카오스 암호를 이용한 개선된 암호화 웹 메일 시스템의 설계와 구현

김 대 영† · 김 태 식††

요 약

스트림 암호 시스템을 중심으로 한 카오스 암호 시스템은 원문의 길이가 클수록 암복호화 및 송수신 속도가 떨어지는 단점을 보여왔다. 본 연구에서는 원문의 길이가 길수록 기존의 웹 메일 시스템에 비해 더욱 우수한 성능을 보이고 있는 암호화 웹 메일 시스템을 설계 구현하였다.

암호화 웹 메일 시스템구현에서 키 수열 생성, 원문의 암복호화, 내외부 메일 뷰어 등을 개발하였고, 성능 평가 결과 암복호화 및 송수신 속도에서 우수한 것으로 평가되어 스트림 암호 시스템이 갖는 단점을 보완하였다고 할 수 있다.

앞으로 지속적인 응용 연구를 통해 암호화 기술을 기반으로 한 서버 시스템 보안 및 파일 보안, 인터넷 정보의 보안, 전자 상거래 시스템의 정보 보호 등 여러 분야에서 블록 암호 시스템을 대체할 수 있는 새로운 범용 암호 시스템으로 활용 할 수 있을 것으로 기대된다.

키워드 : 카오스 암호화, 웹메일 시스템

Design and Implementation of a Improved Cipher Web Mail System using a Chaos Cipher

Dae Young Kim† · Tae Sik Kim††

ABSTRACT

A chaos cipher system that focuses on the stream cipher system has a demerit that the longer the text is, the slower the speed of the encryption and description and the transmission and reception. On this study, we designed the cipher web mail system showing much better capabilities than the existing web mail system as the text is longer.

In the embodiment of the cipher web mail system, we developed the key stream, the encryption and description of the text and the inside and outside mail viewer and so on. After the efficiency test, it was valued high in the respect of the speed of the encryption and description and the transmission and reception. And it made up for the defect of the stream cipher system.

We expect that we can use it through the persistent applied study in the server system security, the file security, the security of the internet information, the protection of the e-commerce system information and other fields based on the cipher technique as the wide use cipher system that can replace the block cipher system.

Key Words : Chaos Cipher, Weg Mail System

1. 서 론

1.1 연구의 배경과 필요성

현대사회는 개방형 네트워크의 급속한 발전과 정보인프라의 구축을 통해 정보화 사회로의 입지를 넓히고 있다. 이러한 컴퓨터 네트워크 환경에서 수없이 많은 정보의 교류가 진행되고 있으며, 정보의 안전성과 신뢰성을 보장하기 위한 수단으로서 암호가 적용되고 있다.

1949년 발표된 샤논(Shannon)의 논문[1]이후 현대 암호는 이 같은 요구에 적절히 부응하기 위해 많은 암호 알고리즘이 연구, 개발, 사용되어 왔으며, 암호 알고리즘의 종류는 관점과 방법에 따라 비밀키 암호 시스템(single-key cryptosystem)과 공개키 암호 시스템(public-key cryptosystem)으로 크게 나눌 수 있다.

비밀키 암호 시스템은 1977년 미국 표준국(NBS : National Bureau of Satandard, 현 NIST의 전신)에 의해 미 연방 정보 처리 표준 46(FIPS PUB46)으로 채택된 DES(Data Encryption Standard)[2]를 비롯한 많은 종류가 있다.

공개키 암호 시스템은 비밀키 암호 시스템의 문제점들을 해결하고자 하는 시도에서 MIT의 R. Rivest, A. Shamir, 그

† 정 회 원 : 안동정보대학 인터넷전자상거래과 조교수
†† 정 회 원 : 계명대학교 정보통신대학 미디어테크놀로지학과 부교수
논문접수 : 2006년 2월 14일, 심사완료 : 2006년 5월 17일

리고 L. Adleman에 의해 1977년에 개발된 RSA[3]를 비롯한 많은 종류가 개발되어 있다.

그러나, 최근 암호 해독을 위한 여러 가지 알고리즘의 개발과 컴퓨터 기술의 발전은 암호 시스템의 안정성을 보장하고 있던 암호 키의 계산을 짧은 시간에 가능하게 하였으며, 암호문의 해독을 더욱 효과적으로 할 수 있도록 하였다[4].

스트림 암호 시스템은 블록 암호 시스템에 비해 에러의 확산이 없고, 비도 수준과 관련된 여러 가지 중요한 수치에 대한 정량화가 가능하며, 하드웨어나 소프트웨어로 구현이 용이하고, 통신 지연이 없으며, 고속 통신이 가능한 것을 비롯하여 여러 가지 장점을 지니고 있어 안전한 암호 시스템을 설계하기에 적당하다[5-6].

일반적으로 스트림 암호 시스템의 안전성에 대한 측도로 이용되는 비도(security level)는 키 수열의 길이와 임의성 및 주기성, 상관면역도 등에 크게 좌우되는데, 스트림 암호 시스템에서는 키 수열의 발생을 위해 지금까지 선형 귀환 쉬프트 레지스터(Linear Feedback Shift Register; LFSR)가 일반적으로 이용되어 왔다.

이러한 가운데 초기조건에 민감성을 가지는 카오스 신호를 이용하여 정보를 암호화 하는 연구가 증가하고 있는데, 암호화 및 복호화 단계가 카오스적이라는 본질적 이유 때문에 수학적 방식으로는 절대로 풀리지 않는다고 알려져 있고, 비선형 함수를 기반으로 카오스 신호를 발생시켜 암호화에 이용하므로 주로 스트림 암호 시스템에 적용되고 있다.

스트림 암호 시스템은 안전성이 높지만 원문의 길이에 해당하는 키 수열을 사용하기 때문에 원문의 길이가 큰 경우 속도가 늦는 등의 문제점이 있어 암호 시스템으로 활용하기에 부적합하다. 특히 웹 메일 시스템의 경우 대용량의 원문이 자주 사용되므로 카오스 암호 기술을 이용할 경우 키 수열 생성, 암호화, 송수신등에서 한계를 보이고 있어 이에 대한 연구가 필요하다.

따라서, 본 연구에서는 카오스 특성을 갖는 안전한 키 수열 알고리즘을 이용하여 대용량 원문의 암호화 수행시 스트림 암호 시스템과 같이 안전성에서 뛰어나고, 암호화 및 복호화 그리고 송수신 과정에서 빠른 속도를 가질 수 있는 시스템을 개발하여 스트림 암호 시스템과 블록 암호 알고리즘의 장점을 모두 갖추고 있는 이상적인 형태의 암호화 웹 메일 시스템을 구현하고자 한다.

2. 카오스 이론과 암호화

2.1 카오스 이론의 개요

카오스 이론은 결정론적 비선형 동역학 시스템(Deterministic Nonlinear Dynamic System)을 다루는 학문으로 불안정한 비주기적 운동을 정성적으로 연구하는 학문으로[7], 카오스의 일반적인 정의는 첫째, 어떤 동력학계의 복잡하고 비주기적이며 유인적인 궤도이고 둘째, 주기성이 없는 일종의 질서이며 셋째, 새롭게 인식된 보편적인 자연현상으로 넷째, 결정론적인 비선형 동력학계에 나타나는 불규칙적이고 예측 불가능한 형태이다.

자연현상에서 흔히 관찰되는 여러 가지 현상들이 오랜 노력에도 불구하고 규명하기 곤란했었으나, 로렌츠(Lolenz)의 '초기조건의 민감한 의존성'에 관한 연구 이후 자연의 복잡성 속에 숨어 있는 규칙성 및 질서를 찾아내고자 하는 노력이 매우 활발해 지고 있다.

로버트 메이(Robert May)는 1975년에 생물의 개체수 변동을 수학적으로 처리함으로서 카오스 공학을 가전제품이나 전기기기 등에 이용하기 시작하였다. 네이춰지에 발표된 메이의 논문[8]에서 그는 매우 복잡한 동적 시스템을 간단한 수학적 모델로 제안하였고 이 간단하고 단순한 방정식에서 나온 해답이 카오스적인 의미를 갖는다고 하였다.

로버트 메이는 시간의 변화에 따른 동물의 개체수 변화를 구하는 간단한 식을 통하여 발표하였다.

다음개체수 = 증가율×(1-현재의 개체수)×현재의개체수

이러한 개체수를 모델화할 때에는 계의 상태를 0과 1사이로 나타내는데 1은 개체수의 최대수를 나타내고 0은 전멸을 나타낸다. 이것을 다음 (식 1)의 로지스틱 방정식으로 나타낼 수 있다.

$$X_{n+1} = aX_n(1-X_n) \qquad \text{(식 1)}$$

단, $1<=a<=4$, $0<=X_n<=1$

a는 개체수의 증가량이며, X_n은 현재의 개체수, X_{n+1} 은 다음의 개체수이다. 위의 로지스틱 방정식에서 X_n 에서 X_{n+1}로의 변화를 논리사상 (logistic map)이라 한다. a의 값이 크다면 개체수가 적을 때는 빠른 속도로 증가하고 작다면 빠른 속도로 감소함을 나타낸다. 이러한 값의 변화는 매개변수 a의 값에 따라 다른 양상을 나타낸다. 매개변수 a에 따르는 몇 가지 특징을 발견할 수 있다.

(1) 0 < a <= 1	Xn은 0으로 수렴
(2) 1 < a <= 2	Xn은 1 -(1 / a)로 수렴
(3) 2 < a <= 3.5699	Xn는 주기배가 상태
(4) 3.5699 < a	Xn 는 혼돈 상태

즉, 로지스틱 맵을 통해 증가율 $a=3.66 \sim 4$의 값을 가진 경우에는 개체수를 예측하기에 매우 혼란한 상태로 표시되고 있는 것을 알 수 있고, 카오스 암호화는 이처럼 단순한 차원 방정식에 의한 카오스 신호를 이용하여 암호화 및 복호화를 수행하여, 이를 암호화 시스템에 응용하고 있다고 하겠다.

2.2 카오스 암호화

카오스 이론을 공학에 이용할 수 있도록 한 로버트 메이의 연구이후 카오스 이론을 연구하고 있는 연구자들은 대부분 현재 카오스의 연구가 기초적 이론을 축적하는 과정에 있으며 앞으로는 카오스에 관한 연구가 기초적 이론 연구에

서 응용 연구 분야로 비중이 높아질 것으로 보고 있다. 더욱이 최근 컴퓨터의 발달로 카오스에 대한 해석과 그 현상을 기하학적으로 표현할 수 있게 됨에 따라 카오스 이론의 연구가 활발해지고 실생활에 응용하고자 하는 시도도 더욱 활발해지고 있다[9-10].

카오스의 연구 중에는 시계열 데이터의 분석, 기후의 변화, 전염병 발생, 심장 상태 분석 등에 대한 연구와[12-14] 결정론적 비선형 예측 분야, 생체 카오스,, 카오스 패턴인식, NP문제, 화상처리 등 다양한 분야에서 응용연구가 활발하다[15-18].

아울러, 카오스 신호의 초기조건에 대한 민감성을 암호화에 응용하는 다양한 연구를 통해 새로운 암호 시스템을 위한 제안이 증가하고 있다. 카오스 암호화 연구는 카오스 신호를 이용한 키 수열 생성 방법[19-21], 키 수열의 안전성 분석[22-24], 카오스 암호화 모델 제안[25-26] 등 다양한 분야에서 진행되고 있다.

3. 개선된 암호화 웹 메일 시스템

카오스 이론에 기반한 응용 시스템이나 모델들은 대부분 스트림 암호 시스템을 기반으로 연구되었다. 스트림 암호 시스템은 키 수열의 길이가 원문의 길이와 동일한 크기로 만들어져 암호화 또는 복호화하는 방법이므로 원문의 길이가 클수록 암복호화 속도가 떨어지는 단점이 있는 것으로 알려져 있다.

앞서 살펴본 카오스 암호화 관련 연구에서 나타난 바와 같이 카오스 신호를 이용한 다양한 연구 성과에도 불구하고, 새로운 시스템 개발이나 적용이 지연되고 있는 것은 이같은 단점을 극복하기 위한 연구가 뒤따르지 않은데 원인이 있다고 할 수 있다. 따라서, 본 연구를 통해 기존에 제안된 키 수열 알고리즘을 적용한 응용 시스템을 설계하고 구현함으로서 카오스 신호를 이용한 암호화 시스템 개발에 대한 가능성을 확인하고자 한다.

3.1 카오스 키 수열 생성 알고리즘

카오스 이론에 기초한 카오스 암호화 알고리즘은 송신측이 원문에 카오스적인 성질을 갖는 키 수열을 XOR하여 암호화 하고, 수신측이 송신측과 동일한 카오스 시스템을 사용하여 원문을 복호화 함으로서 원문을 복원해낼 수 있다는 카오스 암호화 원리에 기초한다.

카오스 암호화 시스템은 카오스 이론을 암호화에 적용 할 수 있는 안전성이 있는 키 생성 알고리즘을 이용하여 키 수열을 생성하는 것이 매우 중요하다. 본 연구에서 이용하게 되는 카오스 키 수열 생성 알고리즘은 (그림 1)의 균형성을 보장하는 적응적 키 수열 생성 알고리즘이다.

적응적 키 수열 생성 알고리즘을 동일한 조건에서 30회에 걸친 실험하여 Rueppel, Bianco, Gao Zhenyu, Kohda 등이 제안한 알고리즘과과 제안된 알고리즘을 대상으로 실시한 균형성 실험결과와 랜덤특성 실험결과는 <표 1>과 같이

```
function St()
        begin
          loop
              Xn+1= αXn(1-Xn)
              if Xn>threshold then
                    { keystream:=1;  counter1++; }
               else { keystream:=0;  counter0++; }
               if 0=(n mod p) then Reset(counter0, counter1);
              output:=keystream XOR data;
        until end of message;
      end

function Reset(counter0, counter1)
        begin
          balance:=Counter1:Counter0;
          if balance>0.5 then threshold:=threshold-0.05
            else threshold:=threshold+0.05;
        end
```

threshold : 임계값, Reset() : 임계값 조정 함수, balance : '1'과 '0'의 균형성

(그림 1) 적응적 키 수열 생성 알고리즘

〈표 1〉 키 수열의 균형성 및 랜덤특성 비교

구분	기존 카오스 키 수열 생성 알고리즘			사용된 알고리즘
	Bianco	Gao Zhenyu	Kohda	
균형성	0.3490 : 0.6510	0.4946 : 05034	0.5464 : 0.4536	0.5000 : 0.5000
랜덤특성	145,782.6512	29,514.0893	856.7162	0.8196

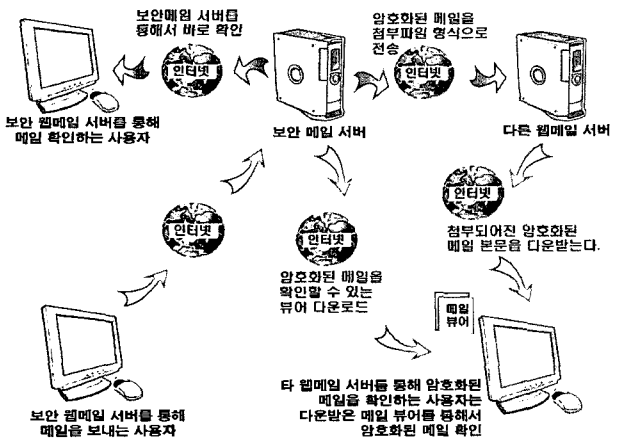
Bianco, Gao Zhenyu, Kohda 등이 제안한 키 수열 생성 알고리즘에 비해 우수하다고 할 수 있다[27].

3.2 웹 메일 시스템 설계

본 연구에서는 카오스 키 수열 생성 알고리즘과 이를 이용한 암복화의 유용성을 확인하고, 새로운 응용 시스템 개발의 방향을 제시하기 위하여 대용량 원문을 암호화하여 송수신하고 복호화할때의 속도를 향상시켜 대용량 원문에 대한 암호화에 적합한 암호 시스템을 개발하여 암호화 웹 메일 시스템을 설계하고 구현하여 보고자 한다.

본 연구에서 구현하게 될 암호화 웹 메일 시스템은 보안 메일 서버에서 암호화된 메일을 내부 메일 사용자나 외부 메일 사용자에게 전송하게 되고, 내부 메일 사용자는 자체 복호화 모듈에 의해 자동으로 복호화된 메일을 열람할 수 있으며, 외부 메일 사용자는 첨부된 메일 뷰어를 이용하여 전송된 메일을 복호화 하여 열람할 수 있게 하는 암호화 시스템으로 주요 기능은 다음과 같다.

- 내부 보안메일
  - 내부사용자(같은 메일 서버, 즉 웹메일로 확인하는 사용자)에게 암호화 메일을 보낼 경우에 사용하는 것으로 웹 메일 자체에 복호화 모듈이 들어있어 비밀 키만 입력하여 암호화 메일을 복호화 할 수 있는 기능



(그림 2) 암호화 웹 메일 시스템 구성

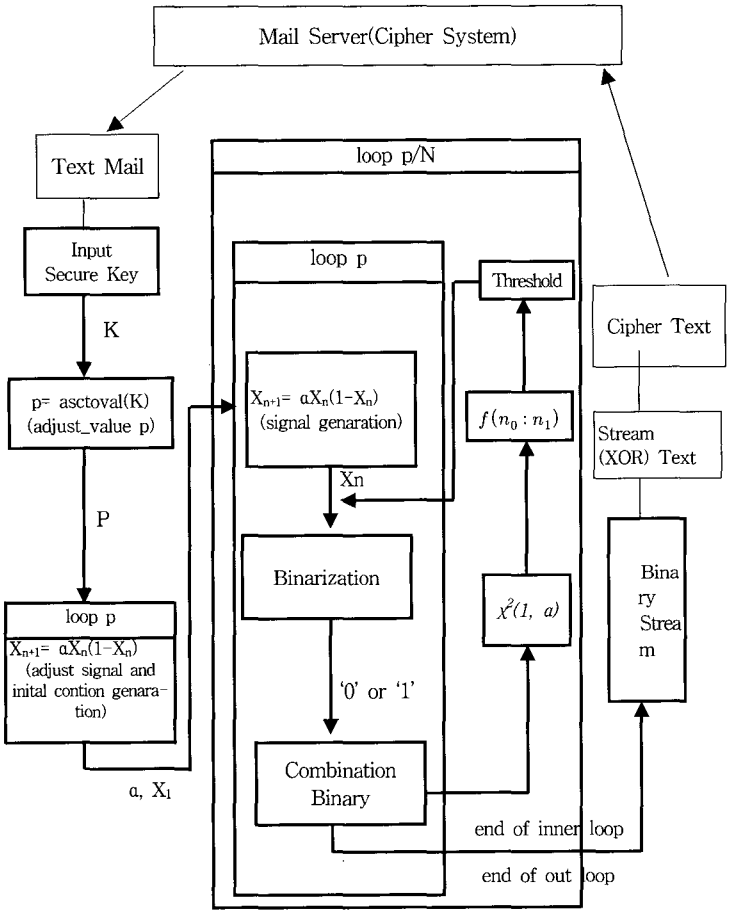
• 외부 보안메일
  - 외부 사용자(즉 다른 메일 서버에서 메일을 확인하는 사용자)에게 암호화 메일을 보낼 경우에 사용하는 것으로 외부 사용자는 따로 만들어진 '암호화 메일 뷰어'를 이용하여 암호화 메일을 복호화 할 수 있는 기능
• 보안메일 뷰어
  - 카오스 암호화 알고리즘을 이용하여 암호화된 메일을 복호시켜 보여주는 기능을 사용자에게 보내줌으로서 외부 사용자가 암호화 메일을 확인할 수 있도록 하는 기능
  - ".ssm"이라는 확장자명으로 암호화되어 수신된 암호화 메일을 복호화 하여 보여줄 수 있도록 제공되며, ssm 파일을 더블클릭하면 보안메일 뷰어가 자동으로 실행되면서 암호화 메일을 복호화 하도록 제공되는 기능

본 연구에서 구현된 암호화 웹 메일의 전체 시스템 구성은(그림 2)과 같고, 이를 구현하기 위한 알고리즘은 (그림 3)과 같다.

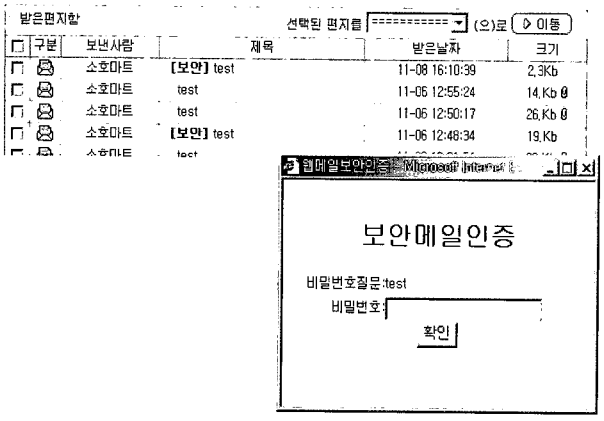
3.3 웹 메일 시스템 구현

시스템 구현을 위해서 사용된 개발 환경은 웹 메일 시스템 개발에서 LINUX 운영체제 기반에서, Apache Web Server, PHP Script Language, My-SQL 데이터베이스를 이용하였으며, 암복호 모듈의 개발 및 테스트를 위해 LINUX와 Windows 기반의 운영체제에서 JDK 1.3.1과 C++를 주로 이용하였다. 그리고, 메일 뷰어의 개발을 위해 Windows 계열의 Visual Basic과 C++를 이용하였다.

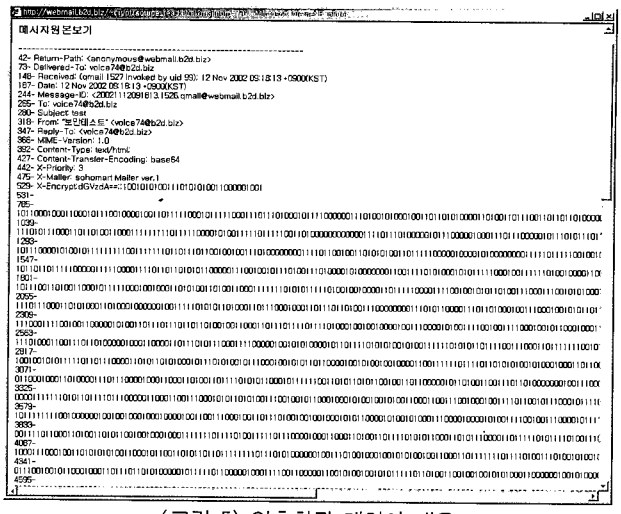
암호화 웹 메일 시스템은 웹 메일 시스템과 암호화된 암호화 메일을 함께 구현한 것으로 메일을 보내거나 받을 때



(그림 3) 카오스 웹 메일 시스템 암복호화 알고리즘 개념도



(그림 4) 비밀 키를 이용한 암호화 메일 인증 과정



(그림 5) 암호화된 메일의 내용

메일이 암호화되어 안전한 메일 관리가 가능하다.

내부 암호화 메일은 암복호화 과정이 메일 시스템 내부에서 진행되므로 빠르고 안전하며, 받은 메일을 확인하기 위해 별도의 Viewer가 필요하지 않아 편리하게 사용할 수 있다. 내부 암호화 메일을 이용할때는 (그림 4)과 같이 송신자와 수신자가 사전에 약속한 비밀키로 카오스 신호를 이용하여 메일을 암호화 한후에 전송할 수 있도록 하였다.

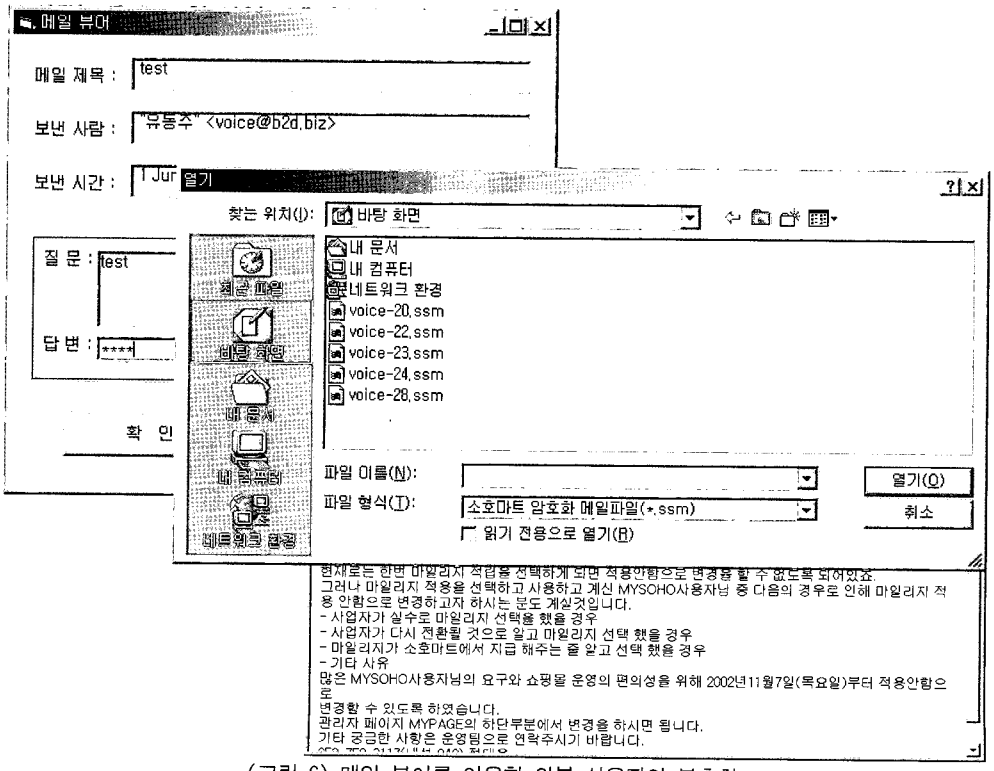
본 연구에서 제안한 카오스 암호화 알고리즘을 통해 메일의 내용을 (그림 5)과 같이 암호화하여 전송하게 된다.

내부 암호화 메일을 확인하기 위해서는 송신자와 수신자가 사전에 약속한 비밀키를 입력하여 카오스 신호를 이용하여 암호문을 복호화한후 보안 메일을 확인할 수 있도록 구현하였다.

또한, 보안메일 뷰어를 이용하여 외부 사용자는 ".ssm"이라는 확장자명을 가지고 수신되는 암호화된 메일을 복호화하여 볼 수 있도록 구현하였다.

3.4 메일 송수신 속도 평가

구현된 암호화 웹 메일 시스템은 앞서 제시된 바와 같이 카오스 이론을 이용한 스트림 암호 시스템을 기반으로 개발되었다. 스트림 암호 시스템은 키 수열의 길이가 원문의 길이와 동일한 크기로 만들어져 암호화 또는 복호화하는 방법



(그림 6) 메일 뷰어를 이용한 외부 사용자의 복호화

〈표 2〉 구현된 암호화 웹 메일 시스템의 암복호화 속도 비교

구 분	제안된 암호화 시스템				JX-Mail			
	내 부		외 부		내부		외부	
	암호	복호	암호	복호	암호	복호	암호	복호
실험 1	1초	1초	1초	1초	3초	2초	4초	1초
실험 2	1초	1초	1초	1초	4초	3초	3초	1초
실험 3	2초	2초	1초	2초	6초	9초	4초	2초
실험 4	2초	2초	2초	2초	7초	13초	4초	2초

이므로 원문의 길이가 클수록 암복호화 속도가 떨어지는 단점이 있는 것으로 알려져 있다. 그러나, 이번 연구에서는 스트림 암호 시스템의 단점을 보완하여 웹 메일 시스템에 적용한 결과 기존의 보안 웹 메일 시스템에 비해 비교적 우수한 것으로 평가된다.

다음 <표 2>는 구현된 암호화 웹 메일 시스템과 기존의 웹 메일 시스템의 암복호화 속도를 비교한 것으로 원문의 길이에 관계없이 개발된 시스템이 우수하거나 비슷한 속도를 보이고 있음을 알 수 있다.

비교된 실험의 경우 웹 메일의 다양성을 고려하여 4가지 실험을 각 10회씩 실시하여 평균값을 기록하였다. 각 실험결과는 시스템 환경, 네트워크 환경, 컴퓨터 성능에 따라 다소 차이가 있어 소수점 이하의 시간을 기록하지 않았으며, 실험결과 원문의 길이가 길수록 우수한 성능을 보이고 있다. 이는 지금까지 스트림 암호 시스템의 단점으로 지적되어 온 속도 문제를 효과적으로 해결한 것으로 평가된다.

(실험 1) 원문의 길이가 1페이지(500자) 이내의 경우
(실험 2) 원문의 길이가 10페이지(5,000자) 이내의 경우
(실험 3) 원문의 길이가 20페이지(10,000자) 이내의 경우
(실험 4) 원문의 길이가 50페이지(25,000자) 이내의 경우

3.5 성능 비교 평가

<표 3>는 구현된 시스템과 비교 대상 시스템중 2개의 메일 시스템을 대상으로 한 일반적 성능 평가를 비교한 것이다. 성능 평가 결과 제안된 알고리즘으로 구현된 시스템이 기존의 시스템과 비교할 때 다소 우수한 것으로 평가되었으나, 평가 항목이나 평가 방법이 수학적인 증명에 기반하지 않았으므로 객관적인 우수성을 인정하기에는 부족한 면이 있다. 앞으로 제안된 시스템에 대한 과학적이고 객관적인 평가를 통해 범용 암호화 시스템의 응용 가능성을 찾을 수 있을 것으로 기대된다.

4. 결 론

보안 및 암호 기술이 더욱 중요한 위치를 차지하게 되면서 원천기술에 대한 필요성이 지속적으로 제기되었음에도 불구하고, 새로운 암호 기법으로 각광 받아오던 카오스 이론을 기반으로 한 암호 시스템이 원문의 길이가 클수록 암복호화 속도가 떨어지는 단점으로 인해 기술개발이 지연되어 오고 있다. 이번 연구에서는 스트림 암호 시스템의 단점을 보완한 암호화 웹 메일 시스템은기존의 암호화 웹 메일 시스템에 비해 비교적 우수한 것으로 평가된다.

또한, 구현된 암호화 웹 메일 시스템과 기존의 웹 메일 시스템에서 웹 메일의 다양성을 고려하여 4가지 실험을 각 10회씩 실시하여 평균값을 비교하였다. 그결과 원문의 길이에 관계없이 제안된 시스템이 우수하거나 비슷한 속도를 보이고 있음을 알 수 있으며, 원문의 길이가 길수록 더욱 우수한 성능을 보이고 있다.

특히, 본 연구에서는 기존의 카오스 키 수열 생성 알고리

〈표 3〉 구현된 시스템의 일반적 성능 평가

비교내용	제안된 시스템	JX-Mail	INISAFE Mail
자체 보안 모듈 보유	카오스 알고리즘을 이용한 보안 모듈 사용	없음.	없음.
외부 메일서버에서 메일 확인	자체 메일 뷰어를이용하여 확인(비밀키 이용)	자체 메일 뷰어 (비밀키)	외부메일 인 경우 S/MIME을 이용하기 때문에 공인 인증서 필요
안정성	좋음	좋음	좋음
속도	매우 우수	다소 우수	보통

즘 및 암호화 기법을 응용하여 실제 사용가능한 시스템에 적용하고 구현함으로서 카오스 키 수열 생성 및 암호화 연구를 한 단계 발전시켜 새로운 암호 시스템 개발의 가능성을 확인하였음이 입증되었다.

또한, 성능 평가 결과 제안된 알고리즘으로 구현된 시스템이 기존의 시스템과 비교할 때 다소 우수한 것으로 평가되었으나, 앞으로 과학적이고 객관적인 평가를 위한 연구를 통해 대용량 원문을 암호화에 적극적으로 대응할 수 있을 것으로 기대된다.

본 연구에서 개발된 암호화 웹 메일 시스템은 원문의 길이가 길수록 우수한 성능을 보이고 있어 스트림 암호 시스템이 갖는 단점을 보완했다고 할 수 있으며, 카오스 암호 시스템이 범용 암호화 시스템을 위한 적절히 활용 할 수 있는 암호화 시스템임을 확인 하였다.

앞으로 지속적인 응용 연구를 통해 카오스 암호화 기술을 기반으로 한 서버 시스템 보안 및 파일 보안, 인터넷 정보의 보안, 전자 상거래 시스템의 정보 보호 등 여러 분야의 응용 연구가 계속된다면, 향후 국내 암호 기술 수준을 제고할 수 있는 계기가 될 것으로 기대된다.

참 고 문 헌

[1] C. E. Shannon, "Communication Theory of Secrecy Systems," *Bell Syst. Tech. J.*, vol. 28, pp.656-715, Oct. 1949.

[2] National Bureau of Standards : Data Encryption Standard, *Federal Information Processing Standard-46* , pp.1-18, 1977.

[3] R. L. Rivest, A. Shamir, L. Adleman, "A method for obtaining digital signatures and Public-Key Cryptosystems", Communications of Association of Computer Manufactures, vol.21, No.2, pp.120-126, 2. 1978.

[4] IISI, 'Encryption for meultimedia age GCC Overview', http:// www.iisi.co.jp/research/GCC-over.html

[5] 김철, 암호학의 이해, (주)영풍문고, 서울, 1996.

[6] 포스데이타, "암호를 이용한 정보보호 기법", http://posdata.co.kr/kpc/n2-1. htm, 2001. 10.

[7] 이병채, "카오스 이론을 이용한 생체 비선형 동역학 시스템의 특성 해석", 박사 학위논문, 연세대학교, pp.5-6,34, 1995

[8] R.M. May,"Simple mathematical models with very complicated dynamics", Nature, 261, pp457-461, 1976.

[9] HieTae Moon, Seunghwan Kim, Robert P. Behringer & Yoshiki Kuramoto, "Proceedings of the international Workshop on Nonlinear Dynamics and Chaos", World Scientific, 1995.

[10] 정호선, 여진경, "뇌와 카오스", Ohm사, 1994

[11] 김재훈 외 3인, "시간지연과 입력포화를 갖는 T-S 퍼지 카오스 시스템의 동기화", 대한전자공학회논문지SC, 1229-6392, 제42권1호 , pp.13-21, 2005.

[12] 김혜경, 성보현, 김태식, "Strange Attractor를 이용한 화자인식의 음성 특징추출에 관한 연구", 추계 학술발표논문집, 한국 정보처리 응용학회 , pp.340-343, 1994

[13] 정성용, 김태식, "카오스 어트렉트를 이용한 음성 데이터의 특징 분석 기법에 관한 연구", 춘계학술대회논문집, 한국정보처리학회, pp.625-628 ,1999.4.10.

[14] Herve Bourlard, Nelson Morgan, Chuck Wooters, "Connectionist approaches to the use of markov models for Speech Recognition", Neural Information Processing System 3, pp.213-219, 1995.

[15] 合原一幸, "응용 카오스", サイエソス社, 1994.

[16] 合原一幸, "카오스 응용", サイエソス社, 1995.

[17] 合原一幸, "카오스", サイエソス社, 1994.

[18] 김수민, 서영호, 김동욱, "카오스 시스템을 이용한 JPEG2000-기반 영상의 적응적 정보 은닉 기술", 대한전자공학회논문지SP, 1229-6384, 제41권4호, pp.9-21, 2004.

[19] Bianco M. E. et al., *Encryption System based on Chaos Theory*, United States Patent, no.5048086, Sep. 1991.

[20] Gao Zhenyu, *Method and apparatus for encrypting and decrypting information using a digital chaos signal*, United States Patent, No.5696828, 9. Dec. 1997.

[21] Kohda Tohru, Akio Tsuneda, *Encryption/Decryption apparatus and method incorporating random variable and keystream genetation*, United States Patent, No.6014445, 11. Jan. 2000.

[22] Kohda, Tohru, "Chaotic Bit sequences for stream cipher cryptography and their correlation functions," *Chaotic Circuits for Comm.*, Vol.2612, pp.86-97, USA, 23. Oct. 1995.

[23] Takakubo Hajime, Katsufusa Shono, "Digital Cyphering System using Chaos Time Series," *SPIE*, Vol.2612, pp.64-75, 1995.

[24] Zhou Hong, L. XieTing, "Generating Chaotic Secure Sequences with Desired Statistical Properties and High Security," *Int'l Journal of Bifurcation and Chaos*, Vol.7, No.1, pp.205-213, 1997.

[25] 정호선, "혼돈이론을 이용한 문서 암호화 시스템", 대한민국 특허, 특1998-0041215, 1998. 8. 17.

[26] 이봉환 외 4명, "카오스 암호화 아로글즘을 이용한 웹 보안 시스템 설계 및 구현", 정보처리학회 논문지, 제8-C권, 제5호., 2001.10.

[27] 정성용, 스트림 암호 시스템에서 카오스 이론을 이용한 개선된 키 수열 생성 알고리즘과 암호화, 박사학위 논문, 계명대학교 컴퓨터공학과, 2002. 6.

김 대 영

e-mail : dykim@ait.ac.kr

1991년 경일대학교 전자계산학과(학사)

1995년 대구대학교 정보처리(석사)

1999년 계명대학교 컴퓨터공학과 (박사수료)

1995년~현재 안동정보대학 인터넷전자상거래과 조교수

관심분야 : 인공지능, 카오스, 웹구축

김 태 식

e-mail : tskim@kmu.ac.kr

1984년 계명대학교 전자계산학과(학사)

1987년 Moorhead State Univ. 전자계산학과(공학석사)

1992년 Univ. of North Dakota 전자계산학전공(인공지능)(공학박사)

1993년~현재 계명대학교 정보통신대학 미디어테크놀로지학과 부교수

관심분야 : 인공지능, 카오스, 유전자알고리즘