Technical Group on Cryptography and Information Security(EIC-TGCIS)를 구성하여 87년까지 2년동안 암호학의 연구를 수행하였다.

3) SCIS 86과 WCIS 86

CIS Group과 EIC-TGCIS가 주관하여 열린 SCIS 86에서의 25개 논문중 6개가 새로운 공개키 시스템에 관한 것이고 그 중에 3개는 전년도에 나온 "Obscure Representation" 개념에 기초한 것이었다. 한편, 암호학 기법에서의 키 분배나 IC 카드 이용 등과, 주제를 확대시켜 OS의 보안 시스템까지 다루었다.

그리고 첫번째 개최된 암호학과 정보보안에 관한 workshop WCIS 86(Workshop on Cryptography and Information Security)에서는 공개키 시스템의 새로운 기법 등을 포함하여 12편의 논문이 나왔다. 이 중에 요코하마 대학의 KPS(Key Predistribution Algorithm) 등이 암호학 연구에 많은 영향을 끼쳤다.

KPS는 대규모 네트웍 중심의 키 분배 시스템으로서 이것을 구현하기 위하여 IC 카드를 사용하였다. 이 시스템은 대규모 네트웍에서 키 분배시 발생되는 중요한 문제점들을 해결하는 가장 효과적인 방법중의 하나이다.

한편, FEAL(Fast Data Encipherment Algorithm)은 DES와 유사한 구조를 갖고 있는 public-key 암호방법으로 DES보다 매우 빠른 암호시스템이다. 이 알고리즘이 안전도에서는 약간의 문제가 있지마는 현재 여러가지 응용분야에 실제로 사용되고 있다.

4) SCIS 87과 WCIS 87

암호학 관련 심포지움이나 workshop을 87년 이전에는 주로 요코하마 대학에서 주관하였으나, 87년의 SCIS는 Kansai Crypto Group에서 개최하였다.

이 심포지움에서는 28편의 논문이 발표되었으며 다음과 같은 3가지 특징을 지니고 있다. 첫째는 정보보안 분야에서 가장 중요하고 어려운 문제중의 하나였던 "안전성 평가방법"에 관한 것이고, 둘째는 일본에서 널리 알려지지 않은 "Zero Knowledge Proof"의 내용이었으며, 마지막으로는 ID(identity)-based cryptosystem과 KPS(Key Predistribution System)에 관한 토론이었다. 그밖의 내용으로는 암호 통신장비, FEAL, EFT 방법, 소수계산법, 새로운 공개키 시스템 … 등도 다루어졌다.

그리고 두번째 열린 WCIS에서는 17편의 논문이 나왔으며, ID-based cryptosystem에 대한 토론과 "Theory of computational complexity"에 관한 연구 등이 큰 관심을 끌었다.

5) SCIS 88과 WCIS 88

와세다 대학에 의해 개최된 SCIS 88에는 41개의

논문이 나왔으며, ID-based cryptosystem과 통신 보안용 암호장비에 관한 내용들이 주요 관심사가 되었고, 암호시스템의 하드웨어 구현도 그 중 하나였다.

그밖의 암호화 및 복호화 기능을 갖춘 "FEAL-8"이라는 암호장비, RSA 시스템 구현에 관한 여러 가지 실험들의 결과, Fiat-Shamir 기법과 지문을 이용한 Identification 시스템 … 등도 발표되었다.

그리고 EIC에서는 88년에 EIC-TGISEC(Technical Group on Information Security)을 구성하고 CIS Group과 함께 ZKIP(Zero-Knowledge Interactive Proof)를 주요 주제로 하여 WCIS 88을 개최하였으며 18개의 논문이 발표되었다.

6) SCIS 89와 WCIS 89

CIS Group과 EIC-TGISEC가 SCIS 89를 개최하여 35편의 논문이 나왔으며, 그림을 응용하여 코딩하는 "Picture cryptosystems"과 ZKIP 등이 주요 주제로 다루어졌고 computer virus에 대한 주제도 나오기 시작했다.

한편, 와세다 대학에 의해 개최된 WCIS 89에는 ZKIP를 다룬 내용이 주를 이루었고, computer virus에 대한 과학적 연구결과가 일본에서는 처음 발표되었다. 특히 흥미로운 것은 NTT에서 "FEAL-8"의 암호해독에 현상금을 걸었는데, 이는 아마 89년 초에 부분적으로 FEAL-8을 해독한 A. Shamir의 chosen-plaintext attack에 대한 방어수단인 듯 하다.

7) SCIS 90 및 기타

와세다 대학에서 주관한 SCIS 90에는 43편의 논문이 나왔으며 "Zero-Knowledge Proofs"와 ID-based 서명 등이 주요 주제로 다루어졌다. 그외 응용분야로는 자동 지문 패턴 분류에 의한 암호기법과 팩시밀리의 디지틀 서명과 팩시밀리의 암호화 등의 주제가 나왔다. 그리고 마이크로 프로세서를 이용한 FEAL, FEAL의 확장개념, 공개키를 이용한 Pay-TV 서비스 기법,… 등도 발표되었다.

그리고 일본에서는 91년 11월에 ASIACRYPT '91이라는 암호학 국제회의를 준비중이고, CIS Group(과 EIC-TGCIS) 및 EIC-TGISEC 등에 의해 암호학과 정보보안에 관한 연구개발 활동이 전개되고 있으며, 주요 암호학 기술보유국으로 발돋움하고 있다.

5.2 국내 동향

국내에서도 군이나 일부 특수기관에서 제한된 분야의 암호화기법에 관한 연구개발 및 응용사업이 오래전부터 수행되어는 왔으나, 민간에서 공개적으로 암호학 연구가 시작된 것은 한국전자통신연구소(ETRI)에서 주관하여 제 1 회 정보보안과 암호학에 관한 workshop(Workshop on the Information Security and Cryptography : WISC '89)이 개최된 1989년부터라고 할 수 있다.

1) WISC '89

정부주도의 암호학 연구를 수탁업무 형식으로 수행해 오던 한국전자통신연구소에서 국내 암호학 연구의 활성화를 위하여 개최한 WISC '89가 학계는 물론이고 업계에도 암호기법과 정보보안에 많은 관심을 불러 일으키게 하였다.

WISC '89에 발표된 22편의 논문 중 ETRI에서 12편 그밖의 10편은 대학에서 발표하였다. 이처럼 업계나 기업부설 민간 연구소 등의 참여가 전혀 없었던 것은 참가인원의 제한도 있었지만, 국내 암호학 연구가 아직도 초기단계를 벗어나지 못한 상태로서 커다란 문제점으로 지적되었다.

이 workshop에서는 "정보와 컴퓨터 보안", "각종 암호이론" 및 "암호학 응용분야" 등 크게 3분야에서 다음과 같은 주요 관심주제들이 발표되었다. 즉, 비밀키와 공개키를 합성한 시스템, 전자파에 의한 정보누출 방지 방안, 확률을 이용한 암호기법, 암호데이터 연산법, DES Block cipher 설계 등을 들 수 있으며, "국내 암호학 및 관련분야의 발전방향"에 대한 토의도 많은 관심을 끌었다.

2) WISC '90과 KIISC

ETRI에서 주최한 WISC '90에는 24편의 주제가 발표되었으며, 주요 관심주제로는 Reed-Solomon 코드를 이용한 비도분석, 다항식을 이용한 서명방식, 한글 암호화를 위한 한글빈도와 엔트로피 계산 등이 있다. 그리고 새로운 키분배 방식, 누수전자

파에 의한 정보유출과 보안시스팀, 보안시스팀 개발과 정형화 등에 관한 연구도 많은 관심을 보였다.

한편, 같은 해 12월 12일 암호학을 연구하는 순수 학술단체인 한국통신정보보호학회인 KIISC(Korea Institute of Information Security & Cryptology)가 설립되었다. 이제까지 특수목적과 특수분야를 위해서만 이루어지던 암호학 연구가 이 학회를 중심으로 각 방면에서 수행될 수 있게 되어 앞으로 국내 암호학 연구에 활성화를 기할 수 있을 것이다.

국내에서 WISC가 89년에 시작된데 비하여 일본에서는 SCIS가 84년부터, WCIS는 86년부터 개최되었다. 그리고 KIISC보다 7년 앞선 1983년에 GIS Group이 2년 앞서서는 EIC-TGISEC(1988)이 결성되어(EIC-TGCIS는 87년까지 2년동안 업무수행) 일본의 암호학 및 관련분야의 연구개발을 주도하고 있다.

6. 결 론

암호학의 기법을 여러가지 방향으로 다룰 수 있으나 본고에서는 1970년초를 기준으로 전통적 암호방식을 근대암호기법에서 우선 다루었고, 그후의 비밀키 시스팀(DES)과 공개키 시스팀을 현대암호학으로 분류하여 서술하였으며, 암호학 동향에서는 미국, 일본 및 국내의 암호학 관련 연구분야의 동향을 조사분석하였다.

이러한 암호학의 동향분석 결과와 국내 사정을 감안하여 다음과 같은 점에 노력을 기울여야 할 것으로 판단된다.

- 독자적인 암호시스팀의 연구개발과, 이미 개발된 알고리즘에 의한 암호화 장비의 제품화를 이루어야 한다.
- 한글의 자모 및 받침 등의 요소와 빈도분포 등을 연구하여 한글암호기법을 개발하여야 한다.
- 국내 암호기법의 표준화를 제정하되, 도입된 외국 암호 시스팀이 아닌 국내에서 개발된 고유암호시스팀을 표준으로 채택하여야 대외적인 안전도를 높일 수 있다.
- 제한된 분야보다는 모든 분야에 걸쳐 개방적인 암호학 연구를 확대하여야 하며, 암호학 연구 인력의 저변확대를 위한 적극적인 방안을 강구하여야 한다.

參 考 文 獻

1. R. Andersen "The Destiny of DES" Datamation Mar-87 P. 79-84
2. H. Baker & F. Piper "Cipher Systems" John Wiley & Sons 1982
3. G. Brassard "Cryptology in Academia : A Ten Year Retrospective" COMPCON Feb-87 P. 222-226
4. D. E. R. Denning "Cryptography and Data Security" Addison-Wesley 1983.
5. W. Diffie "The First Ten Years of Public-Key Cryptography" Proc. of the IEEE V-76 N-5 May-88 P. 560-577
6. A. Dror "Secret Code" Byte V-14 N-6 Jun-89 P. 267-270
7. R. Grehan "Cloak and data" Byte V-14 N-6 Jun-90 P. 311-324
8. M. E. Hellman "Commercial Encryption" IEEE Network Magazine V-1 N-2 Apr-87 P. 6-10
9. R. Howard "Data Encryption Standard" Inf. Age V-9 N-4 P. 204-210
10. H. Imai "Recent Development of Cryptology in Japan" Trans. IEICE V-E73 N-7 Jul-90 P. 1026-1030
11. D. Kahn "Cryptology goes Public" IEEE Comm. Mag. Mar-80 P. 19-28
12. S. Kerr "A Secret No More" Datamation V-35 N-13 Jul-89 P. 53-55
13. K. S. Lee "Elaboration d' un cryptosystème hybride à deux niveaux" Univ. Paris 7 Dec-86
14. J. L. Massey "An Introduction to Contemporary Cryptology" Proc. of the IEEE V-76 N-5 May-88 P. 533-549
15. C. H. Meyer "Cryptography-A State of the Review" COMPEURO 89 May-89 P. 4. 150-4. 154
16. C. H. Meyer & S. M. Matyas "Cryptography" John Wiley & Sons 1982

17. C.P.Pfleeger "Security in Computing" Prentice-Hall 1989

18. J.Seberry & J.Pieprzyk "Cryptography" Prentice-Hall 1989

19. A.Sinkov "Elementary Cryptanalysis Mathematical Approach" Random House 1968

20. M.E. Smid & D.K.Branstad "The Data Encryption Standard : Past and Future" Proc. of the IEEE V-76 N-5 May-88 P.550-559

□ 著者紹介

이 경 석(正會員)

1978년 崇実大 電算學(學士)
1981년 成均館大 電算學(碩士)
1986년 프랑스 Paris 7 大學校 電算學 博士(暗號專攻)
1983년~1986년 Univ. Paris 7 研究所(ITODYS) 研究員
1978년~1991년 現在 産業研究院 電算室 副研究委員

關心分野 : 暗號理論, 데이타베이스, 情報檢索 시스템, Image file processing.