정보학연구 제5권 제4호 2002년 12월(pp.129-137)
The Journal of Information Technology, Vol.5, No.4

컴퓨터 통신 네트워크의 보안성을 위한 공개키 배낭 암호시스템에 대한 연구

양태규*

요 약

본 논문에서는 컴퓨터 통신 네트워크의 데이터 안전을 위해서 다항식을 인수분해 하는 데 어려움이 있는 공개키 다항식 배낭 암호시스템 알고리즘을 제안하였다. 제안된 공개키 다항식 배낭 암호시스템은 먼저, 초증가 벡터 P를 변환하여 다항식 벡터 Q(x,y,z)를 형성하고, 다항식 g(x,y,z)를 선택한다. 이러한 두개의 다항식 Q(x,y,z)와 g(x,y,z)를 공개키로 한다. 공개키 다항식 Q(x,y,z), g(x,y,z)와 난수 a를 사용하여 평문을 암호화하여 암호문 R(x,y,z)을 수신자에게 보낸다. 수신자는 암호문 R(x,y,z)을 g(x,y,z)=0의 근, x, y와 z 그리고 비밀키 벡터의 초증가성을 사용하여 평문을 구하게 된다. 따라서 해독과정에서 3변수 다항식 g(x,y,z)=0의 인수분해의 어려움 때문에 안전성을 갖는 공개키 다항식 배낭 암호시스템으로 된다. 제안된 공개키 다항식 배낭 암호시스템의 타당성을 컴퓨터 시뮬레이션을 통하여 입증하였다.

Ⅰ. 서론

컴퓨터의 빠른 보급과 정보통신 기술의 발달로 컴퓨터 네트워크의 진전과 함께 종합 정보 시스템이 구축되고 있으며, 이러한 정보 시스템의 보급 확대로 우리 사회는 고도 정보화 사회로 진입되고 있다. 이에 따라 정보 시스템의 사회적 중요성은 한층 높아지고 있다. 통신 장치, 통신 선로 등으로 구성되는 통신망에서는 도청자가 통신중인 정보를 도청하여 해독함으로써 정보가 누출되거나, 데이터를 변조, 삽입 또는 삭제가 가능하다. 이와 같은 불안전한 통신망의 안전 보호 대책으로 유일한 수단과 방법은 정보를 암호화시키는 기법에 의존할 수 밖에 없다.

* 목원대학교 IT공학부 교수

암호의 역사는 상당히 먼 옛날부터 군사 목적으로 사용되었으며, 가장 오래된 암호화 기법으로 알려져 있는 것이 기원전 400년경 희랍인들에 의해 사용된 Scytale 암호라 불리는 전치 암호(transposition cipher)이다.[1] 최초의 환자 암호(substitution cipher)는 Julius Caesar 암호이고, 합성 암호(product cipher)는 전치 암호와 환자 암호를 적당히 조합한 암호로써, 1914년 제1차 세계 대전중 독일 육군에 의해 사용된 ADFGVX 암호를 들 수 있다. 미국 상무성 표준국(NBS: National Bureau of Standard)에 의해 Lucifer 암호에 근거를 둔 암호화 표준 기법으로 1977년 DES(Data Encryption Standard)가 제정되었다.[2]

암호 방식은 암호키의 분배와 관리 방법에 따라 전통적인 암호방식(conventional cryptosystem)과 공개키 암호방식(public key cryptosy-

stem)으로 나눌 수 있다.[3] 전통적인 암호방식은 암호키와 해독키가 동일하며, 이 두 키는 송신자와 수신자가 공용하는 비밀키가 된다. 공개키 암호는 암호키와 해독키가 서로 다르며 암호키는 공개하나 해독키는 비밀로 보관하는 것이 보통이다.

전통적인 암호시스템의 단점을 1976년 Diffie와 Hellman[4]이 제안한 oneway 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, 사용자 확인 등의 실용을 가능하게 하였다. 공개키 개념을 이용한 암호방법 중 가장 먼저 제안된 것은 1978년 Rivest, Shamir와 Adieman[5]에 의한 RSA 암호이다.

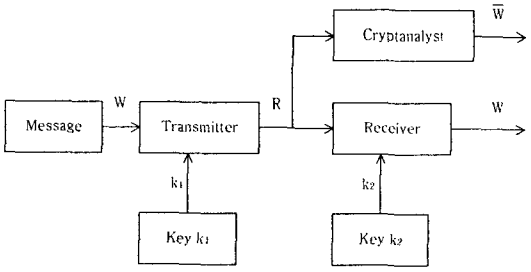
이 암호는 큰 합성수를 소인수분해 하는 어려움에 안전성을 두고 있으며, 발표 후 오늘날에도 가장 널리 쓰이며 안전성을 인정받고 있는 공개키 암호법이나, 소인수분해법의 눈부신 발전 및 하드웨어의 급속한 성능 향상으로 조만간 키의 크기(key size)를 크게 해야 할 것으로 평가받고 있다. 또한 1978년에 Merkle와 Hellman [6], Chor와 Rivest[7] 등에 의해 배낭 문제(knapsack problem)를 사용한 MH 암호 등이 제안되었다. Elgamal[8]은 1985년에 이산적 대수 문제의 어려움에 대한 안전성을 갖는 암호를 제안하였다. 1989년에 Tsujii[9] 등은 비선형 방정식의 해를 구하기 어려움에 기초를 둔 공개키 암호시스템을 일반화하였다.

본 논문에서는 3변수 다항식의 근을 구하는 어려움 때문에 안전성을 갖는 공개키 다항식 배낭 암호시스템을 제안한다. 그리고 시뮬레이션을 통해 주어진 문자 평문에 대하여 암호화하고 해독하여 제안된 공개키 다항식 배낭 암호시스템의 타당성을 입증한다.

II. 공개키 암호 방법

공개키 암호 방법은 전통적인 암호 방법과 달리 암호키와 해독키를 분리하여 암호키는 암호통신망 가입자 모두에게 공개하고, 해독키는 가입자 각자가 비밀리에 보관하는 방법으로 비대칭 알고리즘이다.

이 암호시스템은 그림 1과 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 구하기는 어려움이 있다.



(그림 1) 공개키 암호시스템

(Fig. 1) Public key cryptosystem

암호 과정을 E, 해독 과정을 D, 암호문을 R, 원문을 W, 그리고 키를 k라고 할 때, 공개키 암호시스템의 성질은 다음과 같다.

(1) 모든 키 k에 대하여, E_k와 D_k는 역함수 관계가 성립한다($E_k \cdot D_k=1$).

따라서 $E_k(W)=R$이면, $D_k(R)=D_k(E_k(W))=E_k \cdot D_k(W)=W$이다.

(2) 모든 키 k는 W에 대하여, $E_k(W)$과 $D_k(W)$의 계산이 용이하다.

(3) 암호키 E_k만 아는 상태에서 해독키 D_k를 계산해 내는 것은 실현 불가능하다.

(4) 모든 키 k에 대하여, E_k와 D_k가 역으로 적용될 수 있다. 즉, $D_k(W)=R$이면, $E_k(R)=E_k(D_k(W))=E_k \cdot D_k(W)=W$이다.

여기서 성질 (3)에 의하여 암호키를 공개할 수 있고, 성질 (1), (2), (3)을 만족할 때 "trapdoor one-way function"이라 하며, 성질 (1), (2), (3), (4) 모두를 만족시킬 때 "trapdoor one-way permutation for signature"라 한다.

공개키 암호 방법으로 구성된 암호 통신망 가입자는 암호키와 해독키가 필요하게 되므로 전체 가입자가 n명일 때 암호키의 수는 2n개이고, 실제로 비밀리에 보관해야 하는 해독키의 수는 n개로 각 가입자가 자기 소유인 해독키 하나만을 보관하게 되므로 전통적인 암호 방법보다 보관해야 할 키의 수가 적고, 또한 암호키를 공개하므로 키분배가 필요없어 키 관리가 용이하다.

III. 공개키 다항식 배낭 암호시스템

주어진 정수의 집합과 이 집합의 원소들의 합으로부터, 부분 집합을 찾아내는 데 어려움을 둔 MH 배낭 암호[6]의 안전성에, 공개키 다항식의 근을 구하는 어려움의 안전성을 더함으로써, MH 배낭 암호보다 안전성 있는 공개키 배낭 암호 알고리즘을 제안한다.

3.1 키 생성

먼저 (1)식을 만족시키는 초증가 벡터(superincreasing vector) $P=(p_1,p_2,\cdots,p_n)$를 정의한다.

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

그리고 조건식 $v > \sum_{i=1}^{n} p_i$를 만족시키는 소수(prime number) v를 정한 후, $0<x_1,y_1,z_1<v$를 만족시시키는 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 p_i를 적당하게 p_{i1}, p_{i2}와 p_{i3}으로 3분할하여 표현한다.

$$p_i=(p_{i1}+p_{i2}+p_{i3}) \bmod v \tag{2}$$

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

$$\begin{aligned} p_{i1}&=(q_{i1}x+d_{i1}) \bmod v \\ p_{i2}&=(q_{i2}y+d_{i2}) \bmod v \\ p_{i3}&=(q_{i3}z+d_{i3}) \bmod v \end{aligned} \tag{3}$$

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

$$q_{i4}=(d_{i1}+d_{i2}+d_{i3}) \bmod v \tag{4}$$

따라서 초증가 벡터의 요소 p_i가 (3), (4)식과 같이 다항식으로 표현된다. 이러한 다항식을 사용하여 배열 순서를 적당하게 변환하여 (5)식과 같이 다항식 벡터 Q(x, y, z)를 표현한 후 암호 벡터로써 공개한다. 그러므로 초증가 벡터 P의 요소가 n개이고, 다항식 벡터 Q(x, y, z)의 계수는 4n개로 된다.

$$Q(x,y,z)=(q_{11}x+q_{12}y+q_{13}z+q_{14},\ q_{21}x+q_{22}y+q_{23}z+q_{24},\ \cdots,\ q_{n1}x+q_{n2}y+q_{n3}z+q_{n4}) \quad (5)$$

그리고 다른 하나의 공개키 다항식 g(x,y,z)의 계수 g_1, g_2와 g_3는 다음 식을 만족시키는 정수로 적당히 선택한다.

$$0<g_1,\ g_2,\ g_3<v \quad (6)$$

또한 공개키 다항식의 계수 g_4는 (7)식과 같이 구한다.

$$g_4=(-g_1x_1-g_2y_1-g_3z_1) \bmod v \quad (7)$$

따라서 (6)식과 (7)식에서 나타낸 계수 g_1, g_2, g_3와 g_4를 이용하여 (8)식과 같은 공개키 다항식 g(x,y,z)를 공개한다.

$$g(x,y,z)=g_1x+g_2y+g_3z+g_4 \quad (8)$$

MH 배낭 암호시스템은 초증가 벡터 P를 공개하나 본 논문에서는 소수 v를 공개하고, 초증가 벡터 P를 변환하여 다항식 벡터 Q(x,y,z)로 표현한 것을 공개하고, 또한 다항식 g(x,y,z)를 선택하여 공개한다. 이것이 MH 배낭 암호시스템과 다른 점이며, 이 암호의 안전성은 다음의 조건식 (9)식을 만족시키는 다항식 $g(x,y,z)=0 \bmod v$를 인수분해 하여 근 x_1, y_1과 z_1을 찾는 어려움에 기초를 둔다.

$$(q_{i1}x+q_{i2}y+q_{i3}z+q_{i4})|_{x=x_i,y=y_i,z=z_i} \bmod v > \sum_{j=1}^{i-1}(q_{j1}x+q_{j2}y+q_{j3}z+q_{j4})|_{x=x1,y=y1,z=z1} \bmod v \ (i=2,3,\cdots,n) \quad (9)$$

3.2 암호화

평문은 0-1벡터로써 $W=(w_1, w_2, \cdots, w_n)$로 나타내고, 난수(random number) a를 사용하여 암호문의 다항식 R(x,y,z)를 (10)식과 같이 나타내고, 암호문의 다항식 계수 R_1, R_2, R_3와 R_4를 수신자에게 보낸다.

$$\begin{aligned} R(x,y,z)&=Q(x,y,z)W+ag(x,y,z) \bmod v \\ &=\sum_{i=1}^{n}(q_{i1}x+q_{i2}y+q_{i3}z+q_{i4})w_i+a \\ &\quad (g_1x+g_2y+g_3z+g_4) \bmod v \\ &=R_1x+R_2y+R_3z+R_4 \bmod v \end{aligned} \quad (10)$$

여기서 $\sum_{i=1}^{n} R_j=\Sigma q_{ij}w_i+ag_i$ (j=1, 2, 3, 4)이다.

그러므로 송신하고자 하는 n개(n비트)의 평문 벡터 W를 암호화하면 4개의 십진수로 된 데이터로 변형되어 수신자에게 보내진다.

3.3 해독화

수신자는 수신된 암호문 R(x,y,z)를 해독하기 위하여 먼저 $g(x,y,z)=0 \bmod v$의 근 x_1, y_1과 z_1을 대입하여 (11)식과 같이 D를 구한다.

$$\begin{aligned} D&=R(x,y,z)|_{x=x1,y=y1,z=z1} \bmod v \\ &=\sum_{i=1}^{n}(q_{i1}x+q_{i2}y+q_{i3}z)w_i|_{x=x1,y=y1,z=z1} \bmod v \\ &=\sum_{i=1}^{n}q_iw_i \bmod v \end{aligned} \quad (11)$$

다음에 비밀키 벡터 P의 초증가성을 사용하여 다음과 같은 알고리즘으로 평문 $W=(w_1, w_2, \cdots, w_n)$이 구해진다. 제안된 공개키 배낭 암

호시스템의 블록 선도는 그림 2와 같다.

단계 1. i=0

단계 2. If $p_{n\,i}>D$ then $w_{n\,i}=0$, $D=D-p_{n\,i}$
else $w_{n\,i}=1$

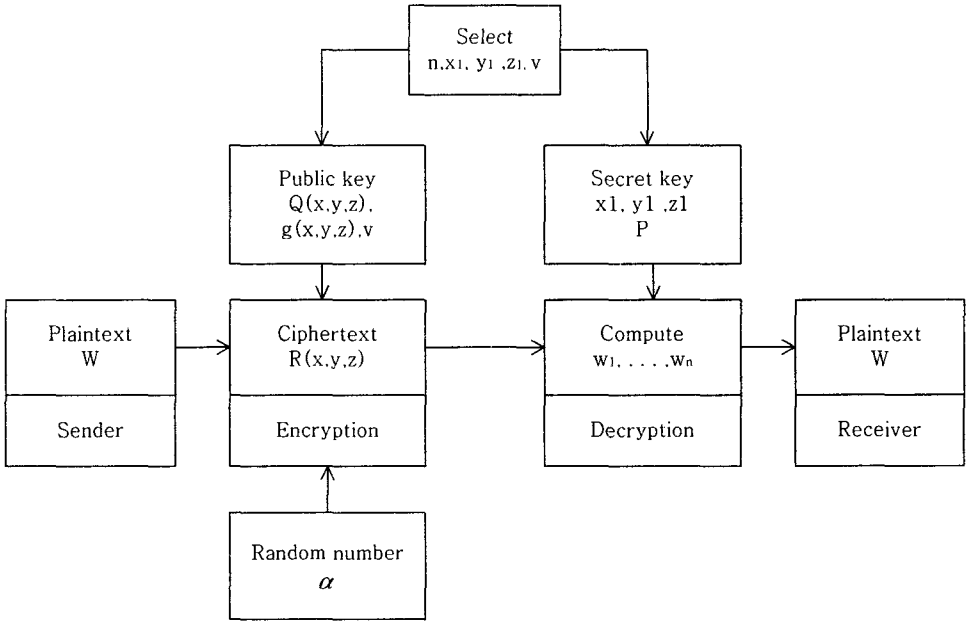
단계 3. If i=n-1 then Stop

단계 4. i=i+1

단계 5. Goto 단계 2

P=(32+33+40, 43+23+40, 28+94+90, 33+38+45, 145+31+55, 73+47+33) (mod 103)

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



(그림 2) 제안된 공개키 배낭 암호시스템

(Fig. 2) Proposed public key knapsack cryptosystem

IV. 시뮬레이션 및 결과 고찰

초증가 벡터 P=(2, 3, 6, 13, 25, 50)를 정의하고, 소수 v=103으로 선택하고, 임의의 정수 x_1=11, y_1=6과 z_1=44로 정한 후 초증가 벡터 P를 요소 p_i를 다음과 같이 변형한다.

Q(x,y,z)=(2x+5y+0z+53, 3x+3y+0z+55, 2x+15y+2z+12, 3x+6y+1z+3, 13x+5y+1z+14, 6x+7y+0z+45)

또한 다항식 g(x,y,z)의 계수를 g_1=12, g_2=33과 g_3=68로 정하면 g_4=77이 되므로 공개키 다항식은 g(x,y,z)=12x+33y+68z+77로 된다. 이와 같은 배낭 암호시스템의 키를 표 1에 나타내었다.

<표 1> 배낭 암호시스템의 키

<Table 1> The key of knapsack cryptosystem

공개키	소수	v=97
	암호벡터	Q(x,y,z)=(2x+5y+0z+53, 3x+3y+0z+55, 2x+15y+2z+12, 3x+6y+1z+3, 13x+5y+1z+14, 6x+7y+0z+45)
	다항식	g(x,y,z)=12x+33y+68z+77
비밀키	초증가 벡터	P=(2, 3, 6, 13, 25, 50)
	정수	x1=11, y1=6, z1=44

<표 2> 문자의 2진수 표현

<Table 2> 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

<표 3>은 송신자가 송신하고자 할 텍스트 평문 "KNAPSACK CRYPTOSYSTEM !"에 송신 2진수 평문(W), 난수(a), 암호문(R), 수신 2진수 평문(W)과 수신 텍스트 평문을 나타내었다. 여기서 송신 2진수 평문은 송신 텍스트 평문 "KNAPSACK CRYPTOSYSTEM !"에 대하여 표 2와 같이 각 문자에 대응하는 6비트 2진수로 나타내었다. 이러한 송신 2진수 평문에 대해 난수 a와 암호 알고리즘을 적용하면 암호문 R이 얻어진다. 암호문 R을 수신자에게 보내면 수신자는 공개키와 비밀키를 사용하여 암호문을 해독하여 표 3의 수신 2진수 평문(W)을 얻는다. 그리고 표 2와 같이 6비트 2진수에 대응시키면 수신 텍스트 평문 "KNAPSACK CRYPTOSYSTEM !"을 얻는다.

그리고 표 3에서 송신 텍스트 평문 "KNAPSACK CRYPTOSYSTEM !"의 첫 번째 문자 "K"를 6비트 2진수로 바꾸면 "101010"와 같은 송신 2진수 평문이 되며, 난수 a=72와 암호 알고리즘을 적용하면 암호문 "57 32 58 61"가 얻어진다. 암호문을 수신자가 해독하면 수신 2진수 평문 "101010"을 얻고 수신 텍스트 평문으로 바꾸면 송신한 문자 "K"를 얻는다.

또한 <표 3>에서 송신 텍스트 평문 "KNAPSACK CRYPTOSYSTEM !"에서 세 번째 문자 "A"와 여섯 번째 문자 "A"에 대하여 암호화하는 데 사용되는 난수 a가 각각 59, 79와 같이 서로 다르므로 암호문도 " 92 98 98 64", "23 37 16 59"와 같이 각각 다르게 되어 해독이 어렵게 된다.

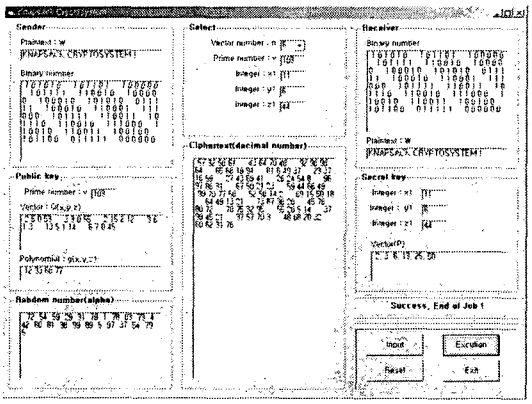
(그림 3)은 시뮬레이션 결과로써 송신자 평문, 공개키, 비밀키, 암호문, 수신자 평문 등을 나타내고 있다.

제안된 배낭 암호시스템은 MH 배낭 암호의 초증가 벡터를 변형하여 다항식을 표현하고 그것을 이용하여 암호화 된 것에 난수를 곱한 공개키 다항식을 가한 것을 암호문으로 하였기 때문에, 이 암호의 안전성은 다항식 벡터 Q(x,y,z)의 각 변수에 공개키 다항식 g(x,y,z)=0 mod v의 근을 대입할 때 공개키 다항식 g(x,y,z)=0 mod v을 인수 분해하여 근을 구하는 데 어려움이 있다.

<표 3> 배낭 암호시스템 데이터

<Table 3> Knapsack cryptosystem data

송신문(W)	KNAPSACK CRYPTOSYSTEM !
2진 송신문	101010 101101 100000 101111 110010 100000 100010 101010 011111 100010 110001 111000 101111 110011 101110 110010 111000 110010 110011 100100 101100 011111 000000
난수(a)	72 54 59 29 31 79 1 78 83 73 4 42 88 81 38 99 89 5 97 37 54 79 5
암호문(R)	57 32 58 61 43 64 70 48 92 98 98 64 65 68 19 94 81 6 49 37 23 37 16 59 27 43 69 41 26 24 54 8 96 97 86 31 67 50 21 23 59 44 66 49 99 70 77 58 52 58 14 2 69 15 50 18 64 49 13 21 73 87 38 20 45 76 80 72 78 75 32 95 55 28 5 14 37 99 45 21 37 57 70 3 48 68 20 32 60 62 31 76
2진 수신문	101010 101101 100000 101111 110010 100000 100010 101010 011111 100010 110001 111000 101111 110011 101110 110010 111000 110010 110011 100100 101100 011111 000000
수신문(W)	KNAPSACK CRYPTOSYSTEM !



(그림 3) 시뮬레이션 결과

(Fig. 3) Simulation result

V. 결론

컴퓨터 통신에 대한 요구와 수요가 확대되어 감에 따라 정보의 내용 변경, 정보의 불법적인 유출, 순서 변경 그리고 미확인 발신자 및 수신자 등에 의하여 항상 위협을 받음으로써 정보의 안전성이 요구된다.

본 논문은 3변수 다항식의 인수분해의 어려움 때문에 컴퓨터 통신의 안전성을 갖는 공개키 배낭 암호시스템을 제안하였다. 공개키 배낭 암호시스템은 MH 배낭 암호의 초증가 벡터 P를 변형하여 다항식 표현하고, 그것을 사용하여 암호화 된 것에, 난수를 곱한 공개키 다항식을 가한 것을 암호문으로 하였다. 이 암호의 안전성은 다항식 벡터 Q(x,y,z)의 각 변수에 공개키 다항식 g(x,y,z)=0의 근을 대입할 때 공개키 다항식 g(x,y,z)=0을 인수분해 하여 근 x, y와 z를 구하는 데 어려움이 있다. 그러므로 초증가 벡터 P의 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.

참고문헌

[1] C. H. Meyer, S. M. Matyas, Cryptography: A New Dimension in Computer Data Security, John Wiley & Sons, 1982.

[2] A. A. Arullah, G. I. Parkin and B. A. Wichmann, A Pascal of the DES Encryption Algorithm Including Cipher Block Chaining, NPL Report DITC 61/85, June 1985.

[3] D. B. Newman, et al., "Public Key Managemant for network Security", IEEE Network Magazine, Vol. 1, No. 2, pp. 11-16, April 1987.

[4] W. Diffie and M. E. Hellman, "New Direction in Cryptography", IEEE Trans. Inform. Theory, Vol. IT-22, pp. 644-654, Nov. 1976.

[5] R. L. Rivest, A. Shamir and L. Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystem", Comm. ACM, Vol. 21, No. 2, pp. 120-126, 1978.

[6] R. C. Merkle and M. E. Hellman, "Hiding Information and Signatures in Trapdoor Knapsacks", IEEE Trans. Info. Theory, Vol. IT-24, 1978.

[7] 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, pp. 901-909, 1988.

[8] T. Elgamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms", IEEE Trans. Inf. Theory, Vol. IT-31, No. 4, pp. 469-472, 1985.

[9] 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", 전자정보통신학회논문지, Vol. J72-A, No. 2, pp. 390-389, Feb. 1989.

A Study on Public Key Knapsack Cryptosystem for Security in Computer Communication Networks

Tae-Kyu, Yang*[1)]

Abstract

In this paper, a public key knapsack cryptosystem algorithm is based on the security to a difficulty of polynomial factorization in computer communication networks is proposed. For the proposed public key knapsack cryptosystem, a polynomial vector Q(x,y,z) is formed by transform of superincreasing vector P, a polynomial g(x,y,z) is selected. Next then, the two polynomials Q(x,y,z) and g(x,y,z) is decided on the public key. The enciphering first selects plaintext vector. Then the ciphertext R(x,y,z) is computed using the public key polynomials and a random integer α. For the deciphering of ciphertext R(x,y,z), the plaintext is determined using the roots x, y, z of a polynomial g(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 g(x,y,z)=0 with three variables. The propriety of the proposed public key cryptosystem algorithm is verified with the computer simulation.

* School of IT Engineering, Mokwon University