정보학연구 제6권 제4호 2003년 12월(pp.59-68)
The Journal of Information Technology. Vol.6. No.4

통신 네트워크의 정보보호를 위한 공개키 다항식 암호시스템

양태규*

요 약

본 논문에서는 컴퓨터 통신 네트워크의 정보보호를 위해 다항식의 인수분해의 어려움이 있는 공개키 다항식 배낭 암호시스템과 공개키 다항식 지수 암호시스템을 제안하였다. 먼저, 제안된 공개키 다항식 배낭 암호시스템에서 공개키는 2개의 다항식 B(x,y,z)와 f(x,y,z)로 하고, 비밀키는 초증가성 벡터로 한다. 암호문의 해독은 f(x,y,z)=0의 근, 그리고 비밀키 벡터의 초증가성을 사용하여 평문이 구해진다. 여기서 3변수 다항식 f(x,y,z)=0의 인수분해의 어려움 때문에 안전성을 갖는 암호시스템으로 된다. 또한 제안된 공개키 다항식 지수 암호시스템에서는 소인수분해의 어려움에 기초를 둔 기존 방법의 안전성에, 2개의 다항식 f(x,y,z)=g(x,y,z)=0을 인수분해 하여 동시에 만족하는 근을 구하는 어려움을 더함으로써 보다 더 안전성 있는 공개키 암호시스템으로 된다. 제안된 공개키 다항식 암호시스템의 타당성을 컴퓨터 시뮬레이션을 통하여 입증하였다.

Ⅰ. 서론

컴퓨터 통신 네트워크는 컴퓨터 기술과 통신 기술의 집합체로 오늘날 고도의 정보화 사회에서 요구되는 각종 서비스를 제공해 주고 있다.

암호 방식은 암호키의 분배와 관리 방법에 따라 전통적인 암호 방식(Conventional cryptosystem)과 공개키 암호 방식(Public key cryptosystem)으로 나눌 수 있다.[1][2] 전통적인 암호 방식은 암호키(Enciphering key)와 해독키(Deciphering key)가 동일하며 이 두 키는 송신자와 수신자가 공용하는 비밀키가 된다. 일반적으로 전통적인 암호는 전치 암호, 환자 암호 및 합성 암호 등으로 분류된다. 공개키 암호는 암호키와 해독키가 서로 다르며 암호화 키는 공개하나 해독키는 비밀로 보관하는 것이 보통이다.

정보보호에서 문제가 되는 중요 서비스로는 보관중이거나 전송중인 정보가 우연히 혹은 의도적으로 인가되지 않은 제3자에게 노출되는 것을 예방하는 기밀성(Confidentiality), 정보가 변조되지 않고 원래의 상태를 유지하는 것을 보증하는 무결성(Integrity), 통신하는 상대방이 정당한 상대방인가를 확인하는 인증(Authentication), 인가되지 않은 사람이 정보에 접근하지 못하도록 하는 접근제어(Access control), 정보의 발신 및 수신 사실을 사후에 부정하지 못하도록 하는 부인봉쇄(Nonrepudiation) 등이 있다.

전통적인 암호시스템의 단점은 1976년 Diffie Hellman[3]이 제안한 One-way 함수를 이용한 공개키 개념을 도입함으로써 해결될 수 있게 되었다. 이 개념의 도입은 종래 암호에 있어서 문제점이었던 키 교환 문제를 해결하였을 뿐만 아니라 정보화 사회로 접어든 현대 사회에서 중요한 인증 디지털 서명(Authentication digital signature), 사용자 확인(User identification) 등의 실용을 가능

* 목원대학교 IT공학부 교수

하게 하였다. 공개키 개념을 이용한 암호 방법 중 가장 먼저 제안된 것은 1978년 Rivest, Shamir와 Adieman[4]에 의한 RSA 암호이다.

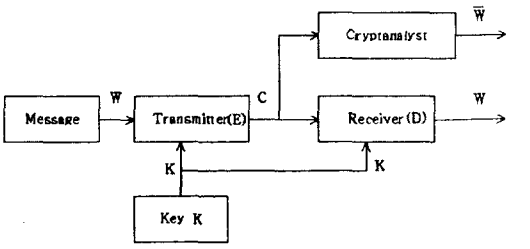
이 암호는 큰 합성수의 소인수 분해의 어려움에 안전성의 근거를 가지고 있으며, 발표 후 20여년이 지난 오늘날에도 가장 널리 쓰이며 안전성을 인정받고 있는 공개키 암호법이나, 소인수 분해법의 눈부신 발전 및 하드웨어의 급속한 성능 향상으로 조만간 키의 크기(Key size)를 크게 해야 할 것으로 평가받고 있다. 또한 1978년에 Merkle와 Hellman[5], Chor와 Rivest[6] 등에 의해 배낭 문제(Knapsack problem)를 사용한 MH 암호 등이 제안되었다. El-gamal[7]은 1985년에 이산적 대수 문제의 어려움에 대한 안전성을 갖는 암호를 제안하였으며, 1989년에 Tsujii[8] 등은 비선형 방정식의 해를 구하기 어려움에 기초를 둔 공개키 암호시스템을 일반화하였다.

본 논문에서는 3변수 다항식의 근을 구하기 어려움, 즉 다항식의 인수분해의 어려움 때문에 안전성을 갖는 공개키 다항식 배낭 암호시스템과 공개키 다항식 지수 암호시스템을 제안한다. 시뮬레이션을 통해 주어진 문자 평문에 대하여 암호화하고 해독하여 제안된 공개키 다항식 배낭 암호시스템과 공개키 다항식 지수 암호시스템의 타당성을 입증한다.

II. 암호화 방법

2.1. 전통적인 암호 방법

전통적인 암호 방법은 공통키 암호 방법, 또는 공개키 암호 방법에 대응되는 비밀키 암호 방법이라 불리는 암호 방법으로 (그림 1)과 같다.



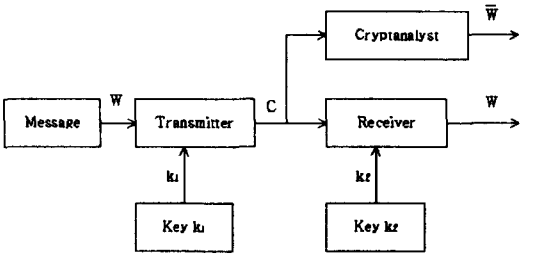
(그림 1) 전통적인 암호시스템
(Fig. 1) Conventional cryptosystem

정보를 교환하고자 하는 상호 암호 통신망 가입자는 사전에 비밀 공통키 K를 제삼자에게 노출되지 않게 나누어 가진 다음, 암호 통신을 필요로 할 때 평문 W(Plaintext)를 암호 알고리즘 E와 공통키 K로 암호문 C(Ciphertext)를 생성시켜 공중 통신 채널을 통해서 전달하고 암호문 C를 수신한 가입자는 해독 알고리즘 D와 공통키 K로 평문 M를 얻는 방법으로 오래전부터 사용되어 온 암호 방법이다.

2.2 공개키 암호 방법

공개키 암호 방법은 전통적인 암호 방법과 달리 암호키(Encryption key)와 해독키(Decryption key)를 분리하여 암호키는 암호통신망 가입자 모두에게 공개하고 해독키는 가입자 각자가 비밀리에 보관하는 방법으로 비대칭(Asymmetric) 알고리즘이라고 한다.

이 암호시스템은 (그림 2)와 같이 암호키 K_1과 해독키 K_2가 다르며, 암호키에서 해독키를 만들어 낼 수 없다는 것이다. 이 방식에서 송신자가 사용하는 암호키 만을 공개하고 수신자는 해독키만을 관리함으로써 도청자가 암호키를 얻더라도 원래의 평문을 구하기가 어렵게 된다.



(그림 2) 공개키 암호시스템
(Fig. 2) Public key cryptosystem

공개키 암호 방법으로 구성된 암호 통신망 가입자는 암호키와 해독키 2개가 필요하게 되므로 전체 가입자가 n명일 때 암호키의 수는 2n개이고, 실제로 비밀리에 보관해야 하는 해독키의 수는 n개로 각 가입자가 자기 소유의 해독키 하나만을 보관하게 되므로 전통적인 암호 방법 보다 보관해야 할 키의 수가 적고 또한 암호화키를 공개하므로 키분배가 필요 없어 키 관리가 용이하다.

Ⅲ. 제안된 공개키 다항식 암호 시스템

3.1. 다항식 배낭암호

주어진 정수의 집합과 이 집합의 원소들의 합으로부터, 부분 집합을 찾아내는 데 어려움을 둔 MH 배낭 암호의 안전성에 공개키 다항식의 근을 구하는 어려움의 안전성을 더함으로써, MH 배낭 암호보다 안전성 있는 공개키 배낭 암호 알고리즘을 제안한다.

3.1.1. 키 생성

먼저 배낭 암호의 키생성을 위해 (1)식을 만족시키는 초증가 벡터(Superincreasing vector) $A=(a_1,a_2,\cdots,a_n)$를 정의한다.

$$a_i > \sum_{j=1}^{i-1} a_j \quad (i=2,\ 3,\ 4,\ \cdots,\ n) \qquad (1)$$

그리고 조건식 $p > \sum_{i=1}^{n} a_i$를 만족시키는 소수(prime number) p를 정한 후, $0<x_1,\ y_1,\ z_1<p$를 만족시키는 임의의 정수 x_1, y_1와 z_1를 선택하여 $x=x_1$, $y=y_1$과 $z=z_1$로 한다. 다음에 (2)식을 만족하도록 초증가 벡터의 요소(element) a_i를 적당하게 a_{i1}, a_{i2}와 a_{i3}로 3분할하여 표현한다.

$$a_i=a_{i1}+a_{i2}+a_{i3} \pmod p \qquad (2)$$

(2)식에서 우변의 각 항을 변수 x, y와 z를 사용하여 (3)식과 같이 변형한다.

$$\begin{aligned} a_{i1}&=b_{i1}x+r_{i1} \pmod p \\ a_{i2}&=b_{i2}y+r_{i2} \pmod p \\ a_{i3}&=b_{i3}z+r_{i3} \pmod p \end{aligned} \qquad (3)$$

여기서 r_{i1}, r_{i2}와 r_{i3}는 나머지이고, 이 나머지의 합을 (4)식과 같이 b_{i4}로 표현한다.

$$b_{i4}=r_{i1}+r_{i2}+r_{i3} \pmod p \qquad (4)$$

따라서 초증가 벡터의 요소 a_i가 (3)식과 (4)식과 같이 다항식으로 표현된다. 이러한 다항식을 사용하여 배열 순서를 적당하게 변환하여 (5)식과 같이 다항식 벡터 B(x, y, z)를 표현한 후 암호 벡터로써 공개한다.

$$B(x,y,z)=(b_{11}x+b_{12}y+b_{13}z+b_{14},$$

$b_{21}x+b_{22}y+b_{23}z+b_{24}, \cdots, b_{n1}x+b_{n2}y+b_{n3}z+b_{n4}$ (5)

그리고 다른 하나의 공개키 다항식 f(x,y,z)의 계수 f_1, f_2와 f_3는 다음 식을 만족시키는 정수로 적당히 선택한다.

$$0<f_1, f_2, f_3<p \quad (6)$$

또한 공개키 다항식의 계수 f_4는 (4-7)식과 같이 구한다.

$$f_4=-f_1x_1-f_2y_1-f_3z_1 \pmod p \quad (7)$$

따라서 (6)식과 (7)식에서 나타낸 계수 f_1, f_2, f_3와 f_4를 이용하여 (8)식과 같은 공개키 다항식 f(x,y,z)를 공개한다.

$$f(x,y,z)=f_1x+f_2y+f_3z+f_4 \quad (8)$$

이 암호의 안전성은 (9)식을 만족시키는 다항식 f(x,y,z)=0을 인수분해 하여 근 x_1, y_1과 z_1을 찾는 어려움에 기초를 둔다.

$$b_{i1}x+b_{i2}y+b_{i3}z+b_{i4}|_{x=x_i,y=y_i,z=z_i} > \sum_{j=1}^{i-1}(b_{j1}x+b_{j2}y+b_{j3}z+b_{j4})|_{x=x1,y=y1,z=z1} \pmod p$$

$$(i=2,3,\cdots,n) \quad (9)$$

3.1.2. 암호화

평문은 0-1벡터 $W=(w_1, w_2, \cdots, w_n)$로 나타내고 난수(random numbers) α를 사용하여 암호문의 다항식 C(x,y,z)를 (10)식과 같이 나타내고 암호문의 다항식 계수 C_1, C_2, C_3 와 C_4를 수신자에게 보낸다.

$$C(x,y,z)=B(x,y,z)W+\alpha f(x,y,z) \pmod p$$
$$=C_1x+C_2y+C_3z+C_4 \pmod p \quad (10)$$

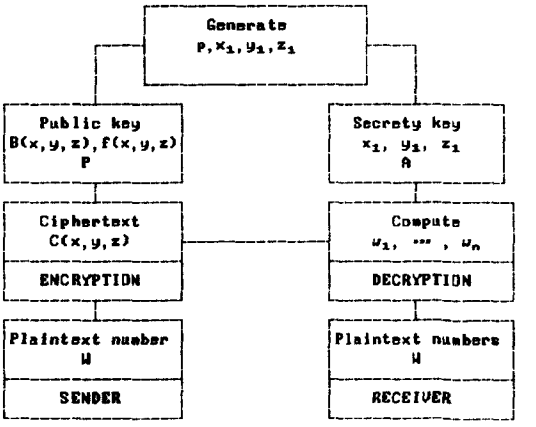
여기서 $C_j=\sum_{i=1}^{n} b_{ij}xw_i+\alpha f_i$ (j=1, 2, 3, 4)이다.

그러므로 송신하고자 하는 n개(n비트)의 평문 벡터 M을 암호화 하면 4개의 십진수로 된 데이터로 변형되어 수신자에게 보내진다.

3.1.3. 해독화

수신자는 수신된 암호문 C(x,y,z)를 해독하기 위하여 먼저 f(x,y,z)=0의 근 x_1, y_1과 z_1을 대입하여 (11)식과 같이 D를 구한다. 제안된 공개키 배낭 암호 알고리즘은 (그림 3)과 같다.

$$D=C(x,y,z)|_{x=x1,y=y1,z=z1} \pmod p$$
$$=\sum_{i=1}^{n} a_{iwi} \pmod p \quad (11)$$



(그림 3) 제안된 공개키 배낭 암호시스템
(Fig. 3) Proposed public key knapsack cryptosystem

3.2. 다항식 지수암호

소인수 분해의 어려움에 기초를 둔 RSA 방

법의 안전성에, 공개키 다항식에 2개의 3변수 다항식을 사용하여, 이 다항식을 동시에 만족하는 근을 구하는 어려움의 안전성을 더함으로써 RSA 방법보다 더 안전성 있는 공개키 암호 알고리즘을 제안한다.

3.2.1. 키 생성

최대 공약수 (3,p-1)=1을 만족하는 소수로써 3개의 변수를 x, y, z로 나타낸다. 단, $0<x_i, y_i, z_i<p$ (i=1,2,3)인 정수 x_i, y_i, z_i을 적당하게 정하고, (12)식을 만족하는 승법 역원(multiplicative inverse element) z_i^{-1}을 구한다.

$$z_i z_i^{-1}=1 \bmod p \tag{12}$$

또한 $0<a_j, b_j<p$ (j=1,2,...,6) 인 정수 a_j, b_j을 적당하게 선택하고, (13)식에서 r_i, r_{i+3}을 구한다.

$$r_i=-(a_i x_i+b_i y_i)z_i^{-1} \bmod p$$
$$r_{i+3}=-(a_{i+3} x_i+b_{i+3} y_i)z_i^{-1} \bmod p \ (i=1,2,3) \tag{13}$$

다음에 2개의 독립된 다항식 f(x,y,z)와 h(x,y,z)을 계산하여 공개한다.

$$f(x,y,z)=\prod_{j=1}^{3}(a_j x+b_j y+r_j z) \bmod p$$
$$=f_1x^3+f_2y^3+f_3z^3+f_4x^2y+f_5x^2z+f_6xy^2+f_7y^2z+ f_8xz^2+f_9yz^2+f_{10}xyz \tag{14}$$

$$g(x,y,z)=\prod_{j=4}^{6}(a_j x+b_j y+r_j z) \bmod p$$
$$=g_1x^3+g_2y^3+g_3z^3+g_4x^2y+g_5x^2z+g_6xy^2+ g_7y^2z+g_8xz^2+g_9yz^2+g_{10}xyz \tag{15}$$

해독키는 x_i, y_i, z_i (i=1,2,3)와 (16)식을 만족하는 d 이다.

$$3d=1 \bmod p-1 \tag{16}$$

그리고 (17)식을 만족하는 승법 역원 $(T_1T_2-T_3T_4)^{-1}$이 비밀키 이다.

$$(T_1T_2-T_3T_4)(T_1T_2-T_3T_4)^{-1}=1 \bmod p \tag{17}$$

여기서, $T_1=x_1z_2-x_2z_1$, $T_2=y_1z_3-y_3z_1$, $T_3=x_1z_3-x_3z_1$, $T_4=y_1z_2-y_2z_1$ 또한 (18)식을 만족하는 승법 역원 T_4^{-1}이 해독키가 된다.

$$T_4T_4^{-1}=1 \bmod p \tag{18}$$

3.2.2. 암호화

3개의 평문 W_i의 범위를 $0\le W_i<p$ (i=1,2,3)로 정하고, 평문 다항식을 (19)과 같이 나타낸다.

$$W(x,y,z)=W_1x+W_2y+W_3z \tag{19}$$

암호화는 평문 다항식 W(x,y,z)을 3승하고, 부등식 $0<a,b<p$ 을 만족시키는 2개의 임의의 수 α, β를 공개키 다항식 f(x,y,z), g(x,y,z)에 각각 곱하여 (20)식과 같은 암호문을 수신자에게 보낸다.

$$C(x,y,z)=W(x,y,z)^3+\alpha f(x,y,z)+\beta g(x,y,z) \bmod p$$
$$=c_1x^3+c_2y^3+c_3z^3+c_4x^2y+c_5x^2z+c_6xy^2+ c_7y^2z+c_8xz^2+c_9yz^2+c_{10}xyz \tag{20}$$

여기서, $c_1=W_1^3+\alpha f_1+\beta g_1 \bmod p$
$c_2=W_1^3+\alpha f_2+\beta g_2 \bmod p$
$c_3=W_1^3+\alpha f_3+\beta g_3 \bmod p$
$c_4=3W_1^2W_2+\alpha f_4+\beta g_4 \bmod p$
$c_5=3W_1^2W_3+\alpha f_5+\beta g_5 \bmod p$
$c_6=3W_1W_2^2+\alpha f_6+\beta g_6 \bmod p$
$c_7=3W_2^2W_3+\alpha f_7+\beta g_7 \bmod p$

$c_8=3W_1W_3^2+\alpha f_8+\beta g_8 \bmod p$

$c_9=3W_2W_3^2+\alpha f_9+\beta g_9 \bmod p$

$c_{10}=6W_1W_2W_3+\alpha f_{10}+\beta g_{10} \bmod p$

3.2.3. 해독화

$f(x,y,z)=g(x,y,z)=0 \bmod p$ 의 근 x_i, y_i, z_i $(i=1,2,3)$을 사용하여

$$D_i(C)=C(x,y,z)|_{x=x_i,\ y=y_i,\ z=z_i} \bmod p \quad (i=1,2,3) \quad (21)$$

을 구하기 위해 다음에 해독키 d를 사용하고,

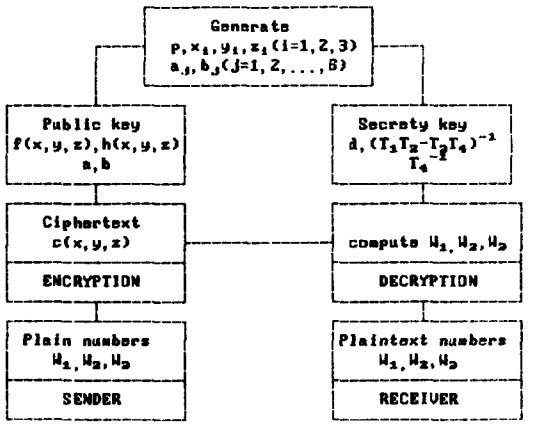
$$\{D_i(C)\}^d \bmod q=W_1x_i+W_2y_i+W_3z_i \quad (i=1,2,3) \quad (22)$$

을 계산한 후, 비밀키의 승법 역원 $(T_1T_2-T_3T_4)^{-1}$ 와 T_4^{-1}을 사용하면 3개의 평문이 (23), (24)와 (25)식에서 구해진다.

$$W_1=[\{D_1(C)^dz_2-D_2(C)^dz_1\}T_2-\{D_1(C)^dz_3-D_3(C)^dz_1\}T_1](T_1T_2-T_3T_4)^{-1} \bmod p \quad (23)$$

$$W_2=[D_1(C)^dz_2-D_2(C)^dz_1-T_1W_1]T_4^{-1} \bmod p \quad (24)$$

$$W_3=[D_1(C)^d-W_1x_1-W_2y_1]z_1^{-1} \bmod p \quad (25)$$



(그림 4) 제안된 공개키 지수 암호시스템
(Fig. 4) Proposed public key exponent cryptosystem

제안된 공개키 지수 암호 알고리즘은 (그림 4)와 같다.

Ⅳ. 시뮬레이션 및 결과 고찰

제안된 공개키 다항식 암호시스템의 타당성을 시뮬레이션에서 사용된 평문을 "THE PUBLIC KEY POLYNOMIAL CRYPTOSYSTEM"으로 하여 송신한다.

배낭 암호시스템에서 암호화 구현방법은 스트림(Stream) 암호로써 사용되는 문자의 2진수 표현은 <표 1>과 같이 각 문자에 대응하는 6비트 2진수로 나타내었다.

〈표 1〉 문자의 2진수 표현
〈Table 1〉 Binary numbers representation of characters

문자	2진수	문자	2진수	문자	2진수	문자	2진수
!	000000	"	000001	#	000010	$	000011
%	000100	&	000101	'	000110	(	000111
)	001000	*	001001	+	001010	,	001011
-	001100	.	001101	/	001110	0	001111
1	010000	2	010001	3	010010	4	010011
5	010100	6	010101	7	010110	8	010111
9	011000	:	011001	;	011010	<	011011
=	011100	>	011101	?	011110		011111
A	100000	B	100001	C	100010	D	100011
E	100100	F	100101	G	100110	H	100111
I	101000	J	101001	K	101010	L	101011
M	101100	N	101101	O	101110	P	101111
Q	110000	R	110001	S	110010	T	110011
U	110100	V	110101	W	110110	X	110111
Y	111000	Z	111001	[	111010	\	111011
]	111100	^	111101	_	111110	`	111111

또한 지수 암호시스템에서 암호화 구현방법은 블록(Block) 암호로써 사용되는 문자의 10진수 표현은 <표 2>와 같이 각 문자에 대응하는 2자리 10진수를 나타내었다.

〈표 2〉 문자의 10진수 표현

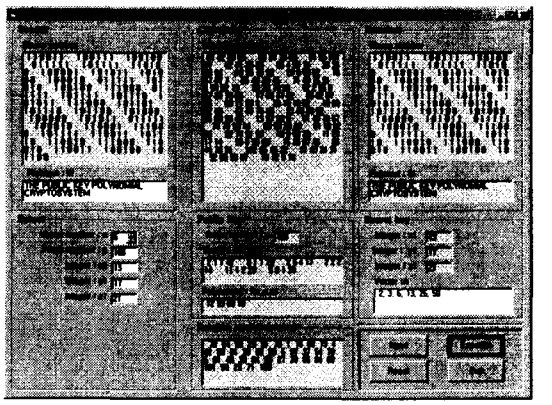
〈Table 2〉 Decimal numbers representation of characters

문자	10진수	문자	10진수	문자	10진수
	00	I	09	R	18
A	01	J	10	S	19
B	02	K	11	T	20
C	03	L	12	U	21
D	04	M	13	V	22
E	05	N	14	W	23
F	06	O	15	X	24
G	07	P	16	Y	25
H	08	Q	17	Z	26

(그림 5)는 키생성에 필요한 자료와 송신문을 입력, 공개키, 비밀키, 암호문, 수신문 등을 나타내주는 공개키 배낭 암호시스템이다. 여기서 벡터 수 n=6, 소수 p=103, 임의의 정수 x_1=13, y_1=17과 z_1=21, 초증가 벡터 A=[2, 3, 6, 13, 25, 50], 다항식 암호 벡터 B=[2 1 1 41, 3 1 1 29, 2 5 4 17, 2 2 2 14, 11 1 2 29, 5 2 1 33], 다항식 f(x,y,z)의 계수 벡터 f=[12 33 68 18]을 나타내고 있다.

(그림 5)에서 송신자가 송신하고자 할 텍스트 평문 "THE PUBLIC KEY POLYNOMIAL CRYPTOSYSTEM"에 송신 2진수 평문(W), 난수(α), 암호문(R), 수신 2진수 평문(W)과 수신 텍스트 평문을 나타내었다. 여기서 송신 2진수 평문은 송신 텍스트 평문에 대하여 <표 1>과 같이 각 문자에 대응하는 6비트 2진수로 나타내었다. 이러한 송신 2진수 평문에 대해 난수 α와 암호 알고리즘을 적용하면 10진수의 암호문 C가 얻어진다. 암호문 C를 수신자에게 보내면 수신자는 공개키와 비밀키를 사용하여 암호문을 해독하여 수신 2진수 평문(W)을 얻는다. 그리고 <표 1>과 같이 6비트 2진수에 대응시키면 수신 텍스트 평문 "THE PUBLIC KEY POLYNOMIAL CRYPTOSYSTEM"을 얻는다.

그리고 텍스트 평문의 첫 번째 문자 "T"를 6비트 2진수로 바꾸면 "110011'와 같은 송신 2진수 평문이 되며, 난수 α=72와 암호 알고리즘을 적용하면 암호문 "61 12 60 89"가 얻어진다. 암호문을 수신자가 해독하면 수신 2진수 평문 "110011"을 얻고 수신 텍스트 평문으로 바꾸면 송신한 문자 "T"를 얻는다. 또한 송신 텍스트 평문에서 세 번째 문자 "E"와 열세 번째 문자 "E"에 대하여 암호화하는 데 사용되는 난수 α가 각각 59, 88과 같이 서로 다르므로 암호문도 " 94 96101 87", "30 23 13 94"와 같이 각각 다르게 되어 해독이 어렵게 된다.



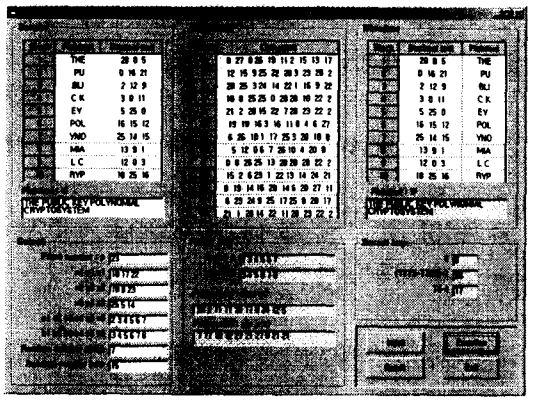
(그림 5) 배낭 암호시스템의 시뮬레이션 결과

(Fig. 5) Simulation result of knapsack cryptosystem

(그림 6)은 키생성에 필요한 자료와 송신문을 입력, 공개키, 비밀키, 암호문, 수신문 등을 나타내주는 공개키 지수 암호시스템이다. 여기서 소수 p=23, 정수 x_i, y_i, z_i, a_i, b_i, 난수 α=7, β=15, 다항식 공개키 벡터 f=[24 2 11 11 24 17 0 24 12 5], g=[7 17 18 12 27 21 27 0 21 21] 등을 나타내고 있다.

(그림 6)과 같이 평문의 문자들을 <표 2>와 같이 " "=00, A=01, B=02, C=03,...,Z=26으로 대

응시키고, 송신문 "THE PUBLIC KEY POLYNOMIAL CRYPTOSYSTEM"에서 3개 문자를 하나의 블록으로 하면, 원래의 평문이 "THE"인 경우 10진수는 "20 8 5"가 된다.



(그림 6) 지수 암호시스템의 시뮬레이션 결과
(Fig. 6) Simulation result of exponent cryptosystem

임의의 정수 α=7, β=15로 선택하면, (20)식에 의해 암호 벡터 C=[8 27 8 26 19 11 2 15 13 17]와 같이 구해진다. 이 암호 벡터를 수신자에게 보내면, 수신자는 암호 벡터 C를 (21)식-(25)식을 이용하여 해독하면 10진수의 평문 "20 8 5"이 구해지고, 문자로 표현하면 송신자가 보낸 평문 "THE"가 얻어진다. 또한 블록별 10진 송신문, 암호문, 10진 수신문, 수신문 등을 나타내고 있다. 문자 3자를 하나의 블록으로 지정하므로 "THE", " PU", "BLI", "C K", "EY ", "POL", "YNO", "MIA", "L C", "RYP", "TOS", "YST", "EM" 등 13개의 블록으로 표현된다.

<표 3>은 배낭암호와 지수암호에 대한 공개키 및 비밀키의 벡터, 다항식, 정수 등을 나타낸다.

〈표 3〉 공개키 및 비밀키
〈Table 3〉 The public key and secret key

배낭암호	공개키	소수	v=97
		암호벡터	B=[2 1 1 41, 3 1 1 29, 2 5 4 17, 2 2 2 14, 11 1 2 29, 5 2 1 33]
		다항식 계수벡터	f=[12 33 68 77]
	비밀키	초증가 벡터	A=(2, 3, 6, 13, 25, 50)
		정수	$x_1=13$, $y_1=17$, $z_1=21$
지수암호	공개키	암호벡터	a=[2 3 4 5 6 7], b=[3 4 5 6 7 8]
		다항식 계수벡터	f=[24 2 11 11 24 17 0 24 12 5] g=[7 17 18 12 27 21 27 0 21 21]
	비밀키	정수	d=19, $(T_1T_2-T_3T_4)^{-1}=28$, $T_4^{-1}=17$

또한 제안된 배낭 암호시스템은 초증가 벡터를 변형하여 다항식을 표현하고 그것을 이용하여 암호화 된 것에 난수를 곱한 공개키 다항식을 가한 것을 암호문으로 하였기 때문에, 이 암호의 안전성은 공개키 다항식 f(x,y,z)=0를 인수분해하여 근을 구하는 데 어려움이 있다. 그리고 지수 암호시스템은 공개키 다항식에 2개의 3변수 다항식을 사용하여, 이 다항식을 동시에 만족하는 근을 구하는 어려움에 안전성을 두고 있다.

V. 결론

본 논문은 3변수 다항식의 인수분해의 어려움 때문에 컴퓨터 통신의 안전성을 갖는 공개키 배낭 암호시스템과 공개키 지수 암호시스템을 제안하였다.

첫째 공개키 배낭 암호시스템은 MH 배낭 암

호의 초증가 벡터 A를 변형하여 다항식 표현하고, 그것을 사용하여 암호화 된 것에, 난수를 곱한 공개키 다항식을 가한 것을 암호문으로 하였다. 이 암호의 안전성은 다항식 벡터 B(x,y,z)의 각 변수에 공개키 다항식 f(x,y,z)=0의 근을 대입할 때 공개키 다항식 f(x,y,z)=0을 인수분해하여 근 x, y와 z를 구하는 데 어려움이 있다. 그러므로 초증가 벡터 A의 요소들의 합으로부터 부분 집합을 찾아내는 데 어려움이 있는 MH 배낭 암호의 안전성에 공개키 다항식의 근을 구하는 어려움의 안전성을 더함으로써 MH 배낭 암호보다 안전성이 있는 공개키 배낭 암호시스템으로 되었다.

둘째 공개키 지수 암호 알고리즘은 공개키 다항식에 2개의 3변수 다항식을 사용하여, f(x,y,z)=g(x,y,z)=0을 동시에 만족하는 근을 인수분해하여 구하는 어려움에 대한 안전성을 기초로 두었다. 암호문은 평문 다항식을 3승하여, 그것에 2개의 공개키 다항식을 각각 임의의 정수를 곱하여 더한 것을 암호문으로 하였으며, 비록 암호문의 길이는 평문 길이의 약 10/3배가 되나, 이 암호는 소인수분해의 어려움을 이용한 RSA 공개키 방법에, 다항식의 인수분해의 어려움을 부가하여 RSA 방법보다 더 안전성을 가진 암호로 되었다. 컴퓨터 시뮬레이션을 통해 주어진 문자 평문에 대하여 암호화 하고 해독하여 제안된 공개키 배낭 암호시스템과 공개키 지수 암호시스템의 타당성이 입증되었다.

참고문헌

[1] C. S. Kline and G. J. Popek, *Public Key vs. Conventional Key Encryption*, National Computer Conference, 1979, pp. 831-837.

[2] D. B. Newman, et al., Public key management for network security, *IEEE Network Magazine, Vol.1,* No.2, pp. 11-16, April 1987

[3] W. Diffie and M. E. Hellman, New direction in cryptography, *IEEE Trans. Inform. Theory, Vol.IT-22,* Nov. 1976, pp. 644-654.

[4] R. L. Rivest, A. Shamir and L. Adleman, A method for obtaining digital signatures and public key cryptosystem, *Comm. ACM, Vol.21,* No.2, 1978, pp. 120-126.

[5] R. C. Merkle and M. E. Hellman, Hiding information and signatures in trapdoor knapsacks, *IEEE Trans. Info. Theory, Vol. IT-24,* 1978.

[6] B. Chor and R. L. Rivest, A knapsack-type public ley cryptosystem based on arithmetic in finite fields, *IEEE Trans. Inf. Theory, Vol.34,* No.5, 1988, pp. 901-909.

[7] T. Elgamal, A public key cryptosystem and a signature scheme based on discrete logarithms, *IEEE Trans. Inf. Theory, Vol.IT-31,* No.4, 1985, pp. 469-472.

[8] S. Tsujii, A. Fujioka and Y. Hirayama, Generalization of the public-key cryptosystem based on the difficulty of solving a system of non-linear equations, *電子情報通信學會論文誌, Vol.J72-A,* No.2, Feb. 1989, pp. 390-389.

The Public Key Polynomial Cryptosystem for Data Security in Communication Networks

Tae-Kyu Yang*

Abstract

In this paper, a public key knapsack cryptosystem algorithm is based on the security to a difficulty of polynomial factorization in computer communication is proposed.

For the proposed public key knapsack cryptosystem, a polynomial vector B(x,y,z) is formed by transform of superincreasing vector A, a polynomial f(x,y,z) - is selected. Next then, the two polynomials B(x,y,z) and f(x,y,z) is decided on the public key. Therefore a public key knapsack cryptosystem is based on the security to a difficulty of factorization of a polynomial f(x,y,z)=0 with three variables.

In this paper, a public key encryption algorithm for data security of computer network is proposed. This is based on the security to a difficulty of factorization. For the proposed public key encryption, the public key generation algorithm selects two polynomials f(x,y,z) and g(x,y,z).

The propriety of the proposed public key cryptosystem algorithm is verified with the computer simulation.

* School of IT Engineering, Mokwon University