Newton-Raphson Method를 이용한 스트림 암호 알고리즘

신승호° 노희영
강원대학교 컴퓨터과학과
michael@kangwon.ac.kr, rohhy@kangwon.ac.kr

Stream Cryption Algorithm using a Newton-Raphson Method

Seung-Ho Shin° Hi-Young Roh
Dept. of Computer Science, Kangwon University

1. 서 론

암호에 대한 기대와 발전이 급격하게 대두되기 시작 한 것은 근대 들어서면서 국가 간의 전쟁에서 이기고자 하는 군사 목적으로써 많은 발전을 하였다. 이 전에도 암호를 사용하는 방법에 대한 여러 가지 방법이 있었지만 그때마다 사용하는 암호의 사용법은 주로 사용자들만이 아는 간단한 변환 과정을 거쳐서 주고받는 서신이나 연락체계에 불과 했다. 하지만 지금은 군사 목적 이외에도 통신의 발달로 인한 사람들의 서신이나 전자 상거래에도 암호는 중요한 위치에서 가장 긴요하게 쓰이고 있다.

이렇듯 암호는 통신의 발달로 전자적 왕래가 빈번한 현대를 살아가는데 있어서는 필수 불가결한 수단이 되어 버렸다. 이와 함께 컴퓨터가 발달하고 인터넷의 증가로 인하여 많은 사람들이 나누는 정보의 복잡화로 인하여 보안의 필요성이 크게 나타나고 있다. 이에 따라 여러 가지 암호 기법이 나타나고 있으며 실제로 사용하고 있다.

암호는 처음 shannon에 의해서 기초이론이 확립 되었다.[1] 이러한 암호체계는 평문을 암호화 하는 방법에 따라 비밀 키 암호체계 (secret-key cryptosystem)와 공개 키 암호체계(public-key cryptosystem)로 나누어 질 수 있다.[2] shannon에 의해서 기초이론이 확립된 암호는 비밀 키 암호이다.[1]

암호 기법은 운영방식에 따라 비밀 키 암호(secret-key cipher), 공개 키 암호(public-key cipher), 암호 알고리즘에 따라 블록암호, 스트림암호 등으로 나누어 볼 수 있는데 본 논문에서는 스트림 암호 기법을 다루고자 한다.

스트림 암호 기법을 사용하는데 있어서 필요한 수치를 생성하는 수치 접근 방식에 있어서는 수치해석 방법에서 잘 알려져 있는 Newton-Raphson Method를 이용하였으며, 거기에서 생성되는 수치 반복법을 이용한 키 수열 생성 알고리즘 방식을 사용하였다.

암호를 다루는 과정에서는 여러 가지 함수를 사용하고 있다. 본 논문에서는 간단한 수식을 이용하여 암호 알고리즘을 적용시켜 보고자 한다. 여기에서 말하는 간단한 수식의 함수라 함은 복잡한 수치의 해석을 배제한 대수적으로 단순한 방정식을 말한다.

로버트 메이(Robert May)가 1975년에 생물의 개체수 변동을 수학적으로 처리함으로써 카오스 공학을 가전제품이나 전기기기 등에 이용하기 시작하였으며,[3]

그 예로써 카오스적인 의미를 갖고 있으며 시간의 변화에 따라 동물의 개체 수에 변화가 일어나는 식을 예로 들어 볼 수 있다.

다음개체수
=증가율*(1-현재의개체수)*현재의개체수

이렇게 개체수를 모델화 할 때에는 계의 상태를 0과 1사이로 나타내는데 1은 개체수의 최대수, 0은 전

멸을 나타낸다. 우리는 이것을 로지스틱 방정식으로 나타낼 수 있다.[3]

$$X_{n+1} = aX_n(1-X_n) \qquad \text{단, } 1 \le a \le 4,\ 0 \le X_n \le 1$$

2. 본 론

본 논문에서는 수학적 함수를 이용하는 방식중의 하나로써 f(x)=0의 근을 찾는 수치해석의 방법 중 가장 강력하고 잘 알려진 방법 중의 하나인 Newton-Raphson Method를 이용한 암호 키 생성 알고리즘과 복호 알고리즘을 제안 하려고 한다.

Newton-Raphson Method는 함수의 해를 찾는 수치해석 방법들 중에서 함수의 반복으로 수치 접근을 하는 또 다른 형태의 다른 방식보다 간단한 기법을 가지고 있으며 가장 빠르게 수렴하는 방식중의 하나이다.

Newton-Raphson Method는 주어진 그래프에서 $f(x)$의 그래프가 x축과 교차되는 지점이 최초 제시하는 한 점 p_0와 Newton-Raphson Method에 의한 또 다른 한 점 p_1 사이에 존재하면서, 그래프의 한 지점과 x축이 교차되는 지점을 $f(x)=0$이라고 할 때 그 지점을 찾아서 수렴 접근하여 오차의 범위가 아주 작을 때 그 지점을 찾아내는 방법이다.

ASCII 코드를 이용하여 평문 데이터 입력 값 S 로 사용한다.

수치 접근으로 얻어지는 지점 p_0, p_1, p_2, p_3, ... p_n 각각의 정수부분을 2로 나누어서 나머지가 0이면 0을 표기하고 2로 나누어서 나머지가 1이면 1을 표기하여 2진수 8비트 키 값 B 를 만든다.

그래서 얻어지는 암호화 된 수치값을 T 라고 한다.

$$T = S \veebar B$$

역으로 진행하여 얻어지는 복호된 수치 값을 S'라고 한다.

$$S' = T \veebar B$$

3. 결 론

암호는 현대의 사회에 있어서 군사, 정치, 경제, 산업 등의 여러 방면에서 중요한 문서의 보안을 지켜왔다.

본 논문에서는 수치해석 방법의 하나인 Newton-Raphson Method 알고리즘을 이용하여 스트림 암호 기법 8비트 키 수열 생성 알고리즘을 이용함으로써 평문을 암호화 하여 사용할 수 있음을 보였다.

Newton-Raphson Method를 이용함으로써 평문을 암호화 하는데 걸리는 시간을 빠르게 하였다. 암호화 하는데 사용하는 암호화 함수를 한 가지만 사용하게 되면 암호 공격자에게 누출이 될 가능성도 높고, 보안 효과를 보기가 어렵게 되는데, 본 논문에서는 암호화 함수를 한 가지만 사용함으로써 염려되는 암호 공격자들로부터 보호하기 위하여 암호화 함수를 다양하게 사용 할 수 있게 만듦으로써 암호 공격자들로부터 안전하게 보안을 유지할 수 있는 효과를 기대할 수 있을 것이다.

수치해석의 방법에는 Newton-Raphson Method 뿐만 아니라 여러 가지 방법이 사용되고 있다. 그러므로 Newton-Raphson Method 뿐만 아니라 다른 수치해석 방법을 사용함으로써 또 다른 암호 알고리즘을 만들 수 있을 것이다.

참고문헌

[1] C.E. Shannon, A mathematical theory of communication, Bell Sys. Tech. j., 27:379-423, 623-656, 1948.

[2] 이민섭, 현대암호학, 교우사, 서울, 2002.

[3] 김대영, 김태식, "카오스 암호를 이용한 개선된 암호화 웹 메일 시스템의 설계와 구현", 정보처리학회 논문지 D, 제13-D권, 제3호, 2006.6.