제18회 한국정보처리학회 추계학술발표대회 논문집 제9권 제2호 (2002.11)

# 디지털 서명이 가능한 보안 전자메일 시스템의 구현

이종철, 강민섭
안양대학교 컴퓨터공학과
e-mail: mskang@aycc.anyang.ac.kr

# Implementation of Secure E-Mail System with Digital Signature

Jong-Chul Lee, Min-Sup Kang
Dept of Computer Engineering, Anyang University

요 약

본 논문에서는 메시지 암·복호화는 물론 디지털 서명 및 배달 증명이 가능 가능한 보안 전자 메일 시스템의 설계 및 구현에 관하여 기술한다. 제안된 시스템은 이메일의 내용을 암호화하여 이메일 수신자만이 그 내용을 볼 수 있도록 하는 기밀성을 제공해 주며, 디지털서명 기능을 제공하여 송신자라고 주장하는 사용자와 이메일을 실제로 보낸 송신자가 동일인인가를 확인해준다.

또한, 메시지 무결성, 송신자 부인 봉쇄 그리고, 배달증명 서비스를 제공한다. 제안된 시스템의 구현은 자바 암호 API 클래스를 기반으로 하였고, GUI를 위해 J빌더 6을 사용하였다.

## 1. 서론

현재의 범세계적인 네트워크 환경에서 광범위하게 사용되고 있는 전자메일 시스템은 데이터에 대한 보호 및 안전성에 있어서 많은 보안상의 취약점에 노출되어 있다[1-2].

메시지의 부당한 노출 및 변조는 일반 개인에게는 프라이버시의 침해가 될 수 있으며, 비밀성을 요구하는 특정한 사용자에게는 심각한 위협이 될 수 있다. 이러한 위협으로부터 사용자 정보를 안전하게 보호하기 위해서는 메시지 발신자의 신원에 대한 믿음을 제공할 수 있는 인증(Authentication) 기술과 안전하게 보호되어 전송되었음을 확인할 수 있는 기밀성(Confidentiality), 송·수신이 이루어진 후에 발생할 수 있는 부인행위에 대한 부인방지(Non-Repudiation) 등과 같은 정보보호 서비스를 제공할 수 있는 전자 메일 시스템이 요구된다[1].

이러한 정보보호 서비스를 제공하는 보안 전자 메일 시스템은 PGP(Pretty Good Privacy), PEM(Privacy Enhanced Mail) 등이 있다[3]. PGP는 RSA[4]와 IDEA 알고리듬를 사용하고 있다[3]. 최근에는 SSL(Secure Socket Layer), SET(Secure Electronic Transaction)등의 암호 알고리즘을 사용한 전자메일 시스템들이 등장하고 있다[5].

본 논문에서는 메시지 암·복호화는 물론 디지털 서명(Digital Signature) 및 배달 증명(Delivery Certification) 이 가능 가능한 보안 전자 메일 시스템의 설계 및 구현에 관하여 기술한다. 암·복호 알고리듬은 3중DES(Triple Data Encryption Standard)를 이용하며[6,7], 서명 인증은 RSA 알고리듬과 MD5 (Message Digest 5) 알고리듬을 이용한다[8].

## 2. 관련 연구

### 2.1 전자메일 시스템

RFC822를 기반으로 하는 전자우편 시스템에서는 전송 표준 프로토콜인 SMTP(Simple Mail Transfer Protocol)의 전송규격인 7bit ASCII로 자료교환이 이루어지고 있으므로 이진 연속의 멀티미디어 데이터는 전송할 수 없다[9]. 기존의 텍스트만의 전자우편에서 탈피하여 사용자가 원하는 형태로 전자우편 서비스를 제공하기 위해, 전자우편 시스템의 표준안으로 MIME (Multipurpose Internet Mail Extension)이 새로이 제안되었다.

인터넷 전자메일 시스템은 여러 개의 UA(User Agent)와 메시지를 전달하는 MTA(Mail Transfer Agent)등으로 구성된다. UA는 사용자와 메시지 전송 시스템 사이의 인터페이스를 제공하여 주며, 메시지의 전송을 위한 준비 및 전송된 메시지를 화면에 출력하게 한다. MTA는 메시지 전송 시스템을 구성하는 프로세스로서 메시지의 전송 기능을 수행한다. 만약 사용자 A가 사용자 B에게 메일을 전송할 경우 다음과 같은 과정을 거치게 된다.

한편, POP3(Post Office Protocol 3)를 이용한 메일 수신은 RFC1725 POP3 Protocol을 이용하여 메일 서버로부터 메일을 가져오는 자바프로그램을 말한다. 클라이언트에게 서비스하기위한 새로운 쓰레드를 띄운다.

[1] 사용자 A는 UA에서 메일 메시지를 작성하여 로컬 MTA에 메시지를 전달한다.

[2] 로컬 MTA에 전달된 메일 메시지는 먼저 메일 큐에 저장된 후, 중개전송 대행자들을 거쳐 최종 목적 MTA에 도달한다.

[3] 사용자 B는 로컬 MTA의 수신된 메시지를 확인하고,

이 메시지를 사용자의 UA로 가져온다.

위와 같은 인터넷 전자메일 시스템은 메시지 전송에 있어서는 효율적이며 신뢰성은 있지만, 메시지의 불법 누출, 불법 변조, 메시지 송·수신자의 신원 조작, 송·수신 사실의 부인 등이 가능하며, 인터넷의 광범위한 특성상 송·수신자의 신원을 정확히 확인하기가 어렵다.

2.2 정보보호 서비스

인터넷을 이용한 전자 메일 환경에서는 보안상의 취약점을 방지하기 위해서는 공격에 대처할 수 있는 정보보호 서비스가 필연적이라 할 수 있다. 정보보호 서비스는 내용 기밀성(Confidentiality), 무결성(Integrity), 메시지 발신자 인증(Authentication), 발신 부인 방지(Non-repudiation of Origin), 수신 부인 방지(Non-repudiation of Receipt) 등이 있다.

내용 기밀성은 권한이 없는 사용자들에게 메시지가 노출되어지는 것을 방지하여, 발신자가 원하는 수신자만이 메시지를 확인할 수 있도록 하는 것이다. 기밀성 서비스는 대칭 또는 비대칭 암호 알고리듬 사용하여 제공할 수 있다.

무결성 서비스는 메시지 스트림(stream), 단일 메시지, 또는 메시지의 특정 필드에 적용될 수 있다. 이 서비스는 메시지가 원래 송신된 대로 ,복사, 추가, 수정, 순서변경 또는 재전송 되지 않고 수신됐음을 확인할 수 있다.

발신자 인증 서비스는 메시지가 자기라고 주장하는 실체의 출처로부터 전송되었음을 수신자에게 확인시키는 서비스이다. 일반적으로 인증이라 함은 전송받은 정보의 내용이 변조 또는 삭제되지 않았는지 와 주체가 되는 송수신자가 정당한지를 확인하는 방법을 말한다. 이와 같은 서비스는 발신자의 개인키를 획득하지 않는 한 위조될 수 없기 때문에 디지털 서명으로 제공할 수 있다.

발신 부인 방지는 메시지가 수신됐을 때, 수신자가 그 메시지가 실제로 송신자에 의해서 송신됐음을 확인 할 수 있게 한다.

또한, 수신 부인 방지는 메시지를 송신한 후에, 송신자가 실제로 수신자에 의해서 이 메시지가 수신됐음을 확인할 수 있게 한다. 이러한 수신 부인방지 서비스의 예로 배달증명과 내용 증명 서비스가 있다. 배달증명(Certification of Delivery)은 컴퓨터 통신망을 통해서 주고받는 전자문서에 대해 문서가 올바르게 의도된 수신자에게 배달되었음을 증명해주는 서비스이다. 내용증명(Certification of Content)은 발신자가 수신자에게 어떤 내용의 메시지를 언제 발송하였다는 사실을 증명해주는 서비스이다.

2.3 디지털 서명 및 암호 알고리듬

디지털 서명이란 상대방에게 전송된 메시지에 대해 그 내용이 수정이나 위조되지 않았음을 보장하는 동시에 메시지의 주체인 사용자들이 정확함을 제 3자가 확인할 수 있게 해주는 인증 방식이다. 디지털 서명을 위한 구현방안으로서 주로 ElGamal, RSA (Rivest Shamir Adleman) 등과 같은 공개키 암호 알고리듬을 이용하고 있다[9,10]. RSA 알고리듬은 0 ~ (n-1) 사이의 정수를 modular n 연산을 수행하는 블록암호이다. RSA의 안정성의 근거는 커다란 소수를 소인수 분해하는 적당한 방법이 없다는데 기반을 두고 있어 상당히 커다란 킷값을 사용한다.

디지털 서명을 위해 송신 측에서 증거 생성을 하고 수신 측에서 검증을 위한 과정이 필요하다. 이를 위한 메커니즘으로서 메시지의 크기를 줄이기 위한 해쉬 함수(hash function)와 암호화를 위한 공개키 알고리듬이 사용되고 있다.

본 연구에서의 디지털 서명은 높은 안정성이 인정되고 있는 RSA 알고리듬과 MD5(Message Digest 5) 알고리듬을 이용한다. MD5는 512비트 단위의 메시지 블록을 처리하여 128비트 메시지 축약 값을 생성한다. 4라운드로 구성되며, 각 라운드는 16단계이다. 메시지 축약은 데이터 무결성을 검증하기 위해 사용될 수 있으며, 입력된 데이터 집합으로부터 계산된 암호화 해시 함수라 할 수 있다.

암호화 방법은 크게 대칭형(symmetric) 암호 시스템과 비대칭형(asymmetric) 암호 시스템으로 나눌 수 있다. 대칭형은 송신 측과 수신측이 동일한 비밀키(개인키)를 이용하며, DES(Data Encryption Standard), 3중DES가 이에 속한다. 비대칭형(공개키)은 자유롭게 공개된 공개키와 비밀스럽게 유지되어야하는 개인키로 구성된다. 공개키 시스템의 대표적인 예로는 RSA가 있다. 본 연구에서의 메시지 암호화는 3중 DES를 이용한다.

## 3. 보안 전자메일 시스템 설계

3.1 자바 암호 API

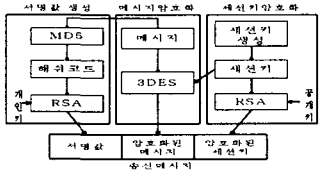
자바 암호 아키텍처(JCA : Java Cryptography Architecture)와 자바 암호 확장(JCE : Java Cryptography Extension)은 자바에서 구현에 무관한 암호 API를 제공한다. JCA는 Java 2 run-time environment의 일부이고, JCE는 JDK1.3에 들어 있지 않는 JCA의 확장 팩이다. JCE는 JCA에서 간단한 암호화와 복호화 API를 제공한다.

JCA는 암호화개념과 알고리듬을 정의하기 위한 설계패턴과 확장 가능한 구조를 명세하고 있으며, 암호화개념을 실제 구현과 독립시키도록 설계되어 있다. SUN사의 JDK에서 기본적으로 제공하는 암호화 구조이며 java.security 패키지와 그 서브패키지 안에 있는 많은 클래스들로 구성되어 있으며, JCE는 javax.crypto 패키지와 그 서브패키지들 안의 클래스로 이루어져 있다.

한편, 본 논문에서 사용할 암호 개념을 나타내는 클래스와 인터페이스는 java.security 와 javax.crypto 패키지를 사용한다. 하지만 SUN의 JCE에는 RSA암호화 기능이 없으므로 세션키를 암호화하는 과정에서는 Bouncy Castle JCE를 사용 한다.

3.2 메시지 암호화 및 서명값 생성

송신 측에서 메시지의 암호화 및 서명값을 생성하기 위한 블록은 <그림 1>과 같이 서명값 생성부, 메시지 암호화부, 그리고 세션키 암호화부로 구성된다.




<그림 1> 메시지 암호화 및 서명값 생성과정

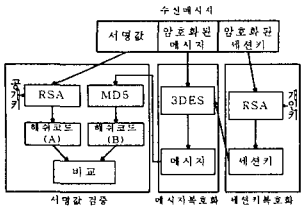
서명값 생성부에서는 서명값 생성을 위해 전송할 메시지를 MD5 알고리듬을 사용하여 해쉬코드를 생성한 다음 송신자의 개인키를 가지고 RSA 알고리듬을 사용하여 생성된 결과값, 즉 서명값을 만든다.

메시지 암호화부에서는 세션키 암호화부에서 만들어진 세션키를 가지고 메시지를 3중DES 알고리듬을 사용하여 암호화된 메시지를 만든다.

세션키 암호화부에서는 3중DES 알고리듬에 사용할 세션키를 만들고 만들어진 세션키를 수신측에게 보내기 위해서는 암호화해야 하기 때문에 송신자의 공개키를 가지고 RSA 알고리듬을 사용하여 암호화된 세션키를 만든다.

3.3 메시지 복호화 및 서명값 검증

수신측에서 메시지의 복호화 및 서명값을 검증하기 위한 과정이 필요하다. <그림 2>는 수신된 메시지 복호화 및 서명값 검증 과정을 나타내며, 서명값 검증부, 메시지 복호화부, 그리고 세션키 복호화부로 구성된다.




<그림 2> 메시지 복호화 및 서명값 검증과정

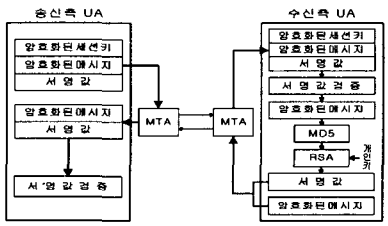
서명값 검증부에서는 메시지 복호화부에서 얻은 메시지를 MD5 알고리듬을 사용하여 해쉬코드(B)를 만들고, 수신메시지의 서명값을 수신자의 공개키를 가지고 RSA 알고리듬을 사용하여 해쉬코드(A)를 얻어 낸다. 이렇게 만들어진 해쉬코드(A)와 해쉬코드(B)를 같은지 올바른지 검증한다.

메시지 복호화부에서는 세션키 복호화부에서 얻은 세션키를 가지고 3중DES 알고리듬 사용하여 암호화된 메시지를 복호화 시켜서 메시지를 얻는다.

세션키 복호화부에서는 암호화된 세션키를 수신자의 개인키를 가지고 RSA 알고리듬을 사용하여 복호화 시켜서 세션키를 얻는다.

3.4 디지털 서명 및 배달증명

<그림 3>은 디지털 서명을 통하여 의도된 수신자가 올바르게 메일 메시지를 수신하였음을 확인하는 배달증명 과정을 보여주고 있다.




<그림 3> 배달 증명 과정

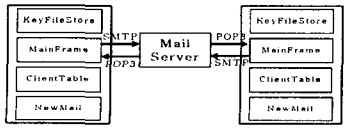
송신 측에서 배달 증명 서비스를 요청했을 때 수신측은 서명값 검증과정을 통하여 서명값이 올바르다면 수신된 메시지의 암호화된 메시지를 가지고 서명값 생성과정을 통하여 새로운 서명값을 만들어서 암호화된 메시지와 함께 송신 측에 보낸다.

송신측은 수신 측에서 보내온 메시지를 가지고 서명값 검증과정을 통하여 서명값이 올바르다면 의도된 수신자가 메시지를 받았다는 것을 알 수 있으므로 배달증명이 된 것이다.

## 4. 전자메일 시스템의 구현 결과

4.1 시스템 구현 및 환경

시스템의 구현은 자바 암호 API 클래스를 기반으로 하였고, GUI(Graph User Interface)을 위해 J빌더6을 사용하였다. 본 논문에서 구현된 보안 전자메일 시스템의 모듈 구성은 <그림 4>와 같다.



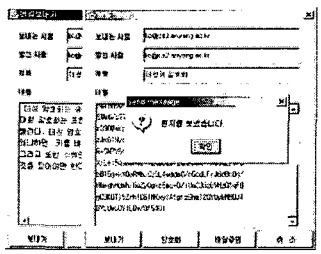

<그림 4> 전자 메일 시스템 모듈

구현된 전자메일 시스템은 메일 클라이언트로 제공되며 메시지의 암호화를 담당하는 NewMail 클래스와 메시지의 복호화와 배달증명을 담당하는 MainFrame과 메일을 보내는 SMTPSender 클래스와 메일을 받는 POP3Reader 클래스와 메일의 내용을 보여주는 ClientTable 클래스와 공개키/개인키 생성 및 저장을 담당 하는 KeyFileStore 클래스로 이루어져 있다. 이와 같이 메일 클라이언트를 기반으로 하기 때문에 MTA의 변경 없이 정보보호 서비스가 가능하며, 메일 메시지를 암호화 및 서명하여 전송함으로써 메시지가 네트워크 상의 전송과정에서 도청되거나, 불법 변조되는 등의 보안상의 문제에 효율적으로 대처할 수 있다.

4.2 구현 결과

4.2.1 메시지 작성 및 암호화

메시지 암호화를 하기 위해선 키생성 버튼을 클릭 하여 키를 저장할 파일의 이름을 입력해서 RSA 알고리듬에 사용할 공개키와 개인키를 저장한다. 메인 메일 시스템 애플리케이션에서 메일 보내기 버튼을 클릭 하여 <그림 5>와 같은 창을 띄운 다음 메시지를 작성하도록 한다.

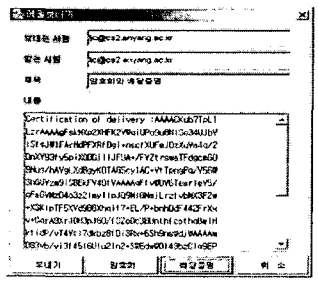


<그림 5> 평문 및 메시지 암호화

<그림 5>의 왼쪽부분은 평문메시지이고 오른쪽은 평문메시지를 암호화하여 전송한 모습을 보여주고 있다. 메시지를 암호화 하기 위해서는 메일 보내기 창에서 암호화 버튼을 클릭 하면 메시지 암호화에 필요한 세션키를 만들고, 이 세션키와 3중DES 알고리듬을 사용해서 암호화하게 된다.

4.2.2 배달 증명 요청

의도된 수신자에게 메시지가 올바르게 도착하였는지 검증하기 위해서는 <그림 6>과 같이 암호화된 메시지의 앞부분에 플래그를 주어 전송해야 한다.

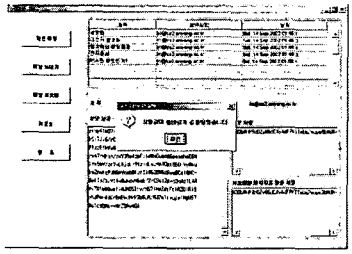


<그림 6> 배달증명 플래그가 붙은 암호화된 메시지

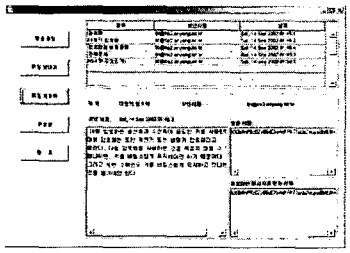
배달증명을 요청하는 플래그를 주려면 메일보내기 창의 배달증명 버튼을 클릭 하여 메시지를 암호화한 다음 암호화된 메시지의 앞부분에 "Certification of delivery :"를 첨부하여 메시지를 전송한다.

4.2.3 메시지 복호화 및 서명 검증

수신메시지를 복호화 하기 위해서는 우선 수신메시지의 암호화된 세션키 부분을 개인키와 RSA알고리듬을 사용해서 메시지 복호화에 쓰이는 세션키를 얻어낸다. 이렇게 얻어낸 세션키와 3중 DES 알고리듬을 사용해서 수신메시지의 암호화된 메시지부분을 복호화시켜 메시지를 얻어낸다. 하지만 메시지가 송신자가 보낸 것인지 검증하고자 할때에는 수신메시지의 서명값을 공개키와 RSA 알고리듬을 사용해서 얻어낸 해쉬코드와 복호화된 메시지를 가지고 MD5알고리듬을 사용하여 만든 해쉬코드가 같은지 검증해야 한다.



<그림 7> 서명값 검증



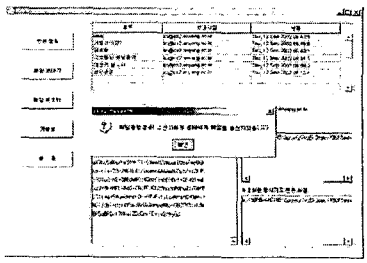
<그림 8> 복호화된 메시지

<그림 7>은 수신된 메시지중 하나를 선택하고 메일 복호화 버튼을 클릭하게 했을 때 위에 설명한 과정을 통하여 얻은 두 해쉬코드를 보여주고 있으며 다이얼로그 박스를 통해 검증여부를 알려주고 있다. <그림 8>은 <그림 7>과 같이 서명값이 올바르게 검증되었을 때 복호화된 메시지를 보여주는 그림이다.

4.2.4 메시지 회신 및 배달 증명

수신된 메시지를 복호화할 때 배달증명을 요청하는 플래그가 있었다면 서명값 검증이 올바르게 된 후 암호화된 메시지를 MD5 알고리듬을 사용하여 해쉬코드를 만들고 개인키와 RSA 알고리듬을 사용하여 서명값을 만든 후, 암호화된 메시지와 함께 송신자에게 전송한다. 이 때 암호화된 메시지의 앞부분에 "Receipt:"플래그를 암호화된 메시지의 처음에 첨부하여 송신자가 배달증명을 요청했던 송신메시지의 회신 메시지임을 알 수 있게 해준다.

송신자는 수신자로부터 받은 암호화된 메시지를 MD5 알고리듬을 사용하여 만들어진 해쉬코드와 수신자로부터 받은 서명값을 공개키와 RSA 알고리듬을 사용하여 얻어낸 해쉬코드를 같은지를 검증하여 배달증명을 한다.



<그림 9> 배달 증명 결과

<그림 9>는 위에 설명한 위에 설명한 서명값을 검증하는 과정을 통하여 얻은 두 해쉬코드를 보여주고 송신자가 보낸 메시지가 올바르게 수신자에게 전송되었음을 다이얼로그 박스를 통하여 보여주고 있다.

## 5. 결론

본 논문에서는 메시지 암·복호화는 물론 디지털 서명 및 배달 증명이 가능 가능한 보안 전자 메일 시스템의 설계 및 구현에 관하여 기술하였다.

구현된 시스템에서는 메시지 기밀성, 무결성, 송신자 인증, 송신자 부인 봉쇄 그리고, 배달증명 서비스를 제공한다. 암·복호 알고리듬은 3중DES를 이용하였고, 서명 인증은 RSA 알고리듬과 MD5를 이용한다.

제안된 시스템의 구현은 자바 암호 API 클래스를 기반으로 하였고[10], GUI(Graph User Interface)를 위해 J빌더 6을 사용하였다.

## 참고문헌

[1] 우준, 하영국, "자바 기반의 배달증명이 가능한 전자메일 시스템 구현", 한국 정보처리학회 논문지 제6권 제11호, 1999.
[2] 나성주, 한선영, "인터네트상의 멀티미디어 전자우편 시스템의 설계 및 구현", 한국 정보처리학회 논문지, 제2권 제6호, 1995.
[3] http://www.pgpi.com.
[4] R. L. Rivest, A. Shrmir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-key Cryptosystems," Communications of the ACM, Vol. 21, No. 2, pp. 120-126, Feb. 1978.
[5] http://www.swiftsite.com/e-gift-baskets/fil_ e-mail_form.htm.
[6] NBS, 'Data Encryption Standard', FIPS Pub, 46, U.S, National Bureau of Standard, Washington DC, Jan. 1977.
[7] ANSI, "Data Encryption Algorithm," American National Standard X3, 92. NY. 1981.
[8] http://www.faqs.org/rfcs/rfc1321.html.
[9] 체신부, "단순우편전송 규약(SMTP) 표준", 1993.
[10] Sun Microsystems, "Java Cryptography Extension Documention", 2000