# 미래과학자 양성 프로그램

# 수 학

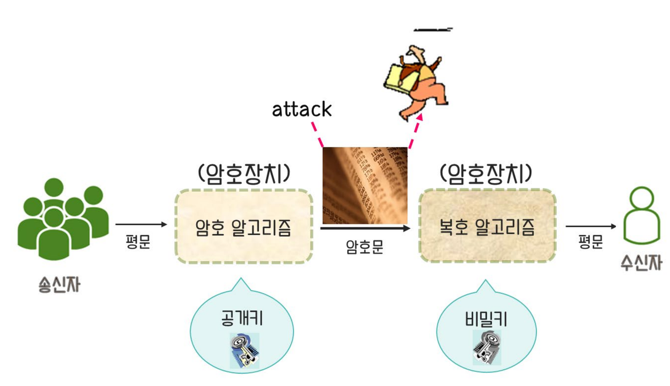
# 이산대수 기반 공개키 암호 방식 연구

경산과학고등학교 1학년 강 민 석
김 화 영
윤 창 호
장 민
지도교사 김 형 섭
금오공과대학교 응용수학과 교수 유 원 석

## 1. 서론

현대사회가 점점 정보화 사회로 발전함에 따라 다양한 종류의 정보를 교환하는데 필요한 대량 정보시스템이 구축되고, 이에 따라 정보를 안전하게 교환할 수 있는 암호방법의 중요성이 강조되고 있다. 이러한 암호방법 중 1980년대부터 소개된 공개키 암호방법은 키의 배송문제와 관리문제를 해결하고 다양하게 응용되는 장점이 있어 현재도 여러 가지 알고리즘이 발표되어 활용되고 있다.

공개키 암호의 개념




## 2. 연구 배경

공개키 암호 알고리즘은 대부분 풀기 어려운 계산 문제 즉, 이산대수 문제에 근거를 두고 개발되었으나 컴퓨터 계산 능력의 발전에 따라 보안성의 문제 때문에 현재는 소수의 알고리즘만이 실용화되고 있다([4]). 따라서 공개키 암호 알고리즘의 안전성을 높일 수 있는 여러 가지 방안을 연구하고 새로운 암호 알고리즘을 개발할 필요가 있다.

## 3. 연구 방법

이 연구를 수행하기 위하여 먼저 배낭암호([1]), 타원곡선 암호([3]) 등의 안전성의 문제점을 알아보고 이를 개선하기 위한 여러 가지 방안을 연구한다. 이 과정에서 행렬의 성질과 벡터의 직교 공간의 성질을 응용하여 보안성을 높이는 방법을 연구하며, 배낭암호, 타원곡선암호 등을 혼합한 새로운 암호 알고리즘을 개발한다.

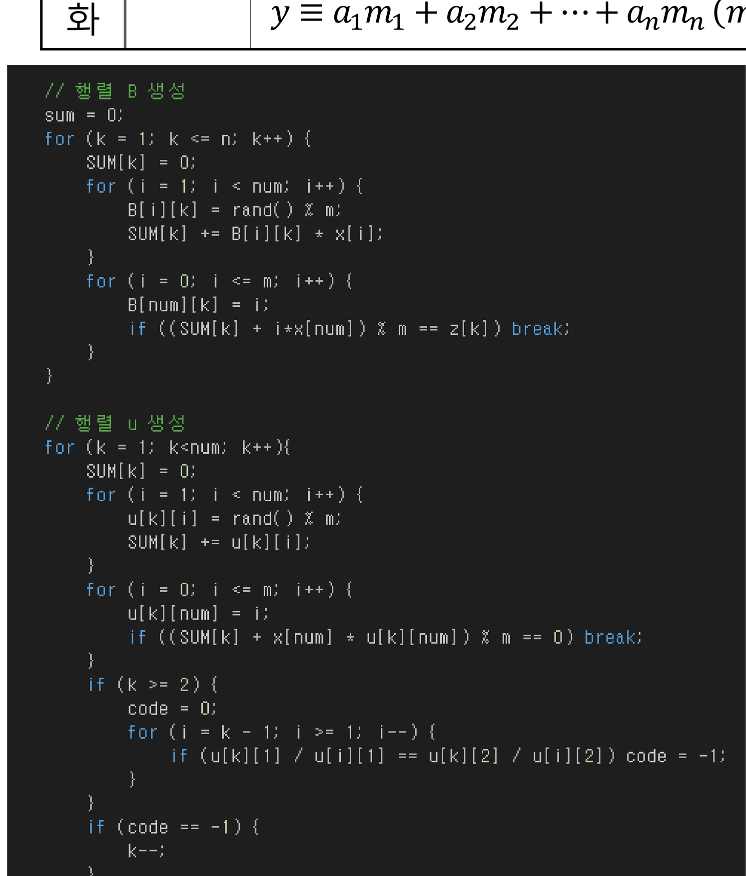
## 4. 연구 결과

이 연구에서는 배낭암호와 타원곡선암호에서 이용하고 있는 이산대수 문제를 응용하여 보안성이 강화된 새로운 세 개의 공개키 알고리즘을 개발하고, 이 중 하나의 알고리즘에 대해서는 전산프로그램으로 개발하여 컴퓨터를 통해 암호화 및 복호화 과정을 실행한다.

### (1) 행렬과 초월증가수열을 이용한 공개키 암호 알고리즘 1

배낭암호 알고리즘을 개선한 것으로서 기존 초월증가수열 이외에도 벡터공간에서 벡터의 독립성과 직교성을 이용하여 안정성을 높여준다([2]).

| 단계 | 행위자 | 내 용 |
|---|---|---|
| 준비 | 수신자 | ① 양의 정수 $n,\ l,\ k$ 를 $k<l\le n$ 이 되도록 택하고, $a_1+a_2+\cdots+a_n<m$을 만족하는 초월증가수열 $a_1,a_2,\cdots,a_n$을 $\mathbb{Z}_m$에서 택한다.<br>② $\mathbb{Z}_m$ 의 원소로 된 벡터 $\vec{x}=(x_1,x_2,\cdots,x_l)$ 와 $l\times n$ 행렬 $B$를<br>$\vec{x}B=(a_1,a_2,\cdots,a_n)(mod\ m)$<br>가 되도록 선택한다.<br>③ $\mathbb{Z}_m^l$ 에서 서로 독립이면서 $\vec{x}$ 에 서로 직교하는 벡터들<br>$\overrightarrow{u_1},\overrightarrow{u_2},\cdots,\overrightarrow{u_k}$<br>를 선택한다.<br>- - - - -<br>행렬 $B$와 벡터 $\overrightarrow{u_1},\overrightarrow{u_2},\cdots,\overrightarrow{u_k}$ 를 공개한다. |
| 암호화 | 송신자 | 길이가 $n$인 이진평문 $\vec{m}$과 공개키 $B,\ \overrightarrow{u_1},\ \overrightarrow{u_2},\ \cdots,\ \overrightarrow{u_k}$ 가 주어질 때,<br>① Span $\{\overrightarrow{u_1},\overrightarrow{u_2},\cdots,\overrightarrow{u_k}\}$ 에서 임의로 $n$ 개의 벡터를 택하고, 이들 벡터들을 각 열로 놓은 크<br>기 $l\times n$의 행렬을 $H$라고 한다.<br>② 암호문 $\vec{C}=(B+H)\vec{m}^T\ (mod\ m)$ 을 만든다. |
| 복호화 | 수신자 | $y\equiv\overrightarrow{x}\,\overrightarrow{c}(mod\ m)$ 을 계산하면,<br>$y\equiv a_1m_1+a_2m_2+\cdots+a_nm_n\,(mod\ m)$ 이 되어 이진평문 $\vec{m}$ 을 구할 수 있다. |



### (2) 행렬과 초월증가수열을 이용한 공개키 암호 알고리즘 2

앞에서 소개한 공개키 암호 알고리즘과는 달리 아래에 소개하는 알고리즘에서는 송신자가 임의로 행렬을 선택하여 메시지를 간단하게 암호화 할 수 있는 장점이 있다.

| 단계 | 행위자 | 내 용 |
|---|---|---|
| 준비 | 수신자 | ① 이진평문의 블록 단위와 행렬의 크기 $(n\times n)$ 로 사용할 $n$을 선택한다.<br>② 초월증가수열로 이루어진 행렬 $A=(a_1,a_2,\cdots,a_n)$ 와 $a_1+a_2+\cdots+a_n<m$ 을 만족하는 $m$을 선택한다.<br>③ 비밀키 행렬 $K=(k_1,k_2,\cdots,k_n)$ 와 $k_1s_1+k_2s_2+\cdots+k_ns_n\equiv 0(mod\ m)$을 만족하는 $k_i,s_i\in\mathbb{Z}_m(1\le i\le n)$을 선택하고, 모든 열이 $\begin{bmatrix}s_1\\s_2\\\vdots\\s_n\end{bmatrix}$으로 된 $n\times n$행렬을 $S$ 라 하자.<br>③$KB\equiv(a_1,a_2,\cdots,a_n)(mod\ m)$을 만족하는 $n\times n$ 행렬 $B$를 선택한다.<br>- - - - -<br>$n$ 과 $m$ , 행렬 $S$ 와 $B$를 공개하고, 행렬 $A$와 $K$는 비밀키로 보관한다. |
| 암호화 | 송신자 | ① $n\times n$ 행렬 $P=[p_{ij}]\ (p_{ij}\in\mathbb{Z}_m,\ 1\le i,j\le n)$을 임의로 선택한다.<br>② 행렬 $S$와 $P$및 행렬$B$ 를 사용하여 이진평문 $M=(m_1,m_2,\cdots,m_n),\ m_i\in\{0,1\}$을 $(SP+B)M^T\equiv C^T(mod\ m)$ 에 의하여 $C$로 암호화 한다. 즉, $(SP+B)\begin{bmatrix}m_1\\m_2\\\vdots\\m_n\end{bmatrix}\equiv\begin{bmatrix}c_1\\c_2\\\vdots\\c_n\end{bmatrix}(mod\ m)$을 계산하여 $M$을 $C=(c_1,c_2,\cdots,c_n)$으로 암호화한다. |
| 복호화 | 수신자 | 암호문 $C^T$의 왼쪽에 비밀키 $K$를 곱하여 얻은 숫자 $\alpha$는<br>$\alpha\equiv a_1m_1+a_2m_2+\cdots+a_nm_n(mod\ m)$ 이 되므로, 초월증가수열의 성질을 이용하여 이진평문 $M=(m_1,m_2,\cdots,m_n)$ 을 복호화할 수 있다. |

### (3) 타원곡선암호와 초월증가수열을 응용한 새로운 공개 암호키 3

이 알고리즘은 타원곡선암호와 배낭암호 알고리즘을 동시에 응용하여 안전성을 높인 것으로, 수신자가 준비해야 하는 과정은 타원곡선 암호 알고리즘과 동일하나 송신자가 메시지를 암호화하면서 초월증가수열을 이용하기 때문에 배낭암호 보다 안전성이 높다.

| 단계 | 행위자 | 내 용 |
|---|---|---|
| 준비 | 수신자 | ①유한체 $F=GF(p)=\mathbb{Z}_p$ 위의 타원곡선군 $E(F)$를 택하고, $E(F)$의 원소 중 큰 위수를 갖는 원소 $P$를 택한다.<br>② 임의의 정수 $\alpha$ 를 택하고, $Q=\alpha P$인 $Q$를 계산한다.<br>- - - - -<br>$(F=GF(p),E(F))$및 $P$와 $Q$를 공개키로 공개하고, $\alpha$는 비밀키로 보관한다. |
| 암호화 | 송신자 | ① 임의의 정수 $k$를 택하여 $kP,\ kQ=(c_1,c_2)$ 를 계산한다.<br>② 초월증가수열 $a_1,a_2,\cdots,a\sum_{i=1}^{n}a_i<p$ ) 을 택하고, $b_i\equiv c_1a_i\equiv(mod\ p)$를 계산한다.<br>③ 보내고자 하는 이진평문 $x=(x_1,x_2,\cdots,x_n)$으로부터<br>$S\equiv\sum_{i=1}^{n}b_ix_i\,(mod\ p)$<br>를 계산하고, 암호문으로 $C\equiv c_2S\ (mod\ p)$를 구한다.<br>④ 초월증가수열 $a_1,a_2,\cdots,a_n,\ kP,C$ 를 보낸다. |
| 복호화 | 수신자 | ① $\alpha kP\ =(c_1,\ c_2)$를 계산한다.<br>② $c_1^{-1}c_2^{-1}C\equiv c_1^{-1}c_2^{-1}(c_2S)\equiv\sum_{i=1}^{n}a_ix_i(mod\ p)$ 로부터 이진평문 $x=(x_1,x_2,\cdots,x_n)$ 을 얻는다. |

## 5. 결론 및 제언

이 연구에서 개발한 공개키 암호 알고리즘은 벡터 공간에서의 직교성, 행렬이론, 초월증가수열 등을 응용하고 기존의 알고리즘을 복합적으로 응용함으로써 기존의 타원곡선암호나 배낭암호 알고리즘에 비해 안정성이 높다. 따라서 이 연구에서 개발한 새로운 암호 알고리즘 개발에 대한 창의적 결과는 향후 암호학의 발전에 기여할 것으로 기대한다.

## 6. 참고 문헌

[1] 김흥수, 공개키 다항식을 사용한 배낭 암호 방식, 東州大學, 1999
[2] 정보통신부, 공개키 암호알고리즘 개발에 관한 연구, 한국정보보호센터, 1999
[3] 황규범, 이시창, 정명인, 암호학의 이해, 경문사, 2009
[4] James A. Buchmann, Introduction to Crytography. Springer, 2000