論 文

컴퓨터 통신의 안전을 위한 공개키 배낭 암호계 앨고리듬

正會員 李 榮 魯* 正會員 申 仁 澈**

A Public Key knapsack Crytosystem Algorithm for Security in Computer Communication

Young No LEE* In Chul SHIN** *Regular Members*

要 約 본 논문에서는 컴퓨터 통신의 안전을 위해서 다항식을 인수분해하는 데 어려움이 있는 공개키 배낭 암호계 앨고리듬을 제안하였다.

제안된 공개키 배낭 암호계에서 초증가 벡터 A를 변환하여 다항식 벡터 B(x,y,z)를 형성하고, 다항식 f(x,y,z)를 선택한다. 이러한 두개의 다항식 B(x,y,z)와 f(x,y,z)를 공개키로 한다. 암호화는 처음에 평문 벡터 M을 선택하고, 공개키 다항식 B(x,y,z), f(x,y,z)와 난수 α를 사용하여 암호문 C(x,y,z)를 계산하여 수신자에게 보낸다. 암호문 C(x,y,z)의 해독은 f(x,y,z)=0의 근 x, y와 z, 그리고 비밀키 벡터의 초증가성을 사용하면 평문 M이 구해진다. 따라서 3변수 다항식 f(x,y,z)=0의 인수분해의 어려움 때문에 안전성을 갖는 공개키 배낭 암호계로 된다. 제안된 공개키 배낭 암호계 앨고리듬의 타당성이 컴퓨터 시뮬레이션을 통하여 입증되었다.

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. The enciphering first selects plaintext vector M. Then the ciphertext C(x,y,z) is computed using the public key polynomials and a random integer α. For the deciphering of ciphertext C(x,y,z), the plaintext M is determined using the roots x, y, z of a polynomial f(x,y,z)=0 and the increasing property of secrety key vector. 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. The propriety of the proposed public key knapsack cryptosystem algorithm is verified with the computer simulation.

I. 서 론

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

통신 매체를 통한 정보 교환 및 자원 공유와 관련하여 정보의 양적 증가와 부대 가치의 증가라는 측면에서 정보를 생성 가공하여 사용자의 위치까지 전파하는 기술은 이제 괄목할 만한 발전을 이루었다. 그러나 고도의 정보 통신 기술의 발전은 이와같은 긍정적인 측면 외에 정보의 내용 변경, 정보의 불법적인 유출, 순서 변경 그리고 미확인 송신자 및 수신자 등에 의하여 항상 위협을 받음으로써 정보의 안전성이 요구되고 있는 실정이다.

암호화 기법(cryptography)은 메세지를 받도록 된 사람에게만 그 메세지를 이해하도록 하고, 그와 다른 사람들이 그 메세지를 이해하지 못하도록 하기 위해 메세지를 변형시키는 기술이다.

* 서울産業大學 電子工學科
Dept. of Electronic Engineering, Seoul National Polytech. Univ.
** 檀國大學校 電子工學科
Dept. of Electronic Engineering, Dankook University
論文番號 : 91-83(接受1991. 6. 10)

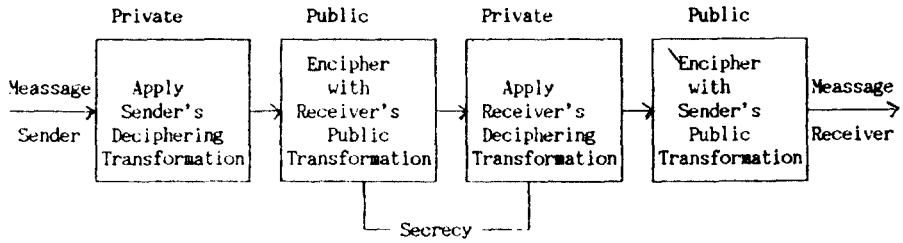


그림 1. 공개키 암호계를 사용한 안전
Fig. 1. Secrecy using public key cryptosystems

[1] 데이타가 통신 선로를 경유하여 이동할 때 다른 이용자 들이 도청하여 해독하기 어렵게 하는 데이타의 여러가지 암호화 기법은 크게 전통적인 암호계(conventional cryptosystem)와 공개키 암호계(public key cryptosystem)로 나눌 수 있다.[2][3] 공개키 암호의 대표적인 RSA[4] 암호는 큰 합성수의 소인수 분해의 어려움에 안전성의 근거를 가지고 있으며, Elgamal[5]은 이산적 대수 문제의 어려움에 대한 안전성을 가지고 있다. 다른 하나는 1976년 Diffie와 Hellman[6]이 제안한 배낭(Knapsack) 암호계이다. 이것은 송신자와 수신자가 각각 2개의 키 즉, 하나의 개인키, 하나의 공개키를 사용하는 암호계이다. 송신자와 수신자는 각자의 다른 공개키를 알고 통신하므로 키 분배는 요구되지 않는다.

송신자와 수신자는 그림 1과 같이 공개 해독 변환과 비밀 암호 변환을 하며, 비밀변환은 하나의 비밀키를 사용하여 변환하고, 공개 변환은 매우 많은 계산시간이 걸리는 단방향 변환인 비밀키로 생성되는 하나의 공개키를 사용한다.

본 논문에서는 3변수 다항식 $f(x,y,z)=0 \pmod p$의 근을 구하기 어려움, 즉 다항식의 인수분해의 어려움 때문에 안전성을 갖는 공개키 배낭 암호계를 제안한다.

MH 배낭(Knapsacks) 암호계의 초증가 벡터 A를 다항식 표현하고, 그것에 난수(random number) 를 곱한 후 공개키 다항식을 더한 것을 암호문으로 한다. 이 암호의 안전성은 다항식 암호 벡터 B(x,y,z)가 초증가 벡터로 되므로 공개키 다항식 f(x,y,z)가 초증가 벡터로 되므로 공개키 다항식 $f(x,y,z)=0 \pmod p$의 근을 구하는 데 어려움이 있다. 해독은 f(x,y,z)의 근 x, y와 z를 대입하고 벡터의 초증가성을 이용하면 평문이 구해진다. 시뮬레이션을 통해 주어진 문자 평문에 대하여 암호화 하고 해독하여 제안된 공개키 배낭 암호계의 타당성을 입증한다.

Ⅱ. 키 분배와 공개키 암호

Ⅱ.1 전통적인 암호계

전통적인 암호계는 그림 2와 같이 단일키 암호화 방식으로 통신하고자 하는 사용자 사이에 연결된 회선상으로 정보를 전송하는 과정에서 정보의 노출을 막기 위하여, 사용자가 공통적으로 갖고 있는 단일키로 암호화하고 해독하는 시스템이다.

여기서 K는 비밀키, M은 암호화 되지 않은 평문, C는 암호화된 암호문, M는 도청자(eav-

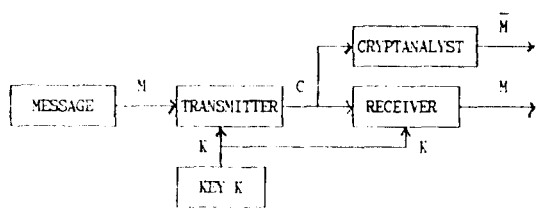


그림 2. 전통적인 암호계
Fig. 2. Conventional cryptosystem

esdropper) 가 얻은 평문이다.

전통적인 암호계에서는 송신자와 수신자가 동시에 동일한 키를 가져야 하므로 어느 한 쪽에서 반드시 상대방에게 약속된 키를 보내야 하는데, 이 과정에서 키가 노출될 수도 있다는 것이 전통적이 암호계의 가장 큰 단점이다.[7]

Ⅱ.2 공개키 암호계

전통적인 암호계의 단점은 1976년에 최초로 Diffie와 Hellman[6]에 의해 제안된 공개키 암호계의 개념으로서 해결될 수 있게 되었다. 이러한 공개키의 제안에 뒤이어 1976년 Rivest, Shamir와 Adlemand[4]에 의해 지수승 암호인 RSA법이 제안되었고, Merkle와 Hellman[8], Chor[9] 등에 의해 배낭 문제(Knapsack problem)를 사용한 MH법 등이 제안되었다.

이 암호계는 그림 3과 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.

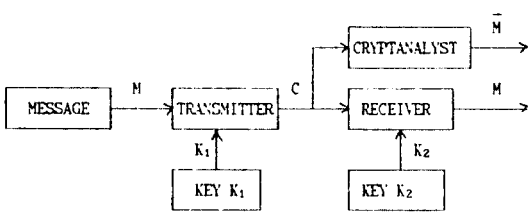


그림 3. 공개키 암호계
Fig. 3. Public key cryptosystem

또한 전통적인 암호계에서 정보 통신을 하는 사람의 수가 n이라 하면 이용해야 하는 키의 갯수는 $n(n-1)/2$, 즉 키의 갯수는 n^2에 비례하나 공개키 암호계에서는 단방향 함수(one-way function)을 이용하여 키의 갯수는 n에 비례한다.[10]

Ⅱ.3 배낭 암호계

배낭 암호계는 주어진 정수 $a_1, a_2, \cdots, a_n$의 집합과 이것의 합 S로 부터, 집합 $\{a_1, a_2, \cdots, a_n\}$의 부분 집합을 찾는 어려움에 기초를 두어 안전성을 갖게 한다.

결과적으로 $\sum_{i=1}^{n} x_i a_i = S$을 만족하는 0-1벡터(벡터의 요소가 0 또는 1인 벡터), 즉 배낭의 하중집합$(x_1, x_2, \cdots, x_n)$을 찾아내는 것이다.

배낭 암호계에서 암호 문제를 사용하기 위한 기본적인 방법의 단계는 다음과 같다.

단계 1. 공개키 : 정수 $a_1, a_2, \cdots, a_n$
단계 2. 비밀키 : $a_1, a_2, \cdots, a_n$을 변형
단계 3. 메세지 : n차원 0-1벡터$(x_1, x_2, \cdots, x_n)$
단계 4. 암호 : $\sum_{i=1}^{n} x_i a_i = S$
단계 5. 해독 : 벡터$(a_1, a_2, \cdots, a_n)$와 합 S로 배낭 문제를 해결

Merkle와 Hellman[8]은 (1)식을 만족하는 초증가(superincreasing) 수열 $b_1, b_2, \cdots, b_n$을 사용함으로써 배낭 문제를 쉽게 해결하는 방법을 제안하였다.

$$b_j > \sum_{i=1}^{j-1} b_i \quad (1 \leq j \leq n) \tag{1}$$

또한 조건식 $M > \sum_{i=1}^{n} b_i$를 만족시키는 M, W와 M의 인수가 1이 되는 W를 정하여 (2)식과 같이 초증가 수열 $b_1, b_2, \cdots, b_n$에 나머지 곱을 하여 a_i로 변형한다.

$$a_i = b_i W \pmod{M} \tag{2}$$

그러므로 배낭 문제 $\sum_{i=1}^{n} x_i a_i = S$에 대한 해 $(x_1, x_2, \cdots, x_n)$는 $\sum_{i=1}^{n} x_i a_i = S'$에 대한 해 $(x_1, x_2, \cdots, x_n)$와 같게 된다. 여기서 $S' = SW^{-1} \pmod{M}$과 $0 \leq S' < M$이다. 따라서 $\sum_{i=1}^{n} x_i b_i = S'$로 부터 원래의 메세지 0-1벡터 $(x_1, x_2, \cdots, x_n)$이 구해진다.

Ⅲ. 제안된 공개키 배낭 암호계

주어진 정수의 집합과 이 집합의 원소들의

합으로 부터, 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.

Ⅲ.1 키 생성

먼저 배낭 암호의 키생성 순서로써, (3)식을 만족시키는 초증가 벡터 $A=(a_1, a_2, \cdots, a_n)$을 정의한다.

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

그리고 조건식 $p > \sum_{i=1}^{n} a_i$을 만족시키는 소수(prime number) p를 정한 후, $0 < x_1, y_1, z_1 < p$를 만족시키는 임의의 정수 x_1, y_1와 z_1을 선택하여 $x=x_1$, $y=y_1$과 $z=z_1$로 한다. 다음에 (4)식을 만족하도록 초증가 벡터의 요소(element) a_i을 적당하게 a_{i1}, a_{i2}와 a_{i3}로 3분할하여 표현한다.

$$a_i = a_{i1} + a_{i2} + a_{i3} \pmod{p} \tag{4}$$

(4)식에서 우변의 각 항을 변수 x, y와 z을 사용하여 (5)식과 같이 변형한다.

$$\begin{aligned} a_{i1} &= b_{i1}x + r_{i1} \pmod{p} \\ a_{i2} &= b_{i2}y + r_{i2} \pmod{p} \\ a_{i3} &= b_{i3}z + r_{i3} \pmod{p} \end{aligned} \tag{5}$$

여기서 r_{i1}, r_{i2}와 r_{i3}는 나머지이고, 이 나머지의 합을 (6)식과 같이 b_{i4}로 표현한다.

$$b_{i4} = r_{i1} + r_{i2} + r_{i3} \pmod{p} \tag{6}$$

따라서 초증가 벡터의 요소 a_i가 (5)식과 (6)식과 같이 다항식으로 표현된다. 이러한 다항식을 사용하여 배열 순서를 적당하게 변환하여 (7)식과 같이 다항식 벡터 B(x, y, z)을 표현한 후 암호 벡터로써 공개한다. 그러므로 초증가 벡터 A의 요소가 n개인데 비해서 다항식 벡터 B(x, y, z)의 계수는 4Xn개로 된다.

$$\begin{aligned} B(x,y,z) = (&b_{11}x + b_{12}y + b_{13}z + b_{14} + b_{21}x + b_{22}y + b_{23}z + b_{24}, \cdots, \\ &b_{n1}x + b_{n2}y + b_{n3}y + b_{n3}z + b_{n4}) \end{aligned} \tag{7}$$

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

$$0 < f_1, f_2, f_3 < p \tag{8}$$

또한 공개키 다항식의 계수는 f_4는 (9)식과 같이 구한다.

$$f_4 = -f_1x_1 - f_2y_1 - f_3z_1 \pmod{p} \tag{9}$$

따라서 (8)식과 (9)식에서 나타낸 계수 f_1, f_2, f_3와 f_4를 이용하여 (10)식과 같은 공개키 다항식 f(x,y,z)를 공개한다.

$$f(x,y,z) = f_1x + f_2y + f_3z + f_4 \tag{10}$$

MH 배낭 암호계는 초증가 벡터 A를 공개하나 본 논문에서는 소수 p를 공개하고, 초증가 벡터 A를 변환하여 다항식 벡터 B(x,y,z)로 표현된 것을 공개하고, 또한 다항식 f(x,y,z)를 선택하여 공개한다. 이것이 제안된 배낭 암호계가 MH 배낭 암호계와 다른점이며, 이 암호의 안전성은 다음의 조건식 (11)식을 만족시키는 다항식 $f(x,y,z)=0 \pmod{p}$을 인수분해하여 근 x_1, y_1과 z_1을 찾는 어려움에 기초를 둔다.

$$\begin{aligned} &b_{i1}x + b_{i2}y + b_{i3}z + b_{i4} \neq \sum_{j=1}^{i-1} (b_{j1}x + b_{j2}y + b_{j3}z + b_{j4}) \pmod{p} \\ &(i=2, 3, \cdots, n) \end{aligned} \tag{11}$$

Ⅲ.2 암호

평문은 0 1벡터 $M=(m_1, m_2, \cdots, m_n)$으로 나타내고 난수(random numbers) α를 사용하여

암호문의 다항식 C(x,y,z)를 (12)식과 같이 나타내고 암호문의 다항식 계수 C_1, C_2, C_3와 C_4를 수신자에게 보낸다.

$$C(x,y,z)=B(x,y,z)M+\alpha f(x,y,z) \pmod p$$
$$\sum_{i=1}^{n}(b_{i1}x+b_{i2}y+b_{i3}z+b_{i4})m_i$$
$$+\alpha(f_1x+f_2y+f_3z+f_4) \pmod p$$
$$=C_1x+C_2y+C_3z+C_4 \pmod p \qquad (12)$$

여기서 $C_j=\sum_{i=1}^{n} b_{ij}xm_i+\alpha f_1(j=1, 2, 3, 4)$이다.

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

Ⅲ.3 해독

수신자는 수신된 암호문 C(x,y,z)를 해독하기 위하여 먼저 f(x,y,z)=0 (mod p)의 근 x_1, y_1과 z_1을 대입하여 (13)식과 같이 D를 구한다.

$$D=C(x,y,z)|_{x=x1,\ y=y1,\ z=z1} \pmod p$$
$$=\sum_{i=1}^{n}(b_{i1}x+b_{i2}y+b_{i3}z)m_i|_{x=x1,\ y=y1,\ z=z1} \pmod P$$
$$=\sum_{i=1}^{n}a_im_i \pmod p \qquad (13)$$

다음에 비밀키 벡터 A의 초증가성을 사용하여 다음과 같은 앨고리듬으로 평문 $M=(m_1, m_2, \cdots, m_n)$이 구해진다. 제안된 공개키 배낭 암호계의 블럭선도는 그림 4와 같다.

단계 1. i=0

단계 2. 만약에 $a_{n-1}>D$이면 $m_{n-1}=0$, $D=D-a_{n-1}$ 그렇지 않으면 $m_{n-1}=1$

단계 3. 만약에 i=n−1이면 정지

단계 4. i=i+1

단계 5. 단계 2번으로 가라.

Ⅳ. 시뮬레이션 및 결과고찰

주어진 문자 평문에 대하여 암호화 하고 해독하여 제안된 공개키 배낭 암호계의 타당성을 입증하기 위해 시뮬레이션을 한다.

먼저 초증가 벡터 A=(2, 3, 6, 13, 25, 50)를 정의하고, 솟수 p=103으로 선택하고, 임의의 정수 x_1=11, y_1=6과 z_1=44로 정한 후 초증가 벡터 A를 요소 a_i를 다음과 같이 변형한다.

$$A=(32+33+40,\ 43+23+40,\ 28+94+90,$$
$$33+38+45,\ 145+31+55,\ 73+47+33) \pmod{103}$$

변수 x, y와 z를 이용한 다항식 암호 벡터 B(x, y, z)를 다음과 같이 표현한 후 암호 벡터로써 공개한다.

$$B(x,y,z)=(2x+5y+0z+53,\ 3x+3y+0z+55,$$
$$2x+15y+2z+12,\ 3x+6y+z+3,\ 13x+5y+z+14,\ 6x+7y+0z+45)$$

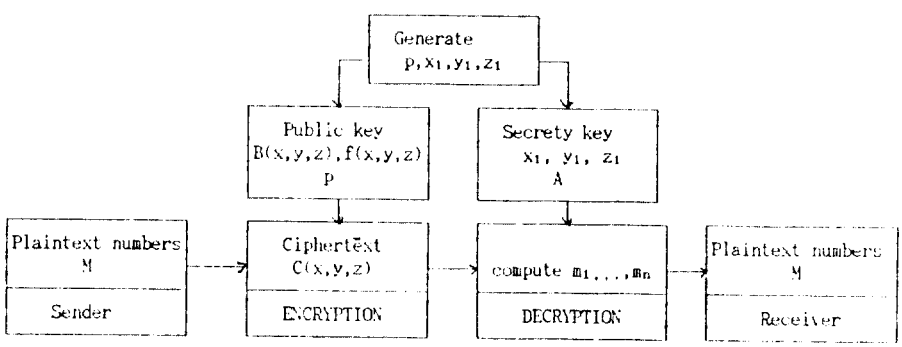


그림 4. 제안된 공개키 배낭 암호계
Fig. 4. Proposed public key knapsack cryptosystem

또한 다항식 f(x,y,z)의 계수를 t_1=12, t_2=33과 f_3=68로 정하면 f_4=77이 되므로 공개키 다항식은 f(x,y,z)=12x+33y+68z+77로 된다.

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

!	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

평문의 문자들을 표 1과 같이 6비트 2진수로 표현한다. 만일 문자 "K"인 경우 6비트 2진수는 "101010"와 같으면 문자 "C"에 대한 평문의 데이타는 M=(1,0,1,0,1,0)이 된다. 난수 α=12로 선택하면 암호문은 (12)식에서 다음과 같이 구해진다.

$$C(x,y,z)=(2x+5y+0z+53)+(2x+5y+2z+12)+(13x+5y+z+14)+12(12x+33y+68z+77) \pmod{103}$$
$$=58x+9y+982+76 \pmod{103}$$

해독은 먼저 (13)식에서 D를 구하면 다음과 같다.

$$D=C(x,y,z)_{(x=11,\ y=6,\ z=44)} \pmod{103}=33$$

a_6=50>33이므로 m_6=0, a_6=25≦33이므로 m_5=1, D=D-a_5 a_4=13>8이므로 m_4=0, a_3=6<8이므로 m_3=1, D=D-a_3, a_2=3>2이므로 m_2=0, a_1=2≦2이므로 m_1=1, D=D-a_1, 그러므로 D=0가 되어 평문 M=(1,0,1,0,1,0)이 얻어진다.

표 2는 송신자가 송신하고자 한 텍스트 평문 "KNAPSACK CRYPTOSYSTEM."에 대한 공개키(p, B, f), 비밀키(A, x_1, y_1, z_1), 송신 2진수 평문(M), 난수(α), 암호문 (C), 수신 2진수 평문(M)과 수신 텍스트 평문을 나타내었다. 여기서 송신 2진수 평문은 송신 텍스트 평문 "KNAPSACK CRYPTOSYSTEM."에 대하여 각 문자에 대응하는 6비트 2진수로 나타내었다. 이러한 송신 2진수 평문에 대해 난수 α와 암호 알고리듬을 적용하면 암호문 C가 얻어진다. 암호문 C를 수신자에게 보내면 수신자는 공개키와 비밀키를 사용하여 암호문을 해독하면 표 2의 수신 2진수 평문(M)을 얻는다. 그리고 표 1과 같이 6비트 2진수에 대응시키면 수신 텍스트 평문 "KNAPSACK CRYPTOSYSTEM."을 얻는다.

그리고 표 2에서 송신 텍스트 평문 "KNAPSACK CRYPTOSYSTEM."의 첫번째 문자 "K"를 6비트 2진수로 바꾸면 "101010"와 같은 송신 2진수 평문(M)이 되며 난수 α=12와 암호 알고리듬을 적용하면 암호문 "58 9 98 76"가 얻어진다. 암호문을 수신자가 해독하면 수신 2진수 평문(M) "101010"을 얻고 수신 텍스트 평문으로 바꾸면 송신한 문자 "K"을 얻는다.

또한 표 2에서 송신 텍스트 평문 "KNAPSACK CRYPTOSYSTEM."에서 "KNAPSACK"에 있는 문자 "P"와 "CRYPTOSYSTEM."에 있는 문자 "P"에 대하여 암호화하는 데 사용되는 난수 α가 각각 75, 100과 같이 서로 다르므로 암호문도 "102 41 57 31", "93 42 6 102"와 같이 각각 다르게 되어 해독이 어렵게 된다.

제안된 배낭 암호계는 MH 배낭 암호의 초증가 벡터를 변형하여 다항식 표현하고 그것을 이용하여 암호화 된 것에 난수를 곱한 공개키 다항식을 가한 것을 암호문으로 하였기 때문에, 이 암호의 안전성은 다항식 벡터 B(x,y,z)의 각 변수에 공개키 다항식 f(x,y,z)=0 (mod p)

표 2. 암호계 데이타
Table 2. Cryptoststem data

Public Key P	103			
B	2	5	0	53
	3	3	0	55
	2	15	2	12
	3	6	1	3
	13	5	1	14
	6	7	68	45
f	12	33		77
Secrety Key A	2 3	6	13 25	50
x_1, y_1, z_1	11	6	44	
Sender Text	KNAPSACK CRYPTOSYSTEM.			
Plaintext Numbers	101010	101101	100000	101111
(Sender)	110010	100000	100010	101010
	011111	100010	110001	111000
	101111	110011	101110	110010
	111000	110010	110011	100100
	101100	001101		
Random Numbers	12	67	89	75
α	82	7	50	46
	11	97	72	54
	100	33	98	96
	55	58	69	72
	76	68		
Ciphertext	58 9 98 76	96 81 27 19	40 58 78 5	102 41 57 31
	75 41 15 50	86 30 64 77	100 12 2 3	54 101 41 16
	56 90 31 49	46 18 5 17	51 22 55 32	37 54 69 55
	93 42 6 102	8 79 82 30	63 72 76 6	37 91 40 98
	49 87 34 29	96 73 31 56	28 31 58 21	45 18 56 38
	95 62 21 49	3 6 95 43		
Plaintext Number	101010	101101	100000	101111
(Receiver)	110010	100000	100010	101010
	011111	100010	110001	111000
	101111	110011	101110	110010
	111000	110010	110011	100100
	101100	001101		
Receiver Text	KNAPSACK CRYPTOSYSTEM.			

의 근을 대입할 때 공개키 다항식 f(x,y,z)=0 (mod p)을 인수 분해하여 근을 구하는 데 어려움이 있다.

V. 결 론

본 논문은 3변수 다항식 f(x,y,z)=0의 인수분해의 어려움 때문에 컴퓨터 통신의 안전성을 갖는 공개키 배낭 암호계 알고리듬을 제안하였다.

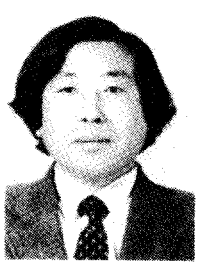
MH 배낭 암호의 초증가 벡터 A를 변형하여 다항식 표현하고, 그것을 사용하여 암호화 된 것에, 난수를 곱한 공개키 다항식을 가한 것을 암호문으로 하였다. 이 암호의 안전성은 다항식 벡터 B(x,y,z)의 각 변수에 공개키 다항식 f(x,y,z)=0의 근을 대입할 때 공개키 다항식 f

(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 암호계로 되었다. 시뮬레이션을 통해 주어진 문자 평문에 대해 제안된 공개키 배낭 암호계의 타당성을 입증하였다.

참 고 문 헌

1. W. Diffie and M. Hellman, "Privacy and Authentication : An Introduction to Cryptography", Proc. IEEE, Vol. 67, pp. 397-527, Mar. 1979.
2. M. E. Hellman, "An Overview of Public Key Cryptography", IEEE Communication Society Magazine, pp. 24-32, Nov. 1978.
3. C. S. Kline and G. J. Popek, "Public Key vs. Conventional Key Encryption", National Computer Conference, pp. 831-837, 1979.
4. R. L. Rivest, A. Shamir and L. Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystem", Comm. ACM, Vol. 21, pp. 120-126, Feb. 1978.
5. T. Elgamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms", IEEE Trans. Inform. Theory, Vol. IT-31, pp. 469-472, July 1985.
6. W. Diffie and M. E. Hellman, "New Direction in Cryptography", IEEE Trans. Inform. Theory, Vol. IT-22, pp. 644-654, Nov. 1976.
7. C. H. Meyer and S. M. Matyas, Cryptography : A New Dimension in Computer Data Security, John Wiley & Sons, 1982.
8. R. C. Merkle and M. E. Hellman, "Hiding Information and Signatures in Trapdoor Knapsacks", IEEE Trans. Inform. Theory, Vol. IT-24, pp. 525-530, Sept. 1978.
9. B. Chor and R. L. Rivest, "A Knapsack-Type Public Key Cryptosystem Based on Arithmetic in Finite Fields", IEEE Trans. Inform. Theory, Vol. 34, pp. 901-909, Sep. 1988.
10. D. B. Newman, Jr., et al., Public Key Managemant for Network Security, IEEE Network Magazine, Vol. 1, pp. 11-16, April 1987.



李 榮 魯(Young No LEE) 正會員

1936年 1月 9日生

- 檀國大學校 電子工學科 卒業(工學士)
- 建國大學校 電氣 및 電子工學科 卒業(工學碩士)
- 檀國大學校 電子工學科 博士課程 修了
- 現在 國立 水産産業大學 電子工學科 副教授
- 關心分野 : 信號處理 및 COMPUTER NETWORK

申 仁 澈(In Chul SHIN) 正會員

1949年 11月 5日生

- 高麗大學校 電子工學科 工學士
- 高麗大學校 大學院 電子工學科 工學碩士
- 高麗大學校 大學院 電子工學科 工學博士
- 現在 : 美國 미시간주립大學 컴퓨터工學科客員 敎授.
  現在 : 檀國大學校 電子工學科 副教授
- 關心分野 : 信號處理 및 Computer Network