제19회 한국정보처리학회 춘계학술발표대회 논문집 제10권 제1호 (2003.5)

카오스 암호 기법을 이용한 보안 웹 메일 시스템 설계 및 구현

정성용
대구보건대학 IT계열
e-mail:syjung@mail.thc.ac.kr

Secure Web Mail System Development Using The Chaos Encryption Method

Sung-Yong Jung
**Dept of Information Technology Daegu Health Collage

요 약

본 연구에서는 카오스 이론을 바탕으로 개발된 카오스 암호 기법을 이용하여 보안 웹 메일 시스템을 개발하였다. 본 연구를 통해 개발된 보안 웹 메일 시스템은 기존의 키 수열 생성 방법과 달리 비선형성이 보장된 카오스 키 수열 생성을 통해 암복호 알고리즘을 구현하고, 이를 웹 메일 시스템에 적용하였다. 개발된 시스템은 균형성과 랜덤특성이 기존의 카오스 키 수열을 사용하고 있으므로, 카오스적 특징에 의해 비교적 안전한 보안 기능을 제공하고 있다.

1. 서론

인터넷이 발달되고 널리 보급됨으로서 많은 사람들이 전자메일을 사용할 수 있게 되어 편리함이 증대되고 있으나, 한편으로는 개인 정보 침해로 인한 피해도 늘고 있다. 따라서, 전자메일을 사용함에 있어 기밀성을 유지하면서 안전하게 수신자에게 문서를 전달할 수 있는 요구가 증가하였으며, 이 같은 요구를 수용하기 위한 많은 연구와 개발이 있어 왔다[1)2)].

이번에 개발하된 보안 메일 시스템은 이런 사용자의 요구를 만족시키기 위해서 카오스 암호 기법을 이용하였으며, 특히 안전성과 응용성이 매우 뛰어난 시스템이다.

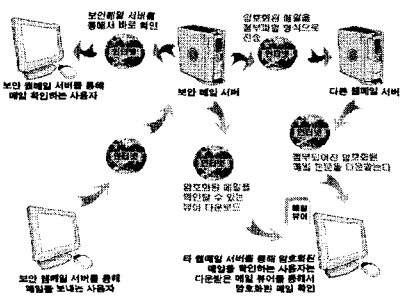
이 시스템은 카오스의 특성을 이용한 최신의 암호 기술로 기존의 암호 해독 방법으로 암호문의 해독이 불가능한 안정성이 보장될 것으로 예상되며[3)], 개발 과정에서 암호 기술에 대한 독립적인 경쟁력을 확보함으로서 전자상거래를 비롯한, Internet/Intranet, 위성 데이터 통신, 홈뱅킹, IC카드 등 다양한 보안 및 암호 시스템에 적용 가능할 것으로 기대된다.

2. 시스템 구성과 카오스 암호 기법

2.1 시스템 구성

개발 시스템은 보안 웹 메일 시스템은 카오스 이론을 암호화에 적용 할 수 있는 안전성이 증명된 키 생성 알고리즘을 개발하고, 이를 스트림 암호 시스템에 적용하여 메일 시스템에서 암호화 기능을 갖도록 하는 것을 목표로 하고 있다.

이를 위해 웹 메일 시스템의 개발, 암호화 모듈의 개발, 암호화 모듈을 장착한 보안 웹 메일 시스템의 개발 등 세 부분에 걸쳐 개발을 진행하였다. 개발된 보안 웹 메일의 전체 시스템 구성은 다음 (그림 2-1)과 같다.



(그림 2-1) 보안 웹 메일의 시스템 구성도

이와 같은 연구 개발을 통해 얻은 주요 기술 개발 내용을 정리하면 웹 메일 시스템에 필요한 기본적인 기능을 개발하였고, 메일의 암호화를 위해 카오스 암호 기술을 개발하였으며, 카오스 암호 기술을 적용한 보안 웹 메일 시스템 구현하였다.

특히, 카오스 암호 기술과 관련하여 암호화 키 생성 방법, 문서의 암복호화 기술, 암복호 문서의 전송 및 수신 기술을 확보하였으며, 카오스 암호 기술을 적용한 보안 웹 메일 시스템에서는 내부 보안메일 응용 기술, 외부 보안메일 응용 기술, 보안메일 뷰어 기술 등을 확보하였다.

2.2 카오스 암호 기법

1999년에는 '딥크랙'이란 암호해독 프로그램과 1만여대의 병렬 컴퓨터를 이용해 22시간15분만에 DES 암호 시스템이 해독한 사실이 있는 등 기존의 시스템의 안전성을 위해 점차 암호 키의 길이를 증가 시켜가고 있는 실정이다. 이는 기존의 암호화 기술이 여러 가지 공격법에 의해 해독이 가능한 것으로 알려져 있으므로 암호 시스템과 암호 시스템을 이용한 보안 시스템의 안전성을 높이는 방법으로 암호 시스템에 사용되는 키 수열에 대한 안전성을 높이는 것이 가장 효과적인 것을 의미한다고 할 수 있다[4)5)6)].

카오스 암호화 기법은 암호화 키로 사용되는 키 수열 생성을 위해 사용되는 카오스 함수를 사용하고 있다. 따라서 암호화 키는 초기조건에 매우 민감한 성질을 갖고 있어 매우 안전하고, 해독이 불가능한 것으로 알려져 있어 이를 이용하여 개발된 보안 시스템은 기존의 어떠한 공격으로부터도 안전할 것으로 판단된다[7)8)9)].

보안 웹 메일 시스템 개발에 사용된 카오스 암호 기법은 기존의 수열 생성 알고리즘에 비해 초기조건을 생성하는 방법을 개선하고, 수열을 생성함에 있어 수열의 균형성과 랜덤 특성을 보장하기 위해 수열 생성 도중 일정한 간격을 두고 균형성을 평가하여 임계값을 조정할 수 있도록 하였다[10)11)]. 구체적인 카오스 암호 기법은,

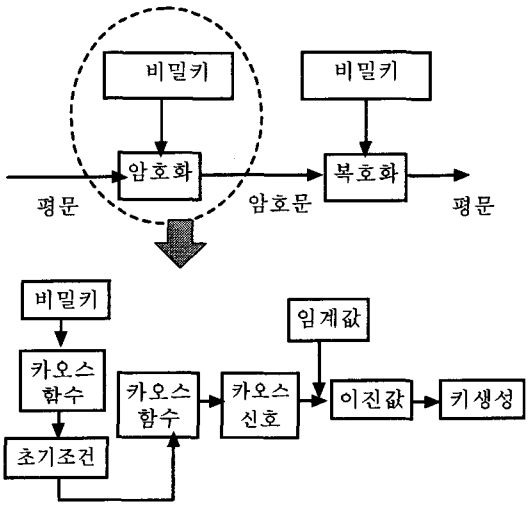
(가) 임의의 비밀키로부터 로지스틱 방정식을 이용하여 카오스 신호 발생에 필요한 초기조건 중 초기 개체수 X, 증가율 α를 생성하고,

(나) 다음으로 (가)에서 비밀키를 이용하여 생성된 초기조건 X와 α를 로지스틱 함수에 넣어 카오스 신호를 생성한 다음,

(다) 위 (나)에서 선택적으로 얻어진 카오스 신호를 임계값을 이용하여 '0' 또는 '1' 의 2진 신호로 바꾸어 이진값들로 이루어진 수열을 얻어서,

(라) 얻어진 이진값들로 이루어진 수열의 균형성 분석을 수행하고, 균형성을 만족할 때까지 임계값을 조정하여 상기 단계 (다)를 반복수행함으로서 암복호화에 필요한 키 수열을 얻게 되는 방법이다.

다음 (그림 2-2)는 카오스 암호화 기법의 범위와 키 수열 생성과정을 보여주고 있다.



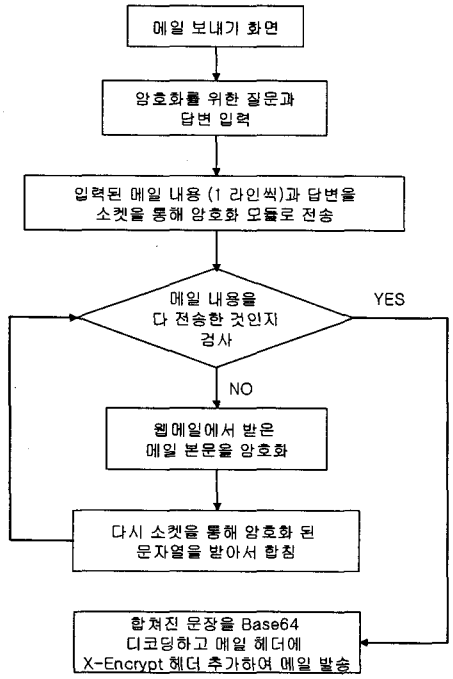
3. 시스템 설계 및 구현

3.1 개발 환경

시스템 개발을 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 JDK와 C++를 주로 이용하였다. 그리고, 메일 뷰어의 개발을 위해 Windows 계열의 Visual Basic과 C++를 이용하였다.

3.2 시스템 설계

보안 웹 메일 시스템에서 메일관리 및 데이터의 관리를 위해 필요한 데이터베이스를 구축하였으며, 보안 메일의 송신을 위한 흐름도는 (그림 3-1)과 같이 설계하였으며, 수신 방법은 송신 방법의 역방향으로 진행된다.



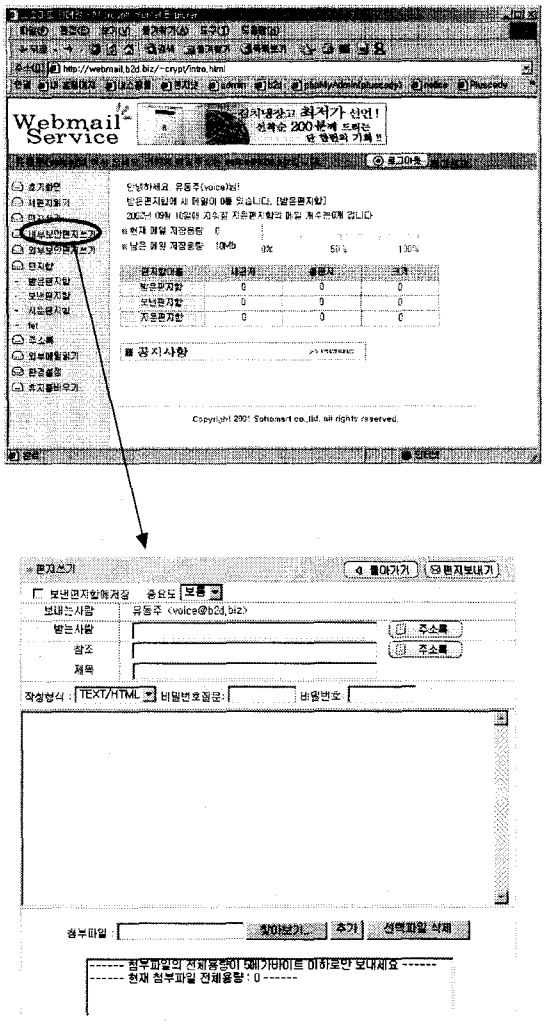
(그림 3-1) 보안메일의 송수신 흐름도

3.3 시스템 구현

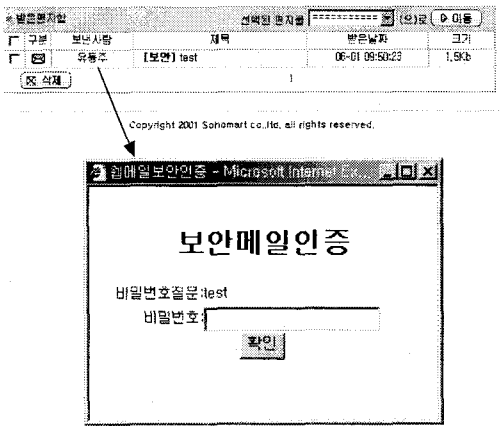
보안 웹 메일 시스템은 웹 메일 시스템과 암호화된 보안 메일을 함께 구현한 것으로 메일을 보내거나 받을 때 메일이 암호화되어 안전한 메일 관리가 가능하다. 여기서는 웹 메일의 일반적인 구현 결과는 생략하고 보안 메일을 보내거나 받기 위해 필요한 기능의 구현 및 결과에 대해 설명하였다.

먼저 다음 (그림 3-2)는 내부보안 메일 작성과정을 보여주고 있다. 내부 보안 메일은 암복호화 과정이 메일 시스템 내부에서 진행되므로 빠르고 안전하며, 받은 메일을 확인하기 위해 별도의 Viewer가 필요하지 않아 편리하게 사용할 수 있다. 내부 보안 메일을 이용할때는 송신자와 수신자가 사전에 약속한 비밀키를 이용하여 암호화 한 후에 전송할 수 있도록 하였다.

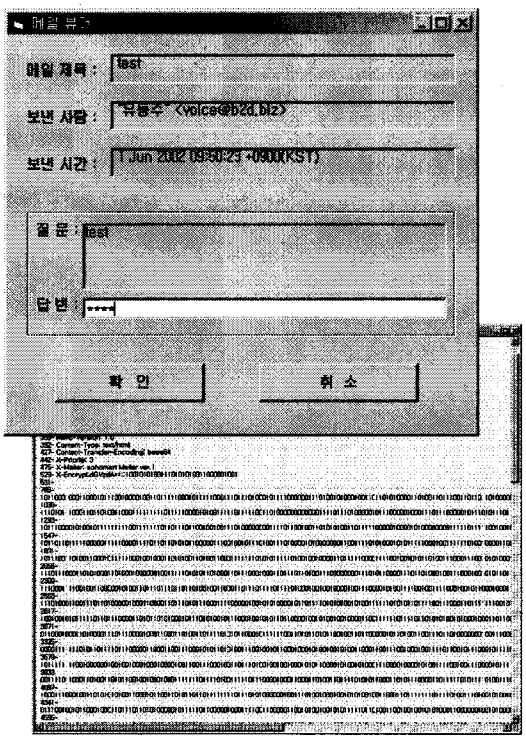
그리고, (그림 3-3)은 받은 내부 보안메일을 확인하는 과정을 구현한 것이다. 내부 보안 메일을 확인하기 위해서는 송신자와 수신자가 사전에 약속한 비밀키를 입력하여 암호문을 복호화하여 보안메일을 확인 할 수 있다.



(그림 3-2)는 내부보안 메일 작성



마지막으로 암호화된 보안 메일을 외부의 다른 메일 시스템에 전송했을 경우 암호화된 보안 메일을 받은 사람은 (그림 3-4)는 문서의 암호문과 복호문이 생성되는 과정을 보여주고 있는데, 시스템에서 자동 설치되도록 제공되는 메일 Viewer을 통해 송신자와 사전에 약속된 비밀키를 이용하여 암호화된 메일을 복호화하여 확인 할 수 있도록 구현하였다.



(그림 3-4) 메일 Viewer와 암호문

이번에 개발된 보안 웹 메일 시스템은 카오스 암호화 기법을 이용하여 기존의 암호 시스템과는 차이가 있다. 카오스 암호화 기법은 키 수열 생성과 암호화에 있어 중요한 척도의 하나인 속도에 빠르지 못한 단점 때문에 상용화하는데 많은 어려움이 있었다. 이번 연구에서도 현재 사용되는 국내외 대부분의 시스템 사용 할 수 있도록 하는데 있어 각 암복호화 속도와 시스템간의 통신 방법에 따른 속도저하 문제가 나타났다. 그러나 이 같은 문제점들을 암복호화 속도에 있어 새로운 알고리즘을 개발하여 해결하였고, 시스템간의 통신에서 소켓 연결 방법을 개선하고 서버와 클라이언트의 데이터 처리 방법을 개선함으로서 문제를 해결하였다.

향후 외부 보안 메일 사용시 첨부파일의 암호화 기술 개발과 메일 뷰어의 플러그인 기술을 개발하는 등 몇가지 보완을 통해 기존의 보안 웹 메일 시스템과 경쟁 할 수 있는 보안 웹 메일 시스템의 개발이 이루어 질 것으로 기대된다.

참고문헌

[1] 정재원, 류대걸, 강한, 보안과 암호화 모든 것, pp71-72, 인포북, 서울, 2001.
[2] 이만섭, 현대암호학, 교우사, 서울, 1999.
[3] 정성용, "스트림 암호시스템에서 카오스 이론을 이용한 개선된 키 수열 생성 알고리즘과 암호화", 박사학위논문, 계명대학교, 2002
[4] 국방일보, 국방홍보-암호해독기술, http://www. dapis.go.kr/mndweb/daily/1999/10/1006-37.htm, 1999. 10. 6.
[5] 송상헌,김충길, "암호 키 찾기", http://esperosun.chungnam.ac.kr/keychallenge /intro.htm, 1998.
[6] 지성택, 박춘식, "비밀키 암호", Telecommunca- ton Review, 제10권, 제5호, pp.877-886, 2000. 10.
[7] Bianco M. E. et al., *High speed encryption and method*, United States Patent, no.030687, 12. Mar. 1994.
[8] Jung Sungyong, Taesik Kim, "Advanced Stream Cipher System using Chaos Theory," *Proceeding of Int'l Conference on East Asian Language Processing and Internet Information Technology*, pp.242-245, China, Aug. 2000. 8.
[9] Kocarev L.et al.,"From Chaotic Map to Encry- ption Schemes," *IEEE*, pp.IV514-IV517, 1998.
[10] Jung Sungyong, Taesik Kim, "nonlinear characteristics on Keystream using Chaos Theory", *Proceeding of Int'l conference of Electronic Commerce*, pp.289-293, Korea, Aug. 2000. 8.
[11] 정성용, "적응적 임계값을 이용한 개선된 카오스 키 수열 생성 기법", 한국정보처리학회 추계학술발표논문집, 2002, 11. 15, pp.1075-1078

1) 정재원, 류대걸, 강한, 보안과 암호화 모든 것, pp71-72, 인포북, 서울, 2001.
2) 이만섭, 현대암호학, 교우사, 서울, 1999.
3) 정성용, "스트림 암호시스템에서 카오스 이론을 이용한 개선된 키 수열 생성 알고리즘과 암호화", 박사학위논문, 계명대학교, 2002
4) 국방일보, 국방홍보-암호해독기술, http://www. dapis.go.kr/mndweb/daily/1999/10/1006-37.htm, 1999. 10. 6.
5) 송상헌, 김충길, "암호 키 찾기", http:// esperosun.chungnam.ac.kr/keychallenge /intro.htm, 1998.
6) 지성택, 박춘식, "비밀키 암호", Telecommuncaton Review, 제10권, 제5호, pp.877-886, 2000. 10.
7) Bianco M. E. et al., High speed encryption and method, United States Patent, no.030687, 12. Mar. 1994.
8) Jung Sungyong, Taesik Kim, "Advanced Stream Cipher System using Chaos Theory," *Proceeding of Int'l Conference on East Asian Language Processing and Internet Information Technology*, pp.242-245, China, Aug. 2000. 8.
9) Kocarev L. et al., "From Chaotic Map to Encryption Schemes," *IEEE*, pp.IV514-IV517, 1998.
10) Jung Sungyong, Taesik Kim, "nonlinear characteristics on Keystream using Chaos Theory", *Proceeding of Int'l conference of Electronic Commerce*, pp.289-293, Korea, Aug. 2000. 8.
11) 정성용, "적응적 임계값을 이용한 개선된 카오스 키 수열 생성 기법", 한국정보처리학회 추계학술발표논문집, 2002, 11. 15, pp.1075-1078