정보학연구 제6권 제1호 2003년 3월(pp.1-10)
The Journal of Information Technology, Vol.6, No.1

컴퓨터 네트워크의 보안을 위한 공개키 다항식 지수 암호시스템에 대한 연구

양태규*

요 약

본 논문에서는 컴퓨터 네트워크의 보안성을 위해서 다항식을 인수분해 하는 데 어려움이 있는 공개키 다항식 지수 암호시스템 알고리즘을 제안하였다. 제안된 공개키 다항식 지수 암호 시스템에서는 암호문은 평문 다항식 W(x,y,z)을 구성하여 이것을 3승하여 그것에 2개의 공개키 다항식 f(x,y,z)와 g(x,y,z)를 각각 임의의 정수를 곱하여 더한 것을 암호문 C(x,y,z)로 하여 수신자에게 보내준다. 공개키 다항식 f(x,y,z)=g(x,y,z)=0 mod p 근을 구하는 어려움 때문에 해독이 힘들게 된다. 제안된 공개키 다항식 지수 암호 알고리즘은 소인수분해의 어려움에 기초를 둔 RSA 방법의 안전성에, 공개키 다항식을 동시에 만족하는 근을 구하는 어려움의 안전성을 더함으로써 보다 더 안전성 있는 공개키 지수 암호 알고리즘으로 된다. 제안된 공개키 다항식 지수 암호시스템의 타당성을 컴퓨터 시뮬레이션을 통하여 입증하였다.

Ⅰ. 서론

컴퓨터 네트워크는 컴퓨터 기술과 통신 기술의 집합체로 오늘날 고도의 정보화 사회에서 요구되는 각종 서비스를 제공하고 있다. 그러나 고도의 정보 통신 기술의 발전은 정보의 내용 변경, 정보의 불법적인 유출, 순서 변경 그리고 미확인 송신자 및 수신자 등에 의하여 항상 위협을 받음으로써 정보의 안전성이 요구된다.

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 AD-FGVX 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]

암호화 구현 방법은 스트림(stream) 암호와 블럭 암호(block cipher)로 구분된다. 스트림 암호는 평문의 각 심볼을 바로 암호문의 한 심볼로 바꾸는 방법이며, 블럭 암호는 스트림 암호와는 달리 평문을 고정된 크기의 연속적인 블럭으로 나누어 같은 키를 사용하여 독립적으로 암호화 하는 방법으로서 DES, RSA[3] 암호 등이 있다.

* 목원대학교 IT공학부 교수

암호 방식은 암호키의 분배와 관리 방법에 따라 전통적인 암호방식(conventional cryptosystem)과 공개키 암호방식(public key cryptosystem)으로 나눌 수 있다.[4] 전통적인 암호방식은 암호키와 비밀키가 동일하며, 이 두 키는 송신자와 수신자가 공용하는 비밀키가 된다. 공개키 암호는 암호키와 비밀키가 서로 다르며 암호키는 공개하나 비밀키는 비밀로 보관하는 것이 보통이다.

전통적인 암호시스템의 단점을 1976년 Diffie와 Hellman[5]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[3]에 의한 RSA 암호이다.

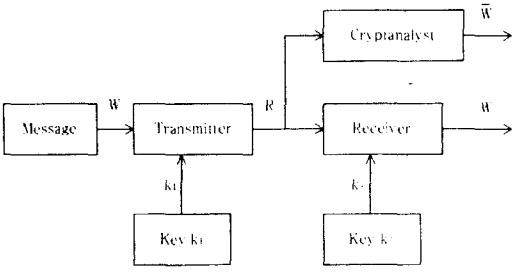
이 암호는 큰 합성수를 소인수분해 하는 어려움에 안전성을 두고 있으며, 발표 후 오늘날에도 가장 널리 쓰이며 안전성을 인정받고 있는 공개키 암호법이나, 소인수분해법의 눈부신 발전 및 하드웨어의 급속한 성능 향상으로 조만간 키의 크기(key size)를 크게 해야 할 것으로 평가받고 있다. 또한 1978년에 Merkle와 Hellman[6], Chor와 Rivest[7] 등에 의해 배낭 문제(knapsack problem)를 사용한 MH 암호 등이 제안되었다. Elgamal[8]은 1985년에 이산적 대수 문제의 어려움에 대한 안전성을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

본 논문에서는 평문 다항식 W(x,y,z)를 구성하여 이 평문 다항식을 3제곱하고, 그것에 2개의 공개키 다항식 공개키 다항식 f(x,y,z)와 g(x,y,z)에 각각 임의의 정수를 곱하여 더한 것을 암호문으로 한다. 해독은 f(x,y,z)=g(x,y,z)=0 mod p의 근 x,y,z를 사용하여야하는 데 공개키 다항식 f(x,y,z)=g(x,y,z)=0 mod p 근을 구하는 어려움 때문에 해독이 힘들어지는 공개키 다항식 지수 암호 알고리즘을 제안한다.

그리고 시뮬레이션을 통해 주어진 문자 평문에 대하여 암호화하고 해독하여 제안된 공개키 다항식 지수 암호시스템의 타당성을 입증한다.

II. 공개키 암호 방법

공개키 암호 방법은 전통적인 암호 방법과 달리 암호키와 비밀키를 분리하여 암호키는 암호통신망 가입자 모두에게 공개하고, 비밀키는 가입자 각자가 비밀리에 보관하는 방법으로 비대칭(asymmetric) 알고리즘이다.



(그림 1) 공개키 암호시스템
(Fig. 1) Public key cryptosystem

이 암호시스템은 전통적인 암호시스템의 키 분배 문제를 해결하고, 디지털 서명이 가능한 방법으로 (그림 1)과 같이 암호키 k_1과 비밀키 k_2가 다르며, 암호키에서 비밀키를 만들어 낼 수 없다. 이 방식에서 송신자가 사용하는 암호키만을 공개하고 수신자는 비밀키만을 관리함으로

써 공중통신망을 사용하는 통신상대자가 늘어남에 따라 통신상대 전원에 대한 많은 키를 가져야 하는 단점을 해결하였다.

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 비밀키 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 비밀키가 필요하게 되므로 전체 가입자가 n명일 때 암호키의 수는 2n개이고, 실제로 비밀리에 보관해야 하는 비밀키의 수는 n개로 각 가입자가 자기 소유인 비밀키 하나만을 보관하게 되므로 전통적인 암호 방법보다 보관해야 할 키의 수가 적고, 또한 암호키를 공개하므로 키분배가 필요없어 키 관리가 용이하다.

Ⅲ. 공개키 다항식 지수 암호시스템

소인수 분해의 어려움에 기초를 둔 RSA 방법의 안전성에, 공개키 다항식에 2개의 3변수 다항식을 사용하여, 이 다항식을 동시에 만족하는 근을 구하는 어려움의 안전성을 더함으로써 보다 더 안전성 있는 공개키 다항식 지수 암호 알고리즘을 제안한다.

3.1 키 생성

최대 공약수 GCD(3,p-1)=1을 만족하는 소수(prime number) p를 선택하고 $0<x_i, y_i, z_i<p$ (i=1,2,3)를 만족하는 정수 x_i, y_i, z_i을 적당하게 정한다.

그리고 (1)식을 만족하는 승법 역원(multiplicative inverse element) z_i^{-1} (i=1,2,3)을 구한다.

$$z_i z_i^{-1}=1 \bmod p \quad (i=1,2,3) \tag{1}$$

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

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

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

다음에 (4)식과 (5)식과 같은 2개의 독립된 다항식 f(x,y,z)와 g(x,y,z)을 계산하여 공개한다.

$$f(x,y,z) = \prod_{j=1}^{3} (a_j x + b_j y + r_j z) \bmod p$$

$$= f_1 x^3 + f_2 y^3 + f_3 z^3 + f_4 x^2 y + f_5 x^2 z + f_6 x y^2 + f_7 y^2 z + f_8 x z^2 +$$

$f_9yz^2+f_{10}xyz$ (4)

$$g(x,y,z) = \prod_{j=4}^{6} (a_jx+b_jy+r_jz) \bmod p$$

$$= g_1x^3+g_2y^3+g_3z^3+g_4x^2y+g_5x^2z+g_6xy^2+g_7y^2z+g_8xz^2+g_9yz^2+g_{10}xyz \quad (5)$$

따라서 다항식 f(x,y,z)와 g(x,y,z)은 공개키가 되며, 비밀키는 x_i, y_i, z_i (i=1,2,3)와 (6)식을 만족하는 d 가 된다.

$3d=1 \bmod p-1$ (6)

그리고 (7)식을 만족하는 승법 역원 $(T_1T_2-T_3T_4)^{-1}$ 을 구한다.

$(T_1T_2-T_3T_4)(T_1T_2-T_3T_4)^{-1}=1 \bmod p$ (7)

여기서, $T_1=x_1z_2-x_2z_1$, $T_2=y_1z_3-y_3z_1$, $T_3=x_1z_3-x_3z_1$, $T_4=y_1z_2-y_2z_1$ 이다.

또한 (8)식을 만족하는 승법 역원 T_4^{-1}이 비밀키가 된다.

$T_4T_4^{-1}=1 \bmod p$ (8)

그러므로 비밀키는 (6)식, (7식), (8)식의 d, $(T_1T_2-T_3T_4)^{-1}$, T_4^{-1}이 된다.

3.2 암호화

제안된 공개키 암호시스템은 블럭 암호시스템으로써 10진수로 표현된 3개의 평문의 문자가 하나의 블럭이 된다. 이때 3개의 평문 W_i의 범위를 $0 \le W_i < p$ (i=1,2,3)로 정하고, 평문 다항식을 (9)식과 같이 나타낸다.

$W(x,y,z)=W_1x+W_2y+W_3z$ (9)

그러므로 10진수 평문 W_1, W_2, W_3가 하나의 블럭으로 나타내진다. 암호화는 평문 다항식 W(x,y,z)을 3승하고, 부등식 $0<u,v<p$ 을 만족시키는 2개의 임의의 수 u, v를 공개키 다항식 f(x,y,z), g(x,y,z)에 각각 곱하여 (10)식과 같은 암호문을 계산하여 수신자에게 보낸다.

$$\begin{aligned} C(x,y,z) &= W(x,y,z)^3+uf(x,y,z)+v^g(x,y,z) \bmod p \\ &= (W_1x+W_2y+W_3z)^3 \\ &+ u(f_1x^3+f_2y^3+f_3z^3+f_4x^2y+f_5x^2z+f_6xy^2+ \\ &\quad f_7y^2z+f_8xz^2+f_9yz^2+f_{10}xyz) \\ &+v(g_1x^3+g_2y^3+g_3z^3+g_4x^2y+g_5x^2z+ \\ &\quad g_6xy^2+g_7y^2z+g_8xz^2+g_9yz^2+g_{10}xyz) \\ &= c_1x^3+c_2y^3+c_3z^3+c_4x^2y+c_5x^2z+c_6xy^2+ \\ &\quad c_7y^2z+c_8xz^2+c_9yz^2+c_{10}xyz \end{aligned} \quad (10)$$

여기서, $c_1=W_1^3+uf_1+vg_1 \bmod p$

$c_2=W_1^3+uf_2+vg_2 \bmod p$

$c_3=W_1^3+uf_3+vg_3 \bmod p$

$c_4=3W_1^2W_2+uf_4+vg_4 \bmod p$

$c_5=3W_1^2W_3+uf_5+vg_5 \bmod p$

$c_6=3W_1W_2^2+uf_6+vg_6 \bmod p$

$c_7=3W_2^2W_3+uf_7+vg_7 \bmod p$

$c_8=3W_1W_3^2+uf_8+vg_8 \bmod p$

$c_9=3W_2W_3^2+uf_9+vg_9 \bmod p$

$c_{10}=6W_1W_2W_3+uf_{10}+vg_{10} \bmod p$

그러므로 암호문 C(x,y,z)의 계수 c_k(k=1,2,... 10)를 수신자에게 보내진다.

3.3 해독화

해독화는 (11)식과 (12)식과 같은 공개키 다항

식의 근 x_i, y_i, z_i (i=1,2,3)을 구하여야 한다.

$$f(x,y,z)=0 \bmod p \quad (11)$$

$$g(x,y,z)=0 \bmod p \quad (12)$$

그리고 근 x_i, y_i, z_i (i=1,2,3)을 사용하여 (13)식의 D_i(i=1,2,3)를 구한다. 여기서 방정식은 2개이고 미지수는 3개이므로 도청자가 비밀키 x_i, y_i, z_i (i=1,2,3)을 모르면 D_i(i=1,2,3)를 구하기 어렵다.

$$D_i(C)=C(x,y,z)|_{x=x_i,\ y=y_i,\ z=z_i} \bmod p \ (i=1,2,3) \quad (13)$$

다음에 비밀키 d를 사용하여 (14)식의 $D_i(C)^d$ (i=1,2,3)을 계산한다.

$$\{D_i(C)\}^d \bmod p = W_1x_i+W_2y_i+W_3z_i \ (i=1,2,3) \quad (14)$$

그리고 비밀키 $(T_1T_2-T_3T_4)^{-1}$ 와 T_4^{-1}을 사용하면 3개의 평문이 (15)식, (16)식과 (17)식에서 구해진다.

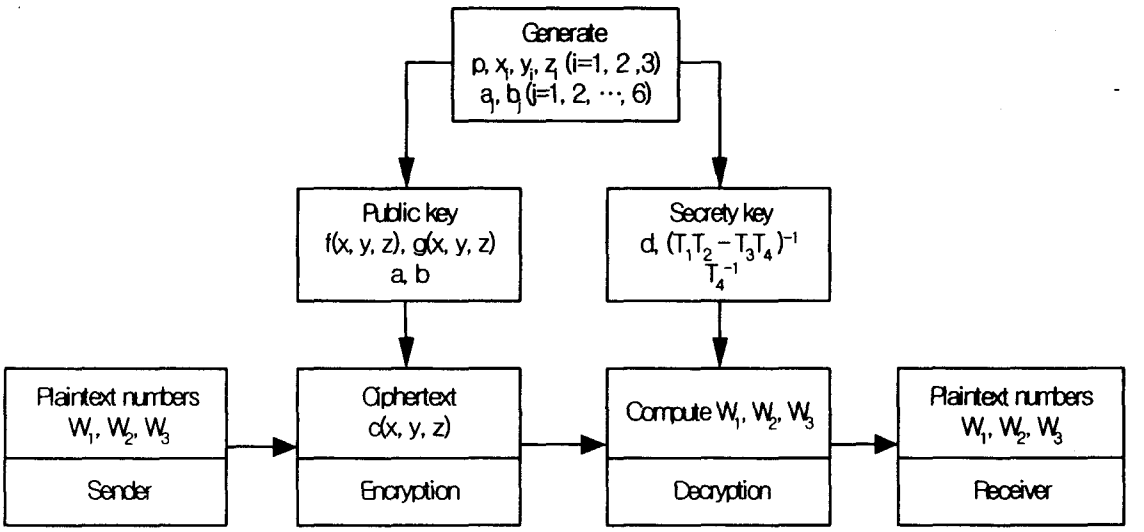
$$W_1=[\{D_1(C)^dz_2-D_2(C)^dz_1\}T_2-\{D_1(C)^dz_3-D_3(C)^dz_1\}T_1](T_1T_2-T_3T_4)^{-1} \bmod p \quad (15)$$

$$W_2=[D_1(C)^dz_2-D_2(C)^dz_1-T_1W_1]T_4^{-1} \bmod p \quad (16)$$

$$W_3=[D_1(C)^d-W_1x_1-W_2y_1]z_1^{-1} \bmod p \quad (17)$$

이와같이 해독하여 평문 W_1, W_2, W_3를 구하는 과정에서 알고리즘이 각각 다르다. W_1 해독시는 $(T_1T_2-T_3T_4)^{-1}$을 사용하였고, W2 해독시는 T_4^{-1}을 사용하였고, W_3 해독시는 z_1^{-1}을 사용하였다. 그러므로 해독 알고리즘 (15)식, (16)식, (17)식은 각각 비밀키 생성식인 (7)식, (8)식, (1)식과 관계가 있다.

제안된 공개키 지수 암호 알고리즘은 (그림 2)와 같다.



(그림 2) 제안된 공개키 지수 암호시스템
(Fig. 2) Proposed public key cryptosystem

Ⅳ. 시뮬레이션 및 결과 고찰

제안된 공개키 지수 암호 알고리즘의 타당성을 입증하기 위해, 소수 p=29와 정수 x_1=10, y_1=17, z_1=22, x_2=18, y_2=8, z_2=23, x_3=25, y_3=5, z_3=14로 정하면, 승법 역원 z_1^{-1}=4, z_2^{-1}=24, z_3^{-1}=27로 구해진다. 또한 임의의 정수 a_i=i, b_i=i+1 (i=1,2,...,6)으로 하면, r_1=27, r_2=10, r_3=16, r_4=22, r_5=23, r_6=22로 구해지고, 이에 따라 공개키 다항식은 다음과 같이 얻어진다

$$f(x,y,z)=6x^3+24y^3+28z^3+0x^2y+21x^2z+17xy^2+7y^2z+7xz^2+28yz^2+4xyzg(x,y,z)=4x^3+7y^3+25z^3+28x^2y+28x^2z+xy^2+11y^2z+27xz^2+15yz^2+xyz$$

또한 <표 1>과 같이 비밀키는 d=19, $(T_1T_2-T_3T_4)^{-1}$=28, T_4^{-1}=17로 구해진다. 평문의 문자들을 <표 2>와 같이 " "=00, A=01, B=02, C=03 ,...,Z=26 으로 대응시키고, 3개의 평문의 3개 문자를 하나의 블럭으로 하면, 원래의 평문이 "EXP"인 경우 10진수는 "5, 24, 16"이 된다.

〈표 1〉 지수 암호시스템의 키

〈Table 1〉 The key of exponent cryptosystem

공개키	암호벡터	a=(1 2 3 4 5 6), b=(2 3 4 5 6 7)
	다항식 계수벡터	f=(6 24 28 0 21 17 7 7 28 4) g=(4 7 25 28 28 1 11 27 15 1)
비밀키	정수	d=19, (T1T2-T3T4)-1=28, T4-1=17

임의의 정수 u=6, v=25로 선택하면, 암호문은 (10)식에 의해 다음과 같이 구해진다.

$$C(x,y,z)=(5x+24y+16z)^3$$

〈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

$$=0x^3+20y^3+17z^3+6x^2y+25x^2z+9xy^2+9y^2z+4xz^2+9yz^2+27xyz$$

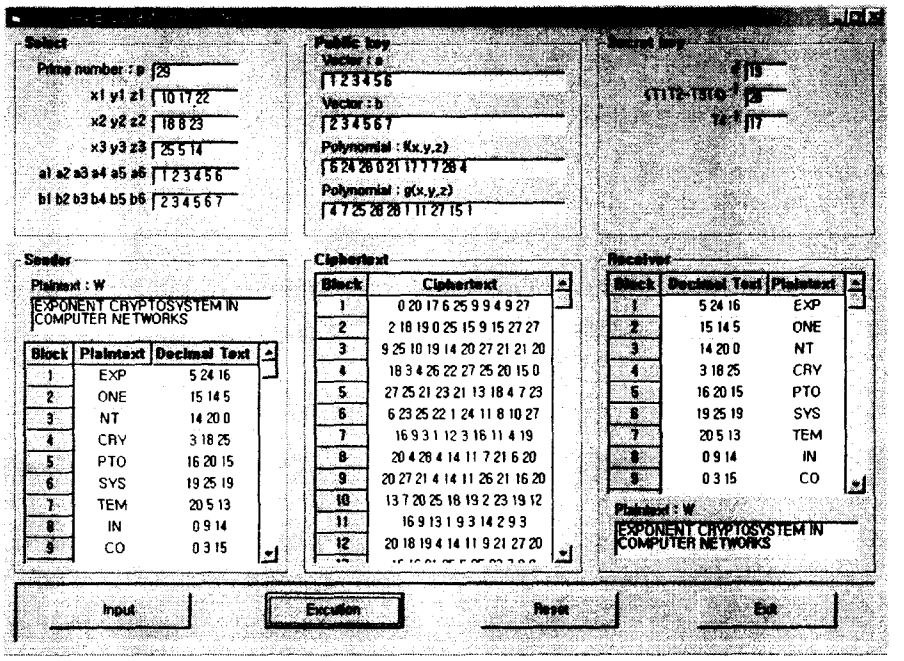
이 암호문의 계수 c_j(j=1,...,10)의 값을 수신자에게 보내지면, 수신자는 암호문 C(x,y,z)을 (13)식-(17)식을 이용하여 해독하면 10진수의 평문 "5, 24, 16"이 구해지고, 문자로 표현하면 송신자가 보낸 평문 "EXP"가 얻어진다.

<표 3>은 송신문이 "EXPONENT CRYPTO-SYSTEM"인 경우의 블록별 10진 송신문, 암호문, 10진수신문, 수신문 등을 나타내고 있다. 문자 3자를 하나의 블럭으로 지정하므로 "EXP", "ONE", "NT ", "CRY", "PTO", "SYS", "TEM" 등 7개의 블록으로 표현된다.

〈표 3〉 지수 암호시스템 데이터

〈Table 3〉 Exponent cryptosystem data

송신문(W)			EXPONENT CRYPTOSYSTEM									
10진 송신문	블럭	1	5				24				16	
		2	15				14				5	
		3	14				20				0	
		4	3				18				25	
		5	16				20				15	
		6	19				25				19	
		7	20				5				13	
암호문(C)	블럭	1	0	20	17	6	25	9	9	4	9	27
		2	2	18	19	0	25	15	9	15	27	27
		3	9	25	10	19	14	20	27	21	21	20
		4	18	3	4	26	22	27	25	20	15	0
		5	27	25	21	23	21	13	18	4	7	23
		6	6	23	25	22	1	24	11	8	10	27
		7	16	9	3	1	12	3	16	11	4	19
10진 수신문	블럭	1	5				24				16	
		2	15				14				5	
		3	14				20				0	
		4	3				18				25	
		5	16				20				15	
		6	19				25				19	
		7	20				5				13	
수신문(W)			EXPONENT CRYPTOSYSTEM									



〈그림 3〉 공개키 지수 암호시스템

〈Fig. 3〉 Public key Exponent Cryptosystem

(그림 3)은 키생성에 필요한 자료와 송신문을 입력, 공개키, 비밀키, 암호문, 수신문 등을 나타내주는 공개키 지수 암호시스템이다.

V. 결론

컴퓨터 통신 기술의 발달로 컴퓨터 네트워크는 고도 정보화 사회에서 중요성이 한층 높아지고 있으며, 이러한 정보 시스템의 정상적인 기능 유지는 무엇보다 중요한 요소가 되고 있다.

본 논문에서는 컴퓨터 네트워크의 보안을 위해서 공개키 다항식을 인수분해 하는 데 어려움이 있는 공개개키 다항식 지수 암호 알고리즘을 제안하였다. 제안된 공개키 다항식 지수 암호 시스템은 공개키 다항식에 2개의 3변수 다항식을 사용하여, $f(x,y,z)=g(x,y,z)=0 \bmod p$를 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 보다 더 안전성을 가진 암호로 되었다. 컴퓨터 시뮬레이션을 통해 주어진 문자 평문에 대하여 암호화하고 해독하여 제안된 공개키 다항식 지수 암호 시스템의 타당성이 입증되었다.

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] 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.

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

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

[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 Exponential Cryptosystem for Security in Computer Networks

Tae-Kyu, Yang*

Abstract

In this paper, a public key exponential encryption algorithm for data security of computer network is proposed. This is based on the security to a difficulty of polynomial factorization. For the proposed public key exponential encryption, the public key generation algorithm selects two polynomials f(x,y,z) and g(x,y,z). The enciphering first selects plaintext polynomial W(x,y,z) and multiplies the public key polynomials, then the ciphertext is computed. In the proposed exponential encryption system of public key polynomial, an encryption is built by exponential encryption multiplied thrice by the optional integer number and again plus two public polynomials f(x,y,z) and g(x,y,z), This is an encryption system to enforce the security of encryption with help of prime factor added on RSA public key. The propriety of the proposed public key exponential cryptosystem algorithm is verified with the computer simulation.

* School of IT Engineering, Mokwon University