안전성이 높은 다변수 Knapsack 암호시스템

이 병 수†

요 약

고도의 정보화 사회에서 데이터의 내용변경,중요한 데이터의 불법적인 유출, 순서 변경 그리고 미확인 송신자와 수신자등에 의하여 항상 위협을 받음으로써 데이타의 안전성이 요구되고 있다.본 연구에서는 컴퓨터 통신의 안전을 위한 다변수 Knapsack 암호시스템을 제안하였다.이 시스템은 기존의 Knapsack 암호시스템보다도 간단하면서 높은 안전성을 갖는다.그리고 제안된 암호 시스템은 초증가벡터의 각 요소를 변형하여 다변수 다항식으로 표현한 것을 암호벡터로 구성한다.암호문의 복호는 비밀의 정수와 초증가벡터를 사용하면 평문이 구해진다.따라서 이 암호의 안전성은 비밀의 정수를 다변수 다항식으로 나타내는 암호벡터에 대입할 때 암호벡터가 초증가벡터로 되는 근을 구하는 것의 어려움에 근거하고 있다.제안된 다변수 Knapsack 암호시스템의 타당성이 컴퓨터 시뮬레이션을 통하여 입증되었다.

High-Secure Multivariable Knapsack Cryptosystem

Byoung Soo Lee†

ABSTRACT

In the high information societies,the requirement of encryption security is increasing so as to protect information from the threat of attacks by illegal changes of data,illegal leakage of data, disorder of data sequences and the unauthorized sender and an unauthorized receiver etc.In this paper,multivariable knapsack cryptosystem is proposed for security of computer communication. This system is securer and simpler than the conventional knapsack cryptosystems. And, proposed cryptosystem composed what represented each element of superincreasing vector with multivar able polynomial after transforming it of ciphervector. For the deciphering of ciphertext,the plaintext is determined by using the integers of secret and the superincreasing vector of secret key. Thus, the stability of this cryptosystem is based on the difficulty of obtaining the root that ciphervector becomes the superincreasing vector, in substituting the integers of secret for ciphervector to represent with the miltivariable polynomial.The propriety of proposed multivariable knapsack cryptosystem was proved through computer simulation.

1. 서 론

고도의 정보화 사회에서 컴퓨터 통신망(computer communication network)은 컴퓨터 기술과 통신 기술의 결합체로 발전하여 종합정보통신 시스템이 구축되고 있으며 사용자에게 요구되는 각종 뉴미디어(new media) 서비스를 제공해 주고 있다.그러나 실제 통신장치,통신 선로등으로 구성되는 통신망에서는 도청자가 통신중인 정보를 도청(eavesdropping)하여 해독하므로써 정보가 누출되거나 데이터를 변조(modification),삽입(injection) 및 삭제(deletion)등이 가능하기 때문에 이를 방지하기 위해서 컴퓨터 및 통신 시스템상에서 정보 보호를 위한 암호화 연구가 활발히 진행되고 있다. 암호화 기법(cryptographic)은 데이터에 대한 변조 또는 정보의 누출을 방지하기 위해서 데이터를 암호화시켜 저장하거나 전송함으로써 비밀키를 알고 있는 인증(authentication)된 사람이 아니면 해독을 할 수 없도록 하는 기술로서 평문(plaintext,message),

† 종신회원 : 인천대학교 전자계산학과 부교수
논문접수 : 1995년 7월 3일, 심사완료:1995년 8월 1일

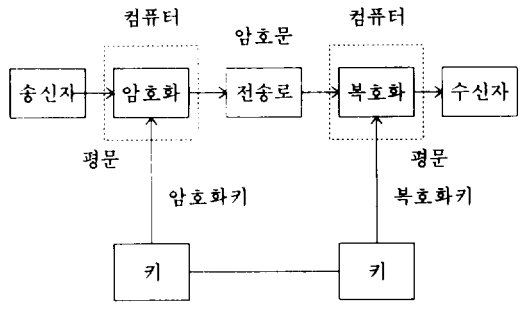
키(key), 알고리즘(algorithm), 암호문(cipher-text)으로 구성되어 있다[1]. 암호시스템은 암호키의 분배와 관리 방법에 따라 관용 암호시스템(conventional cryptosystem)과 공개키 암호시스템(public key cryptosystem)으로 크게 나눌 수 있다. 전자는 암호화키와 복호화키가 동일한 시스템으로 이 두 키는 송신자와 수신자가 공용하는 비밀키가 되며,블럭암호(block cipher)에 속하는 DES(Data Encryption Standard), FEAL (Fast Data Encipherment Algorithm) 및 스트림 암호(stream cipher)등이 있다. 후자는 암호화키와 복호화키가 서로 다르며 암호화키는 공개하고 복호화키는 비밀로 보관하는 공개키(public key)와 비밀키(secret key)를 이용하여 키 전송이 필요치 않는 암호시스템으로 1976년 Diffie-Hellman[2]이 One-way함수를 이용한 공개키 개념을 도입함으로써 기존의 관용 암호시스템의 키 분배 문제를 해결하고,인증과 디지탈 서명(digital signature)이 가능한 공개키 암호 시스템을 제안한 이후 연구가 현재 활발이 진행되고 있다.대표적인 공개키 암호 알고리즘에는 1978년 Rivest,Shamir와 Adleman[3]에 의해 큰 합성수를 소인수분해하는 어려움에 근거한 RSA암호, 1978년에 Merkle와 Hellman[4],Chor와 Rivest[6]등에 의해 수열의 초증가성인 knapsack 문제의 어려움에 근거한 MH knapsack 암호, 1985년에 Elgamal[7]에 의해 유한체상의 이산적 대수(discrete logarithm)문제의 어려움에 근거한 암호등이 있다.

본 논문에서는 초증가벡터 A의 요소 a_i를 비밀의 정수 z_i를 변수로 하여 다항식 즉, $a_i \equiv b_{i1}z_1 + b_{i2}z_2 + r_i \pmod p$로 변환하여 $b_{i1}z_1 + b_{i2}z_2 + r_i$를 요소로 하는 암호벡터를 이용한 다변수 Knapsack 암호시스템을 제안한다. 이 암호는 비밀정수 z_i의 값을 알고 있는 정당한 수신자는 수열의 초증가성을 이용하여 복호를 할 수 있으나 공개키의 요소 b_{ij}, r_i의 값만으로 초증가벡터를 구하는 것은 불가능하며, 또 z_i의 수를 증가면 해독이 보다 곤란하게 되어 안전성을 더욱 높일 수가 있다.한편 컴퓨터 시뮬레이션을 통하여 주어진 평문에 대해 암호화하고 복호화하여 알고리즘의 타당성을 보였다.

2. 암호 시스템

2.1 암호시스템의 개념

데이터 보호를 위한 암호시스템은 (그림 1)과 같이 크게 송신자, 암호화, 복호화, 키, 전송로, 수신자 및 해독자로 구성된다. 송신자가 수신자에게 보내고 싶은 보통의 통신문을 평문(Plain-text)이라 한다. 평문을 이해할 수 없는 암호문(cipher)으로 변환하는 조작을 암호화(encipher-ment)라고 한다. 또 역으로 암호문을 원래의 평문으로 바꾸는 조작을 복호화(decipherment)라 한다. 복호화는 정당한 수신자가 정당한 절차를 통해 평문을 복원하는 경우를 말하며, 부당한 제3자가 다른 수단을 이용하여 평문을 추정하는 것

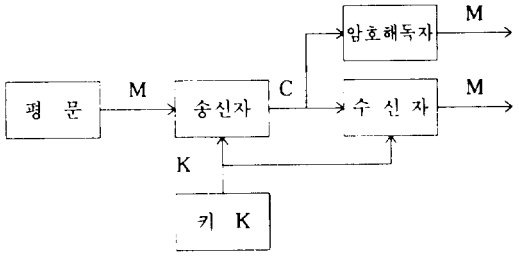


(그림 1) 암호시스템의 블럭도
(Fig.1) Block diagram of Cryptosystem

을 해독(cryptoanalysis)이라 한다. 암호화와 복호화의 조작 원리를 암호 알고리즘이라고 하며, 암호 알고리즘에 의한 변환을 제어하는 파라미터를 키(key)라고 한다. 일반적으로 암호시스템은 암호키의 분배와 관리 방법에 따라 관용암호시스템(conventional cryptosystem)과 공개키 암호시스템(public key cryptosystem)으로 크게 나눌 수 있다[1].

2.2 관용 암호시스템

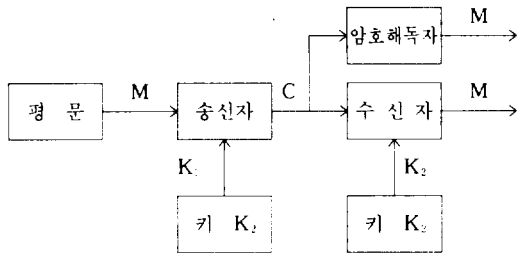
관용 암호시스템은 (그림 2)와 같이 단일키 암호화 방식으로 통신하고자 하는 사용자 사이에 연결된 회선상으로 정보를 전송하는 과정에서 정보의 노출을 막기 위하여, 사용자가 공통적으로 갖고 있는 단일키로 암호화하고 해독하는 시스템이다. 여기서 K는 비밀키, M은 암호화되지 않은 평문,C는 암호화된 암호문,M는 도청자가 얻은 평문이다.관용 암호시스템에서는 송신자와 수신자가 동시에 동일한 키를 가져야 하므로 어느 한쪽에서 반드시 상대방에게 약속된 키를 보내야 하는데, 이 과정에서 키가 노출될 수도 있다는 것이 관용 암호시스템의 가장 큰 단점이다[1, 10].



(그림 2) 관용 암호시스템
(Fig.2) Conventional Cryptosystem

2.3 공개키 암호시스템

관용 암호시스템의 단점은 1976년에 최초로 Diffie와 Hellman[2] 에 의해 제안된 공개키 암호 시스템의 개념으로서 해결될 수 있게 되었다. 이러한 시스템을 제안한 후에 1976년 Rivest, Shamir와 Adleman[3]에 의해 멱암호인 RSA암호시스템이 제안되었고, Merkle와 Hellman, Chor[6]등에 의해 Knapsack 문제를 사용한 MH암호시스템등이 제안되었다.따라서 공개키 암호시 스템은 (그림 3)과 같이 암호키 K_1과 해독키 K_2가 다르며, 암호키에서 해독키를 만들어 낼 수 없 다는 것이다. 이 시스템에서 송신자가 사용하는 암호키 만을 공개하고 수신자는 얻더라도 원래 의 평문을 얻기가 어렵게 된다. 또한 관용 암호시스템에서 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 functtion)을 이용하여 키의 갯수는 n에 비례한다[1,11].



(그림 3) 공개키 암호시스템
(Fig.3) Public Key Cryptosystem

2.4 Knapsack 암호 시스템

Knapsack 암호 시스템은 1978년 Merkle 와 Hellman[4]에 의하여 Knapsack 문제가 최초로 공개키 암호 기법에 적용되었다. Knapsack 문제는 주어진 정수의 집합 $A=(a_1, a_2, \cdots, a_n)$와 이것의 합 S가 주어졌을 때 S가 A의 부분합이 되는지 또는 A의 어떤 원소들의 합이 S가 되는지 알아내는 문제이다.즉, $S=\sum a_i m_i (1\leq i\leq n)$를 만족하는 2진 벡터 $M=(m_1, m_2, \cdots, m_n)$을 찾아내는 문제이다.정수 벡터 A에서 그 부분집합의 합 S를 구하는 것은 쉽지만 그 역과정인 Knapsack 문제는 일반적으로 풀기 어려운 NP-complete 문제로 잘 알려져 있다[1].

Knapsack 벡터 $A=(a_1, a_2, \cdots, a_n)$에서 각 원소의 크기가 그 이전의 원소의 합보다 큰 경우에 A는 초증가한다고 한다. 즉,

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

와 같이 무작위하게 초증가하는 Knapsack 벡터 A를 선택하고 $\sum a_i (1 \le i \le 1)$보다 큰 정수 p와 이에 서로소인 정수 w를 임의로 정한다. 즉,

$$p > \sum_{i=1}^{n} a_i \quad (2)$$

$$GCD(p, w)=1, p>w, w \cdot w^{-1}=1 \pmod p \quad (3)$$

그리고 공개키가 되는 trapdoor Knapsack벡터 $A' = (a_1', a_2', \cdots, a_n')$는 쉬운 Knapsack 벡터 A의 각 원소 a_i에 w를 곱한 다음 법 p를 연산하여 얻는다. 즉,

$$a_i' = a_i \cdot w \pmod p \quad (4)$$

따라서 trapdoor Knapsack벡터 A'는 공개키가 되고, 법 p와 이에 서로소인 정수 W 및 초증가하는 Knapsack 벡터 A는 비밀키가 된다.

이제 원문을 2진수 평문 $M=(m_1, m_2, \cdots, m_n)$으로 변환시켜 공개키인 trapdoor Knapsack 벡터 A'를 사용하여 식(5)와 같이 암호화한다.

$$S = \sum_{i=1}^{n} a_i' m_i \quad (5)$$

다음에 비밀 정보인 W^{-1}과 를 알고 있는 수신자는 평문을 식(6)과 같이 복호화할 수 있다.

$$\begin{aligned} D &= w^{-1} \cdot C \pmod p \\ &= w^{-1} \sum_{i=1}^{n} b_i m_i \pmod p \\ &= w^{-1} \sum_{i=1}^{n} (a_i W) m_i \pmod p \\ &= \sum_{j=1}^{n} (w^{-1} w a_i) m_i \pmod p \\ &= \sum_{i=1}^{n} a_i m_i \pmod p \\ &= A \cdot M \end{aligned} \quad (6)$$

다음에 벡터 A의 초증가성을 이용하여 평문 $M=(m_1, m_2, m_n)$을 구한다.

한편 Knapsack 암호시스템의 가장 큰 장점은 다른 공개키 암호 시스템에 비하여 암호화 및 복호화의 계산이 매우 쉽다는 것이다.그러나 MH Knapsack 암호는 안전성을 위해서 암호화할 때 데 이타의 확장이 불가피하다.또한 공개키는 어려운 Knapsack 벡터로 구성되어 있으므로 공개키의 크기가 매우 커지게 된다. 그러므로 Merkle과 Hellman은 안전상의 관점에서 n이 100 이상이 되어야 한다고 했다.

이러한 Knapsack암호가 발표된 이후 집중적인 암호 분석의 대상이 되어 왔으며,많은 경우에 성공적인 결과를 얻었다.Knapsack암호의 안전성에 대한 의문이 제기되는 이유 중의 하나는 이 암호가 근본적으로 선형이라는 점이다.일반적으로 선형성은 암호시스템의 안전성에 해롭다고 알려지고 있다.한번 변환시킨 Merkle-Hellman암호에 대하여 Shamir가 최초로 성공적인 암호분석을 하였다[11].그는 Lenstra의 정수 계획법 알고리즘을 이용하여 공개된 Knapsack 벡터에서 이를 초증가하는 Knapsack벡터로 변환시키는 (W, p)를 발견하였다. Shamir의 방법은 다른 Knapsack암호에 대한 일반적인 암호분석이 되지 못했는데,Adleman이 Lovasz의 lattice basis reduction알고리즘[13]을 사용하여 Graham-Shamir Knapsack 암호시스템을 분석하였다. 이 알고리즘은 초증가하는 단순 Knapsack 벡터를 법 변환시키는 모든 Knapsack 암호를 암호분석하는 데 이용하였다. 또한 잘 알려진 Knapsack암호의 분석방법으로 Lagarias와 Odlyzko [12]의 저밀도 Knapsack 암호분석이 있다.이 방법은 밀도가 낮은 모든 Knapsack암호에 적용된다.

3. 제안된 다변수 Knapsack 암호 시스템

본 논문에서는 해독이 보다 곤란하도록 비밀의 정수를 변수로 하여 초증가벡터의 요소를 다항식으로 변환하여 안전성을 높인 다변수 Knapsack 암호시스템을 제안한다.

3.1 키 생성

먼저 식(7), (8)를 만족시키는 초증가벡터 $A=(a_1, a_2, \cdots, a_n)$와 법 p의 값을 정한다.

$$a_i > \sum_{j=1}^{i-1} a_j (i=2, \cdots, n) \quad (7)$$

$$p > \sum_{i=1}^{n} a_i \quad (8)$$

그리고 법 p와 (p,w)=1인 승수 w를 선택하여

$$w \cdot w^{-1} \equiv 1 \pmod{p} \quad (9)$$

가 되는 역원 w^{-1}을 구한다. 또 승수 w를 이용하여 초증가벡터 A를

$$A' = w \cdot A \equiv (a_1', a_2', \cdots, a_n') \pmod{p} \quad (10)$$

와 같이 모듈라 변환한다.다음에 $1 < z_j < p (1 \le j \le L)$을 만족시키는 임의의 정수 z_j를 L개 선택하여 변수로 하여 식(10)의 요소 a_i'를 z_j의 다항식으로

$$a_i' \equiv b_{i1}z_1 + b_{i2}z_2 + \cdots + b_{iL}z_L + r_i (1 \le i \le n) \pmod{p} \quad (11)$$

와 같이 변환하고,다음과 같이 나타낸다.

$$\begin{aligned} B = (&b_{11}z_1 + b_{12}z_2 + \cdots + b_{1L}z_L + r_1 \\ &b_{21}z_1 + b_{22}z_2 - \cdots + b_{2L}z_1 - r_2 \\ &\cdots\cdots \\ &b_{n1}z_1 + b_{n2}z_2 + \cdots + b_{nL}z_1 + r_n) \end{aligned} \quad (12)$$

이 요소의 배열순서를 적당히 바꾼 벡터를 암호벡터로 공개한다.

3.2 암호화

암호화는 송신하고자 하는 평문벡터 M을

$$M = (m_1, m_2, \cdots, m_n),\ m_i \in \{0, 1\},\ (1 \le i \le n)$$

로 나타내고,식(13)과 같이 행한 후 암호문의 다항식 계수 L개의 $B_j (1 \le j \le L)$와 R를 수신자에게 보낸다.즉

$$\begin{aligned} C &= B \cdot M \\ &= \sum_{i=1}^{n} (b_{i1}z_1 + \cdots + b_{iL}z_L + r_i)m_i \\ &= \sum_{i=1}^{n} b_{i1}m_iz_1 + \cdots + \sum_{i=1}^{n} b_{iL}m_iz_L + \sum_{i=1}^{n} r_im_i \\ &= B_1z_1 + \cdots + B_Lz_L + R \end{aligned} \quad (13)$$

그러므로 송신하고자 하는 n비트의 평문벡터 M을 암호화하면 (L+1)개의 10진수로 된 데이타로 변형되어 수신자에게 보내진다.

3.3 복호화

복호화는 수신된 암호문을 해독하기 위하여 먼저 식(13)의 암호문 C에 L개의 비밀정수 $z_j (1 \le j \le L)$를 대입하여 D를 구한다.즉

$$\begin{aligned} D_1(C) &= B_1z_1 + B_2z_2 + \cdots + B_Lz_L + R \ \vdots\ z_1 = z_1, \cdots, z_L = z_L \\ &\equiv \sum_{i=1}^{n} b_{i1}m_iz_1 + \cdots + \sum_{i=1}^{n} b_{iL}m_iz_L + \sum_{i=1}^{n} r_im_i \\ &\equiv \sum_{i=1}^{n} (b_{i1}z_1 + r_{i1} + \cdots + b_{iL}z_L + r_{iL})m_i \\ &\equiv \sum_{i=1}^{n} a_i' m_i \\ &\equiv \sum_{i=1}^{n} wa_im_i \pmod{p} \\ &\equiv \sum_{i=1}^{n} \end{aligned} \quad (14)$$

를 구한 다음에 역원 w^{-1}을 곱하여

$$\begin{aligned} D_2(C) &= w^{-1}D_1(C) \pmod{p} \\ &\equiv \sum_{i=1}^{n} a_im_i \pmod{p} \end{aligned} \quad (15)$$

와 같이 계산한다. 다음에 초증가벡터의 배열순서를 바꾼 벡터 $A^* = (a_1^*, a_2^*, \cdots, a_n^*)$의 초증가성을 이용하여 평문 $M = (m_1, m_2, \cdots, m_n)$을 얻을 수 있다.

제안된 다변수 Knapsack 암호는 L개의 비밀정수 z_j인 변수의 값이 없이 b_{ij}, r_i의 값만으로 초증가벡터를 구할 수가 없으므로 해독하는 것이 불가능하여 안전하다.또한 비밀의 정수를 확장함으로써 전수검사에 요하는 시간을 많이하여 안전성을 높일 수 있다.그러나,암호문의 길이는 평문의 길이의 (L+1)배가 된다.

4. 시뮬레이션 과정 및 결과

제안된 다변수 Knapsack 암호 시스템의 타당성을 입증하기 위하여 주어진 평문에 대하여 암호화하고 복호화하여 컴퓨터 시뮬레이션을 한다. 다음에 이 암호의 간단한 수치열을 나타낸다.

먼저 초증가벡터 A=(2,3,6,13,25,50,100,200),

법 p=417,승수 w=19로 정하면 역원 $w^{-1}=22$ 이다. 그리고 초증가벡터 A의 모듈라 변환을 행하면 다음과 같이 된다.

$$\begin{aligned}A' &= w \cdot A \\ &= 19(2,3,6,13,25,50,100,200) \pmod{417} \\ &\equiv (38,57,114,247,58,116,1900,3800) \\ &= (a_1', a_2', a_3', a_4', a_5', a_6', a_7', a_8')\end{aligned}$$

다음에 2개의 변수 $z_1=20$, $z_2=41$로 정한 값을 이용하여 모듈라 변환된 벡터 A′의 요소 a_i'를 다음과 같이 변환한다.

$$\begin{aligned}a_1' &= 38 \pmod{417} \equiv 0z_1+0z_2+38 \\ a_2' &= 57 \pmod{417} \equiv 1z_1+0z_2+37 \\ a_3' &= 114 \pmod{417} \equiv 2z_1+1z_2+33 \\ a_4' &= 247 \pmod{417} \equiv 6z_1+3z_2+4 \\ a_5' &= 58 \pmod{417} \equiv 1z_1+0z_2-38 \\ a_6' &= 116 \pmod{417} \equiv 2z_1+1z_2+35 \\ a_7' &= 1900 \pmod{417} \equiv 5z_1+2z_2+50 \\ a_8' &= 3800 \pmod{417} \equiv 1z_1+0z_2-27\end{aligned}$$

이 요소의 배열 순서를 다음과 같이 바꾼벡터를 암호벡터로 공개한다.

$$\begin{aligned}B &= (a_1', a_2', a_3', a_4', a_5', a_6', a_7', a_8') \\ &= (38,57,114,247,58,116,1900,3800) \\ &= (0z_1+0z_2+38,\ 1z_1+0z_2+37,\ 2z_1+1z_2+33, \\ &\quad 6z_1+3z_2+4,\ 1z_1+0z_2+38,\ 2z_1+1z_2+35, \\ &\quad 5z_1+2z_2+50,\ 1z_1+0z_2+27)\end{aligned}$$

또 평문을 M=(0,1,0,0,1,0,1,1)로 하면 암호화는

$$\begin{aligned}C &= B \cdot M \\ &= (1z_1+0z_2+37)+(1z_1+0z_2+38)+ \\ &\quad (5z_1+2z_2+50)+(1z_1+0z_2+27) \\ &= 8z_1+2z_2+152\end{aligned}$$

로 되어 암호문 8,2,152가 얻어진다.

한편, 복호는 먼저 $z_1=20$, $z_2=41$을 암호문에 대입하면

$$\begin{aligned}D_1(C) &= 8z_1+2z_2+152 \mid z_1=20, z_2=41 \pmod{417} \\ &= 394\end{aligned}$$

이고, 여기에 역원 $w^{-1}=22$를 곱하면 다음과 같다.

$$\begin{aligned}D_2(C) &= w^{-1}D(C) \pmod{p} \\ &= 22 \times 394 \pmod{417} \\ &\equiv 328\end{aligned}$$

따라서 배열 순서를 바꾼 벡터 A'=(2, 3, 6, 13, 25, 50, 100, 200)의 초증가성을 이용하여 평문 M=(0, 1, 0, 0, 1, 0, 1, 1)이 얻어진다. 〈표 1〉에서 〈표 4〉는 송신하고자 할 평문「Knapsack Public Key Cryptosystem」을 시뮬레이션한 결과 송신 2진수 평문,암호문,복호화키,수신 2진수 평문을 각각 나타낸 것이다. 여기에서 송신2진수 평문은 원문의 각 문자에 대응하는 8비트 2진수로 나타내었고,비밀의 정수를 사용한 암호화 알고리즘을 적용하면 암호문이 얻어진다.그리고 수신2진수평문을 8비트2진수에 대응시키면 원문「Knapsack Public Key Cryptosystem」을 얻을 수 있다.즉 송신 원문 [Knapsack Public Key Cryptosystem] 의 첫번째 문자 [K]를 8비트 2진수로 바꾸면 [01001011]과 같은 송신 2진수 평문이 되고,암호 알고리즘을 적용하면 암호문 [8, 2, 152]가 얻어진다. 이 암호문을 수신자가 복호하면 수신 2진수 평문 [01001011]을 얻고 원문으로 바꾸면 송신한 문자 [K]를 얻는다. 송신평문에서「Knapsack」에 있는 대소문자「K」와「k」의 암호문은 각각「8, 2, 152,「10, 3, 185」와 같이 다르게 되어 해독이 어렵게 됨을 알 수 있다. 그러나, 암호문의 길이는 평문길이의 3배로 길어지나 비밀정수의 수를 증가하면 전수검사에 요하는 시간이 많아져 안전성을 더욱 높일 수가 있다고 본다.

제안된 다변수 Knapsack 암호시스템은 초증가 벡터의 요소를 변형하여 다항식으로 표현한 암호 벡터를 다시 이 벡터의 배열순서를 적당히

〈표 1〉 송신 2진수 평문(M)
〈Table 1〉 Sender Binary Digit Plaintext(M)

01001011	01101110	01100001	01110000
01110011	01100001	01100011	01101011
00100000	01010000	01110101	01100010
01101100	01101001	01100011	00100000
01001011	01100101	01111001	00100000
01000011	01110010	01111001	01110000
01110100	01101111	01110011	01111001
01110011	01110100	01100101	01101101

바꾼 벡터를 암호벡터로 공개한다.이 암호의 안전성은 다변수 다항식 암호 벡터에 비밀의 정수를 대입하여 초증가벡터를 구하는 데 어려움이 있다. 또 안전성을 높이기 위해서는 암호 해독을 위한 전수검사에 요하는 시간을 많이 하기 위해서 비밀의 정수를 높이고 법의 값을 가능한 작게 정한다.

〈표 2〉 암호문(C)
〈Table 2〉 Ciphertext(C)

8	2	152	11	4	193	4	1	97	9	4	74
15	6	151	4	1	97	9	3	147	10	3	185
2	1	33	7	3	41	12	5	136	8	3	120
6	2	143	5	1	135	9	3	147	2	1	33
8	2	152	6	2	132	11	4	139	2	1	33
7	2	114	14	6	124	11	4	139	9	4	74
11	5	109	12	4	220	15	6	151	11	4	139
15	6	151	11	5	109	6	2	132	7	2	170

〈표 3〉 복호화키(D)
〈Table 3〉 Decryption Key(D)

328	184	209	22
322	209	309	334
6	16	272	109
84	234	309	6
328	259	247	6
303	122	247	22
72	384	322	247
322	72	259	284

〈표 4〉 수신 2진수 평문(M)
〈Table 4〉 Received Binary Digit Plaintext(M)

0 0 1 0 1 1	1 0 1 1 1 0	1 0 0 1 0 1	1 0 1 1 0 1
1 1 0 1 0 0	1 0 1 1 1 1	1 1 0 0 1 1	1 1 1 0 0 1
1 1 0 0 1 1	1 1 0 1 0 0	1 1 1 0 0 1	1 0 0 0 0 0
0 0 0 0 1 1	1 1 0 0 1 0	1 1 1 0 0 1	1 1 0 0 0 0
1 0 1 0 0 1	1 0 0 0 1 1	1 0 0 0 0 0	0 0 1 0 1 1
1 0 0 1 0 1	1 0 0 0 0 0	0 1 0 0 0 0	1 1 0 1 0 1
1 0 0 0 1 0	1 0 1 1 0 0	1 0 0 0 0 1	1 1 0 0 0 0
1 1 0 0 1 1	1 0 0 0 0 1	1 0 0 0 1 1	1 0 1 0 1 1

5.결 론

본 논문에서는 컴퓨터 통신의 안전을 위한 다변수 Knapsack암호시스템을 제안하였다. 제안된 암호시스템은 암호화와 복호화가 용이한 공개키 암호의 알고리즘을 구하는 목적으로 MH Knapsack암호의 암호벡터를 수정한 것으로,비밀의 정수 z_i를 변수로 하여 초증가벡터 A의 요소 a_i를 $a_i=b_{i1}z_1+b_{i2}z_2+r_i(\mathrm{mod}\ p)$로 변환하여, 그것을 요소로 하는 암호벡터를 이용하였다. 암호문의 복호는 비밀의 정수와 초증가벡터를 사용하면 평문이 구해진다.이 암호의 안전성은 z_i의 값을 알고 있는 정당한 수신자는 수열의 초증가성을 이용하여 복호를 할 수 있으나 공개키의 요소 b_{ij}, r_i의 값만으로 초증가벡터를 구하는 것은 불가능하고 또 비밀의 정수 z_i를 증가하면 해독이 보다 곤란하여 안정성을 어느 정도 높일 수가 있다고 본다. 또 해독이 보다 어려운 다변수의 변형 Knapsack암호로 확장하는 것이 가능하다.그러나 암호문의 길이는 평문길이의 3배로 된다.제안된 암호시스템의 안전성을 컴퓨터 시뮬레이션을 통하여 입증하였다.

참 고 문 헌

[1] 池野信一, 小山謙二, 현대 암호이론, 일본전자정보통신학회, 1989.

[2] W.Diffie and M.E. Hellman, "New Direction in Cryptography", IEEE Trans.Inform. Theory, Vol. IT-22, No. 1976.

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

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

[5] W. Diffie and M.Hellman, "Privacy and Authentication : An Introduction to Cryptography", Proc. IEEE, Vol. 67, pp. 397-527, 1979.

[6] B.Chor and R.L.Rivest, "A Knapsack-Type Public Key Cryptosystem Based on in Arithmetic in Finite Fields", IEEE Trans.Inf. Theory, Vol. 34, No. 5, pp. 901-909,1988.

[7] T.Egamal,"A Public Key Cryptosystem

and a Signature Scheme Based on Discret Logarithms", IEEE Trans. Inf. Theory, Vol. IT-31, No. 4, pp. 469-472, 1985.

[8] M.E. Hellman, "An Overview of Public Key Cryptography", IEEE Communication Society Magazine, pp.24-32, 1978.

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

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

[11] Shamir, A., " Polynomial Time Algorithm for Breaking the Basic Merkle-Hellman Cryptosystem, IEEE Trans.on Informat.Theory 30, pp. 699-704,1984.

[12] J.C.Lagarias and A.M.Odlyzko, "Solving lowdensity subset sum problems", J.Ass. Comput. Mach. vol. 32, 1, pp. 229-246, Jan.1985.

[13] A. K. Lenstra, H. W. Lenstra, Jr. and L. Lovasz, Factoring Polynomial with Rational Coefficients, Mathematische Annalen 261, pp. 515-534, 1982.

이 병 수

1976년 단국대학교 공과대학 전자공학과 졸업(학사)
1980년 동국대학교 경영대학원 정보처리전공(석사)
1981년~현재 시립인천대학교 전자계산학과 부교수
관심분야 : 의사결정지원시스템, 스프트웨어공학, 컴퓨터통신