자바기반의 안전한 전자 메일 시스템 구현

Implementation of Secure E-Mail System based on Java

이 원 구* 김 성 준** 이 희 규*** 조 한 진**** 이 재 광*****
Won-Gu Lee Sung-Jun Kim Hee-Kyu Lee Han-Jin Cho Jae-Kwang Lee

요 약

최근, 컴퓨터와 네트워크의 보급이 일반화되면서, 인터넷을 통한 정보 전달이 일상 생활처럼 되고 있다. 또한, 인터넷, 무선통신, 그리고 자료 교환에 대한 증가로 인해 다른 사용자와 접속하기 위한 방식은 빠르게 변화하고 있다. 이러한 인터넷 사용자간의 자료 교환 수단으로서 전자 메일은 표준이라 말할 수 있을 만큼 많이 사용되고 있고, 현재에는 전세계적으로 보안을 유지하기 위해 보안 메일이 각광을 받고 있다. 일반 편지에서부터 상업광고 목적의 전자 우편에 이르기까지 다양한 분야에서 사용되고 있다. 하지만 이러한 전자 메일에도 많은 문제가 존재한다. 기존의 전자 메일은 간단한 방법으로 내용을 열람하거나 변조할 수 있어 중요한 정보나 사생활 노출의 위험에서 벗어날 수 없다. 이러한 데이터에 대한 보안이 기대에 미치지 못하고 있기 때문에 암호학적으로 강력한 전자 우편 시스템의 개발이 시급하다. 본 논문에서는 기본적인 정보 보호 서비스 외에 기존의 전자 메일 시스템에서는 제공되지 않는 배달 증명 및 내용 증명 기능을 제공하고 자바 암호 API를 사용하여 안전한 키 교환이 가능하도록 하였다.

Abstract

Recently, as computers and networks become popular, distributing information on the Internet is common in our daily life. also, the explosion of the Internet, of wireless digital communication and data exchange on Internet has rapidly changed the way we connect with other people. The e-mail has been commonly used by users as well recognizing it as the standard of manners among users on the Internet. In the past, e-mail has been the primary choice of exchanging information, but secure mail is gaining popularity abroad and domestically because of their nature of providing security. That is, it has been used a variety of fields such as general mail and e-mail for advertisement. But, As the data transmitted on network can be easily opened or forged with simple operations. most of existing e-mail system don't have any security on the transmitted information. Thus, security mail system need to provide security including message encryption, content integrity, message origin authentication, and non-repudiation. In this paper, we design implement secure mail system with non-repudiation service and encryption capability to provide services for certification of delivery and certification of content as well as the basic security services. API.

1. 서 론

인터넷은 전세계를 연결하는 매체로서 그 사용자가 매년 폭발적으로 증가하고 있다. 인터넷을 사용하는 사용자들 간의 의사 교환수단으로서 전자 메일은 표준이라고 말할 수 있을 정도로 광범위하게 사용한다. 안부를 묻는 편지에서부터 상업광고 목적의 편지에 이르기까지 다양한 분야에서 사용되고 있다. 그러나, 공문서와 계약서처럼 법적인 효력을 가지는 중요한 문서는 전자 메일을 이용하여 상호 교환되지 못하고 있다. 그 이유는 전자 메일이 가지는 보안적인 문제점 때문이다. 첫째는 전자 메일 양식상의 문제점이고, 둘째는 프로토콜 상의 문제점이다. 본 논문에서 구현한 전자 메일 시스템은 이러한 보안상의 문제점을 공개키 암호화 방식을 이용하여 해결하였다[1].

* 준 회 원 : 한남대학교 대학원 컴퓨터공학과 석사과정
wglee@netwk.hannam.ac.kr
** 준 회 원 : 한남대학교 대학원 컴퓨터공학과 석사과정
sjkim@netwk.hannam.ac.kr
*** 비 회 원 : 한남대학교 대학원 컴퓨터공학과 박사과정
june@netwk.hannam.ac.kr
**** 비 회 원 : 한남대학교 대학원 컴퓨터공학과 박사과정
hjcho@netwk.hannam.ac.kr
***** 종신회원 : 한남대학교 컴퓨터공학과 부교수
jklee@netwk.hannam.ac.kr

2. 관련 연구

본 절에서는 기존의 PGP. PEM 방식에서 사용하는 전자 메일 표현 방식인 MIME과 프로토콜에 대한 문제점과 본 논문에서 제시한 기법에 대해 기술하기로 한다.

2.1 MIME

전자 메일은 표현방식으로 MIME(Multipurpose Internet Mail Extensions)을 사용하고 있다. 인터넷 상에서 사용되는 HTTP 프로토콜을 비롯해 많은 프로토콜에서 MIME이 사용되고 있다. MIME은 데이터의 내용을 그대로 읽을 수 있거나 또는 간단한 인코딩만을 수행하기 때문에 데이터를 획득한 사람이 약간의 조작만 하면 얼마든지 읽을 수 있는 안전하지 않은 데이터 형식이다. 즉, 만일 어떤 악의를 가진 메일 서버 관리자나, 시스템 침투에 성공한 해커라면 그들에게는 해당 메일 서버를 사용하는 모든 사용자의 프라이버시가 공개되었다고 해도 무방하다.

2.2 전자 메일 프로토콜

전자 메일은 전송 프로토콜로서 SMTP 프로토콜을 사용한다. SMTP 프로토콜은 사용자 메일 서버로의 전송에서부터 메일 서버간 전송에 이르기까지 메일 전송 구간 중 가장 많이 노출된 곳에서 사용되고 있다. 문제는 이 SMTP 프로토콜은 데이터에 어떠한 처리도 하지 않은 채 데이터를 그대로 드러내는 문제점이 있다. 따라서 메일 전송 패킷을 가로챈 해커는 얼마든지 메일을 읽을 수 있고, 또 내용을 바꿔치기 해서 보내도 알 길이 없다. 또한, 사용자가 메일 서버로부터 메일을 수신하는데 있어서 가장 많이 사용되는 프로토콜이 바로 POP3 프로토콜이다. 이 POP3 프로토콜은 SMTP 프로토콜처럼 메일 데이터를 그대로 노출시킨다. 이점 때문에 메일 데이터를 가로채기만 하면 내용이 편집되는 위협에서 벗어날 수 없게 된다. 본 논문에서 구현한 전자 메일 시스템은 이러한 보안상의 문제점을 공개키 암호화 방식을 이용하여 해결하였다.

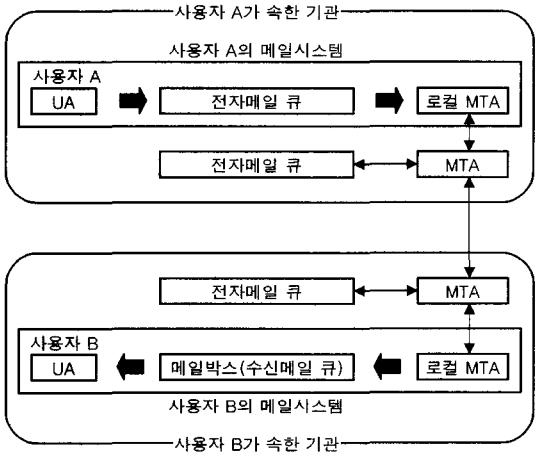
위와 같이 현재 사용하고 있는 PGP. PEM 메일은 보안상 커다란 문제점들을 안고 있다. 즉, 전자의 경우 프로토콜에 관련된 문제이기 때문에 프로토콜을 바꾸지 않는 한 불가능하다. 그러나 후자는 가능하다. 후자의 경우가 본 논문에서 구현한 암호화를 이용한 데이터 보안이다.

본 논문에서 구현한 암호 메일 시스템은 공개키 암호화 방식을 이용한다. 공개키 암호화 방식은 전송자가 수신인을 제외한 다른 사용자가 복호화 할 수 없도록 만드는 방식이다. 따라서 데이터가 전산 관리자나 해커가 메일의 내용에 접근한다 하여도 원문을 얻을 수 없게 되어 전송한 데이터의 안전성을 보장받을 수 있게 된다.

3. 전자 메일 시스템

3.1 전자 메일 시스템의 구조

전자 메일 시스템은 그림 1과 같이 여러 개의 UA(User Agent)와 MTA(Mail Transfer Agent) 등으로 구성되며, 사용자 A가 사용자 B에게 메일을 전



(그림 1) 기존의 전자메일 시스템

송하려 한다면 위와 같은 과정을 거치게 된다[2].

위와 같은 인터넷 전자 메일 시스템은 메시지 전송에 있어서는 효율적이며 신뢰성은 있지만, 메시지의 불법 누출, 불법 변조, 메시지 송·수신자의 신원 조작, 송·수신 사실의 부인 등이 가능하며, 인터넷의 특성상 송·수신자의 신원을 정확히 확인하기가 어렵다[1].

3.2 정보 보호 서비스

인터넷 전자 메일 환경에서는 앞 절에서 기술한 바와 같이 보안상의 취약점에 노출될 수 있다. 이러한 공격에 대처할 수 있는 정보 보호 서비스는 다음과 같다[4,5].

3.2.1 내용 기밀성 (Content Confidentiality)

기밀성은 권한이 없는 사용자들에게 메시지가 노출되어지는 것을 막는 것을 의미한다. 즉, 발신자가 원하는 수신자만이 메시지를 확인할 수 있다. 두 시스템 사이에 가상회선이 개설되었다면 그 가상회선 상에 전송된 모든 사용자 자료를 공개되지 않도록 보호한다.

3.2.2 내용 무결성 (Content Integrity)

메시지 스트림을 대상으로 하는 연결형 무결성 서비스는 메시지가 원래 송신된 대로 즉, 복사, 추가, 수정, 순서변경 또는 재전송되지 않고 수신됐음을 확인한다. 자료에 대한 손상 여부도 무결성 서비스에 의해 제공된다.

3.2.3 발신자 인증(Message Origin Authentication)

발신자 인증은 통신이 신뢰성을 갖도록 보증한다. 발신자 인증 서비스는 메시지가 자기라고 주장하는 실체의 출처로부터 전송되었음을 수신자에게 확인시키는 서비스이다. 이같은 서비스는 전자 서명으로 제공할 수 있다. 전자 서명은 발신자의 개인키를 획득하지 않는 한 위조될 수 없다. 전자 서명을 가진 메시지는 일반적으로 재 사용되지 않는다.

3.2.4 부인 방지(Repudiation)

① 발신 부인 방지 (Non-repudiation of Origin)

메시지가 수신됐을 때, 수신자가 그 메시지가 실제로 송신자에 의해서 송신됐음을 확인할 수 있게 한다.

② 수신 부인 방지 (Non-repudiation of Receipt)

메시지를 송신한 후에, 송신자가 실제로 수신자에 의해서 이 메시지가 수신됐었다는 것을 확인할 수 있게 한다. 이러한 수신 부인 방지 서비스의 예로 배달 증명과 내용 증명 서비스가 있다.

· 배달 증명 (Certification of Delivery)

부인 방지 서비스 중의 하나로써 컴퓨터 통신망을 통해서 주고받는 전자 문서에 대해 문서가 올바르게 의도된 수신자에게 배달되었음을 증명해주는 서비스이다.

· 내용 증명 (Certification of Content)

발신자가 수신자에게 어떤 내용의 메시지를 언제 발송하였다는 사실을 증명해주는 서비스이다.

4. 부인 방지 서비스

4.1 배달 증명 서비스

배달 증명 서비스는 내용 증명 서비스와 연계되어 제공되는 보안 서비스로 현행 우편제도하에서의 특수 우편물 취급 서비스가 그대로 적용될 수 있다. 이들 서비스를 전자 메일에서 제공하기 위한 방식은 직접 방식과 조정자 이용 방식으로 구분된다[3]. 그리고 본 논문에서는 이 두 가지 방식의 장·단점을 비교 분석하여 간편하게 배달 증명 서비스를 제공할 수 있는 방식을 제안하였다.

4.1.1 직접방식

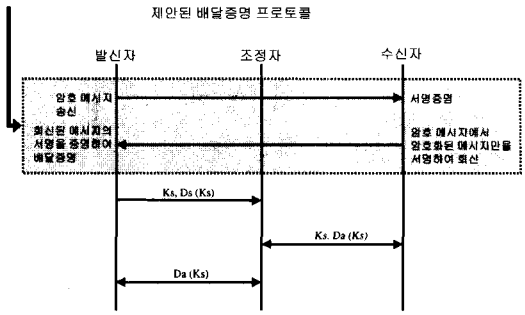
UA가 MTA를 경유하여 직접 다른 UA에게 메일을 전달하는 방식으로, 대표적인 모델은 MHS이다. 이러한 배달 증명 서비스를 제공하기 위하여 많은 시도가 있어왔지만, 수신 증명 서비스를 제공하려고 할 경우 공평한 관계가 이루어지지 못하며 어느 한쪽이 이익을 보게된다.

4.1.2 조정자 이용방식

수신자와 송신자 사이에 모든 참가자가 신뢰할 수 있는 제 3의 조정자를 선정하여 모든 전자 메일이 이를 통하여 행하여지는 것으로 직접 방식의 문제점을 근본적으로 해결할 수 있다. 그러나 조정자가 필요하므로 이로 인한 프로토콜의 증가로 오버헤드가 증가하고 시스템의 구성이 복잡해진다.

4.1.3 제안된 방식

조정자를 이용한 방식은 프로토콜의 증가로 사용자에게 부담을 가중시켜 실질적인 사용을 저해하는 요인이 될 수 있다. 제안된 방식은 조정자 이용방식 중 공평한 부인방지 프로토콜로 가장 최근에 소개된 ZG(Zhou and Gollmann) 방식[3]을 응용하여 배달 증명 서비스를 제공하는 프로토콜을 수용하였다. 그림 2에는 조정자를 이용한 ZG 방식을 응용하여 제안한 배달 증명 프로토콜을 기술하고 있다. 즉, 발신자가 일반 메시지(평문, Plain text)를 암호 알고리즘인 SEED 알고리즘에 의해 암호화하여 수신자에게 전송한다. 그러면, 수신자는 수신한 메시지에 대해 발신자에게 배달 증명을 하기 위해 암호화된 메시지에 서명 알고리즘인 ElGamal 알고리즘으로 서명을 하여 발신자에게 재전송하게 된다. 마지막으로, 발신자는 수신자로부터의 데이터(즉, 비밀키에 의해 암호화된 메시지와 서명)에 대해 수신자의 공개키와 서명 알고리즘에 의해 서명을 검증하여, 수신자에게 올바로 전달되었는지를 확인할 수 있다.

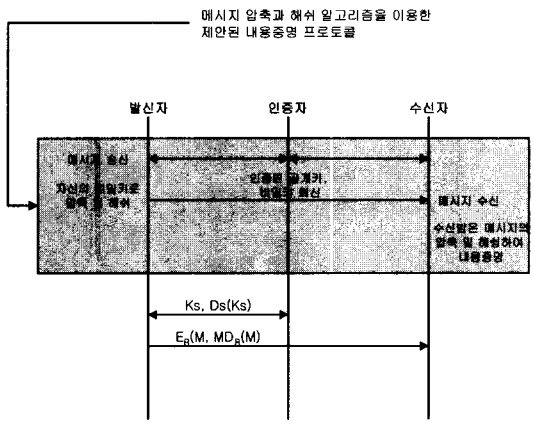


(그림 2) 제안된 배달 증명 프로토콜

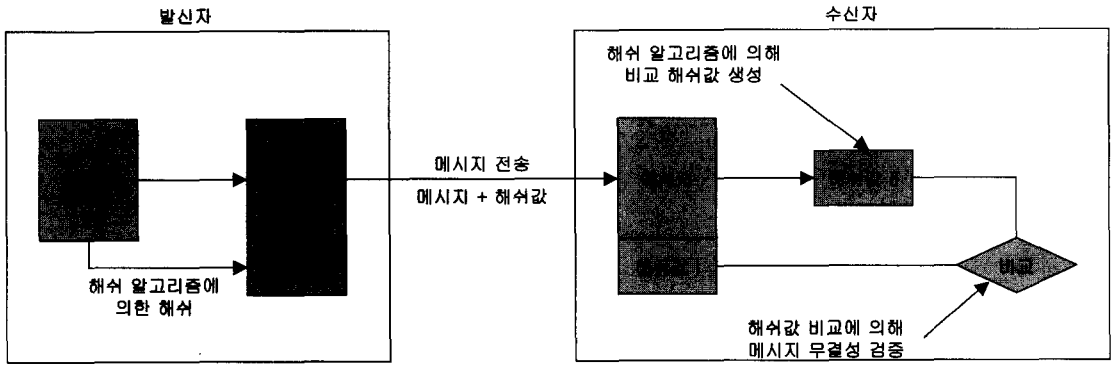
4.2 내용 증명 서비스

내용 증명 서비스는 배달 증명 서비스와 연계되어 제공되는 보안 서비스로 메시지 압축과 해쉬 알고리즘을 이용하여 서비스를 지원할 수가 있다. 본 논문에서는 위 두 가지 방식을 이용하여 내용 증명 서비스를 지원하였다. 본 논문에서 제안한 방식은 다음과 같다. 내용 증명 서비스를 제공하기 위해, 메시지 압축과 해쉬를 이용함으로서, 수신자가 발신자로부터 온 메시지가 변경되지 않았다는 것에 대해 신뢰할 수 있게 된다. 아래 그림 3에서는 이러한 내용 증명 서비스를 제공하기 위한 전체적인 프로토콜을 보여준다.

위에서 제시한 프로토콜은 다음과 같은 흐름에 의해 내용 증명 서비스를 제공한다. 발신자는 수



(그림 3) 제안된 내용 증명 프로토콜



(그림 4) 해쉬 함수를 통한 메시지 무결성 검증 모델

신자에게 송신할 메시지와 그 메시지를 해쉬 알고리즘인 MD5 알고리즘에 의해 해쉬한 데이터를 함께 보낸다. 그러면, 수신자는 발신자로부터의 데이터에 대해 다시 해쉬하여, 발신자가 보낸 해쉬 값과 비교한다. 만일 같으면, 내용이 바뀌지 않았다는 메시지 무결성을 확인하게 된다.

해쉬 알고리즘은 그림 4와 같이 동작하며, 위의 모델에서 단방향 해쉬 알고리즘에 의해 생성된 해쉬값은 유일한 값이다. 따라서, 위의 메시지 무결성 검증 모델을 통해 메시지 무결성을 지원하게 되며, 본 논문에서는 여러 가지의 해쉬 알고리즘 중 MD5 해쉬 알고리즘을 적용하였다.

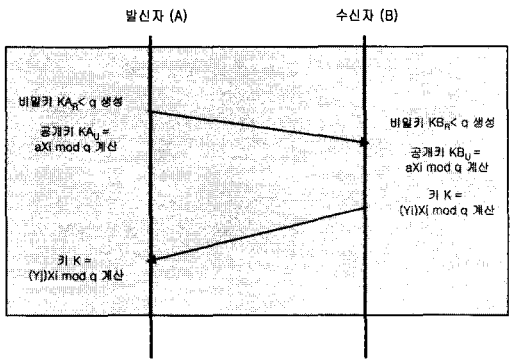
5. 안전한 전자 메일 시스템의 설계

5.1 자바 암호 구조

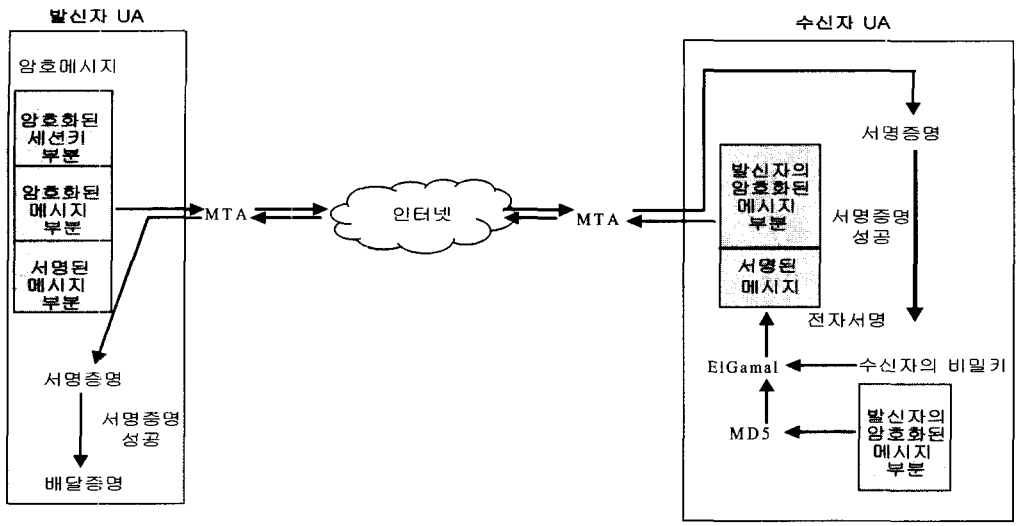
자바 플랫폼에서는 자바 암호 패키지를 이용하여 쉽게 보안 서비스를 구현할 수 있다. 자바 암호 패키지는 Java Security API 소프트웨어 구조를 기반으로 하고 있다. 암호 클래스의 전반적인 설계는 JCA(Java Cryptography Architecture)를 기반으로 한다. JCA는 설계 패턴, 암호 개념, 알고리즘을 정의하기 위한 설계 패턴, 그리고 확장된 구조를 명시한다. JCA는 구현 시 암호 컨셉을 분류하기 위해서 설계되었다. JCE(Java Cryptography Extension)는 JCA의 확장이며, SunJCE라는 다른 암호 Provider를 포함하고 있다. JCE는 핵심 JDK의 일부분이 아니라 JDK와 함께 동작하는 패키지로 추가하여 사용할 수 있는 표준 확장 라이브러리이다[7,9].

5.2 안전한 키 교환 모델

발신자와 수신자가 안전하게 메일을 주고받기 전에, 반드시 상호 키 교환이 필요하게 된다. 본 논문에서는 안전하게 키 교환을 하기 위해 DIFFIE-HELLMAN 알고리즘을 이용한 키 교환 모델을 구현하였다. 이 모델은 이산 대수를 계산하는 난이도를 이용하여 안전한 키 교환을 지원하게 된다. 이러한 키 교환 과정을 구현한 모델은 그림 5와 같다[1].



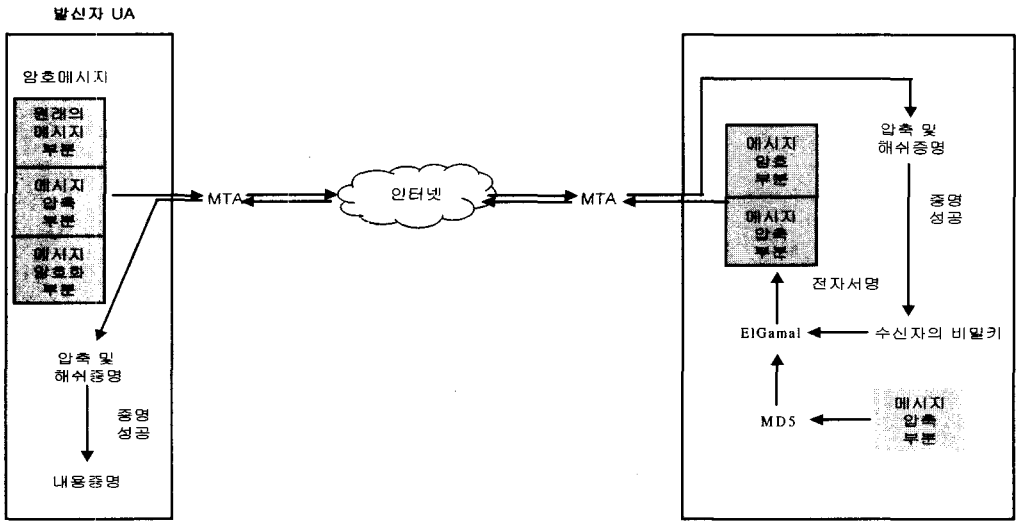
(그림 5) DIFFIE-HELLMAN을 이용한 안전한 키 교환 모델



(그림 6) 배달 증명 모델

5.3 안전한 배달증명 모델

그림 6은 앞에서 제안된 배달 증명 방식을 기반으로 한 배달 증명 모델을 통해서 의도된 수신자가 올바르게 메일 메시지를 수신하였음을 확인하는 과정을 보여주고 있다. 그리고 암호화된 메시지의 서명을 위해서는 암호 모델에서와 같이 MD5와 ElGamal 알고리즘을 사용한다. 향후 배달 증명을 제공하기 위한 방식으로 현재 국내에서 연구가 진행되고 있는 ElGamal 알고리즘을 통한 불확정 전송 프로토콜을 적용 하고자 한다. 불확정 전송 프로토콜은 송신자가 수신자에게 어떤 비밀 정보를 보내고자 할 때 수신자는 그 비밀 정보를 1/2의 확률로 취할 수 있게 하고, 송신자는 수신자가 그 비밀 정보를 취했는지 여부를 1/2의 확률로 추측할 수 있게 하는 프로토콜로써 전



(그림 7) 내용 증명 모델

자 우편에 적용되어 공평한 배달 증명 모델을 설계하는 데 도움을 줄 것으로 기대된다.

5.4 안전한 내용 증명 모델

앞에서 제안된 내용 증명 방식을 기반으로 한 내용 증명 모델을 통해서 수신자는 발신자가 보낸 메시지가 변조되지 않고 전달되었다는 것을 확인하는 과정이 그림 7에 보여지고 있다. 발신자가 보낸 메시지와 메시지 압축 알고리즘인 MD5에 의해 압축되어진 후, 해쉬 알고리즘에 의해 해쉬되어진 데이터가 수신측에 보내어진다. 이 때, 해쉬되어진 데이터는 원래의 메시지로 환원되진 않게 되어, 메시지가 변경되지 않았다는 내용 증명 서비스를 할 수 있게 되는 것이다. 수신측에서는 메시지를 해쉬하여, 발신자가 보낸 해쉬값과 비교하게 되고, 이러한 과정을 통하여 내용 증명을 하게 된다.

5.5 안전한 암호화 모델

본 전자 메일 시스템에서 보안 서비스를 제공하기 위한 암호 모델은 아래에 제시된 알고리즘들을 기반으로 한다.

5.5.1 암호화 알고리즘

① 메시지 암호화 알고리즘 : SEED 알고리즘

SEED 알고리즘은 널리 사용되는 관용 암호 알고리즘이며, 데이터를 128비트 키를 이용한다. 관용 암호 알고리즘이기 때문에 암호화와 복호화에 사용되는 키가 하나이고 속도가 빠르다.

② 전자 서명 알고리즘 : ElGamal, MD5 알고리즘

ElGamal 알고리즘은 유한체에서의 이산대수 계산의 어려움에 기반을 두고 있으며, 전자 서명과 암호화에 사용되는 공개키 암호 알고리즘이다. MD5 알고리즘은 MIT의 Ron Rivest가 개발한 것으로 임의의 길이의 메시지를 입력으로 받아들여서 일정한 길이의 비트열(메시지 다이제스트)을 출력하는 해쉬함수이다.

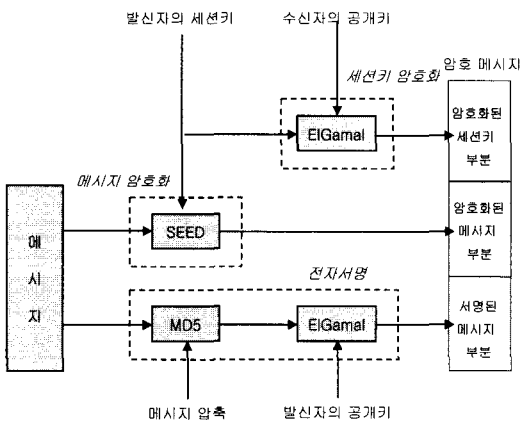
5.5.2 메시지 암호화 모델

발신자가 메시지를 암호화하여 생성하는 암호 메시지는 암호화된 세션키 부분, 암호화된 메시지 부분, 그리고 서명 부분으로 구성된다. 그림 8은 다음에 기술한 메시지 암호화 과정을 거쳐 암호 메시지를 생성하는 과정 및 구현 코드를 보여준다.

① 메시지를 SEED 알고리즘을 사용해서 발신자의 세션키로 메시지를 암호화한다. 그리고 진하게 강조된 글자는 사용된 알고리즘을 보여주고 있다.

② 메시지 암호화에 사용된 SEED 세션키를 ElGamal 알고리즘을 사용해서 암호화한다.

③ MD5 알고리즘을 사용해서 메시지 다이제스트를 생성하고, 이 메시지 다이제스트를 ElGamal 알고리즘으로 암호화하여 전자 서명을 생성한다.



(그림 8) 메시지 암호화

5.5.3 메시지 복호화

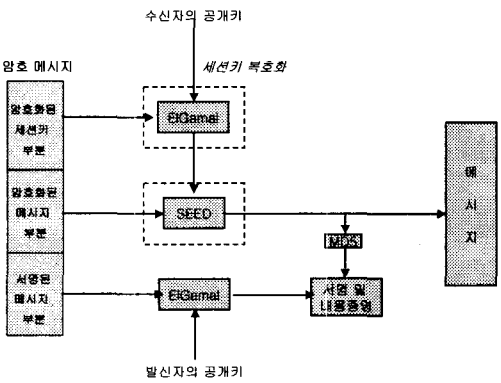
수신된 암호 메시지는 메시지의 각 부분별로 복호화 및 서명을 증명하는데, 그림 9는 이러한

과정을 보여준다.

① ElGamal 알고리즘을 사용해서 SEED 세션키를 복호화 한다.

② SEED 알고리즘을 사용해서 복원된 DES 세션키를 가지고 암호문을 복호화 한다.

③ 복원된 평문 메시지를 MD5 알고리즘을 사용해서 메시지 다이제스트로 변환하고, ElGamal 알고리즘을 사용해서 전자 서명을 증명하게 된다.

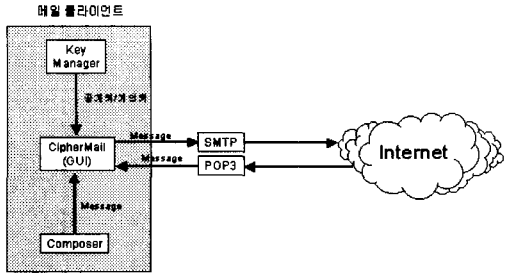


(그림 9) 메시지 복호화

6. 안전한 전자 메일 시스템의 구현

6.1 모듈 구성

본 전자 메일 시스템은 메일 클라이언트로 제공되며, 메시지의 암호화와 복호화 및 배달 증명을 담당하는 CipherMail 클래스와, 메일 메시지를 저장하고 관리하는 Message 클래스를 핵심으로 하고 있다. 이와 같이 메일 클라이언트를 기반으로 하기 때문에 MTA의 변경 없이 정보보호 서비스가 가능하며, 메일 메시지를 암호화 및 서명하여 전송함으로써 메시지가 네트워크 상의 전송 과정에서 도청되거나, 불법 변조되는 등의 보안상의 문제에 효율적으로 대처할 수 있게 되었다. 그림 10은 Message 클래스를 사용하는 CipherMail 애플리케이션 모듈을 구성하는 클래스들의 구성도이다.



(그림 10) 전자메일 시스템 모듈

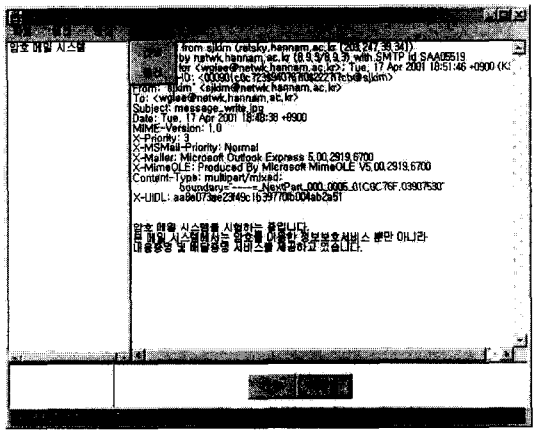
각각의 클래스에 대한 기능을 기술하면 다음과 같다. 메일 송/수신 클래스로는 POP3 클래스와 SMTP 클래스가 있다. 메일 수신 클래스인 POP3 클래스는 POP3 메일 서버로부터 수신된 메시지를 확인하고 사용자의 메일 프로그램으로 메일 메시지를 가져오는 역할을 한다. 메일 송신 클래스인 SMTP 클래스는 설정된 SMTP 메일 서버에 메일 메시지를 전달하는 역할을 한다. 암호화 메일 전송 클래스에는 Send 클래스가 있다. 이 Send 클래스는 새로운 메시지를 작성하는 윈도우를 생성하고, 수신자의 메일 주소와 수신자의 공개키를 선택하고 메일 제목과 본문을 입력하여 메일 메시지를 작성할 수 있게 한다. 키 관리 클래스에는 KeyManager 클래스가 있다. 키 생성 및 공개키 관리 클래스인 KeyManager 클래스는 ElGamal 키 쌍을 생성하고 메시지를 송신하고자 하는 상대방 수신자의 공개키를 관리하는 역할을 한다. 끝으로, 전체 메일 시스템의 메인 윈도우로는 CipherMail 클래스가 있다. 이 CipherMail 클래스는 메일 메시지 리스트를 관리하고 메시지의 내용을 출력하는 메인 애플리케이션 윈도우이다. 그리고 Composer 클래스에 의해서 생성된 메시지를 암호·복호화 및 배달 증명하는 기능을 한다.

6.2 구현 결과

6.2.1 메시지 작성 및 송신

메시지를 작성하기 위해서는 시작 윈도우의 메뉴에서 메시지 작성 메뉴 혹은 버튼을 선택한다.

(그림 11) 메시지 작성



(그림 12) 메시지 암호화 및 서명

Certification of Repudiation : bAd3am5hZssJG+jlkklJJUAAgxuZrsq5+dATONIEZxAiqudx7ppYs+74RARd9H8L6rmjPTuyaDMpm+SOE+pLUI4+BNK2FfwawgzcjdgWGGrrdBvN7Iz18yDhazbTIYsdvA0MtRxsnB5y7dojkuKVQf8R09327yVGW4VAAP/3pIPgYXxJuYLAAAAgFur8S7UYEW7aU5qh556yjwvHSmZUiZ3Yxyg2ZNRf9VKR6Iz22ZBDJAVmEHNNr9L+CYFRgKIm/yxfycwC
.....

(그림 13) 암호화된 메시지

그림 11에서는 메시지 작성 윈도우의 메뉴 바에서 '보안 기능 사용' 메뉴와 '배달 증명 사용', 그리고 '내용 증명 사용' 메뉴를 선택하여 기본 보안 기능과 배달 증명 서비스, 그리고 내용 증명 서비스를 제공받을 수 있도록 설정하였다. 마지막으로 메시지 전송 버튼을 누르면 그림 12와 같이 메일 메시지의 암호화 및 서명 등의 과정을 거쳐 의도된 수신자에게 메시지를 전송한다.

그림 13은 메시지 암호화 및 서명을 통해서 생성된 암호 메시지 자체를 출력한 것으로 배달 증명을 요청하기 위해서 "Certification of Re-pudiation" 태그를 암호 메시지의 맨 처음에 첨부하였다.

6.2.2 메시지 수신 및 서명 증명

메시지를 수신한 수신자의 메일 프로그램은 배달 증명과 내용 증명을 요구하는 메시지임을 메시지 내의 플래그를 인지하여 확인하고, 서명을 증명하여 그림 14와 같이 서명이 올바르게 증명되었음을 다이얼로그 박스에 출력한다. 그리고 수신된 메시지 중에서 암호화된 메시지만을 서명하고 발신자의 암호화된 메시지와 함께 "Receipt:" 플래그와 "Content" 플래그를 메시지의 처음에 첨부하여 발신자에게 회신한다.

6.2.3 메시지 회신 및 부인 방지

회신 메시지를 수신한 발신자는 메시지에 붙어 있는 두 플래그가 배달 증명과 내용 증명에 대한 회신 메시지를 나타냄을 확인한다. 그리고 수신된 메시지의 서명을 증명하여 배달 증명과 내용 증명이 확인되었음을 나타내는 다이얼로그 박스를 그림 15와 같이 출력한다.

6.3 비교 분석

본 논문에서 구현한 메일 시스템은 메시지 기밀성, 메시지 무결성, 송신자 인증, 송신자 부인 봉쇄 서비스 등을 제공하며, PGP와 PEM에서 아직까지 제공하지 않고 있는 배달 증명 서비스를 제공한다. 표 1은 본 논문에서 구현한 메일 시스

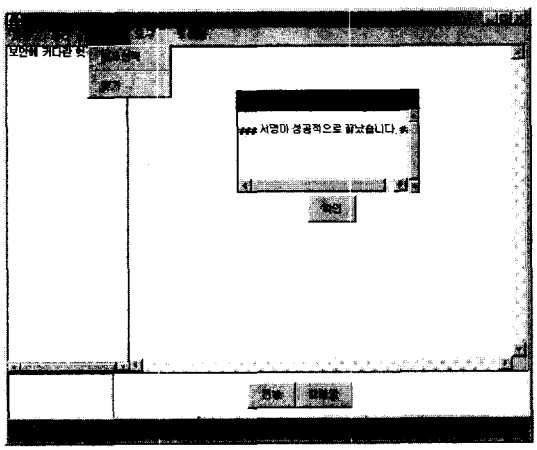
(표 1) PGP 및 PEM과 제안된 메일 시스템 비교

정보 보호 서비스	제안된 시스템	PGP	PEM
메시지 기밀성	제공함	제공함	제공함
메시지 무결성	제공함	제공함	제공함
송신자 인증	제공함	제공함	제공함
송신부인봉쇄	제공함	제공함	제공함
배달증명	제공함	제공하지 않음	제공하지 않음
내용증명	제공함	제공하지 않음	제공하지 않음

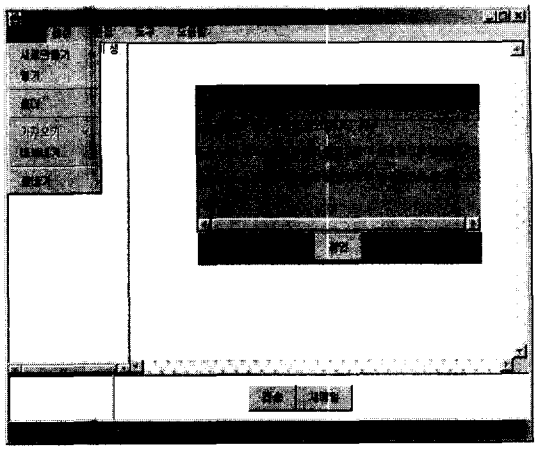
템과 PGP 및 PEM에서 제공하고 있는 정보보호 서비스에 대한 비교를 기술하고 있다.

7. 결 론

현재 네트워크 환경에서 널리 사용되고 있는 전자메일 시스템은 많은 보안상의 취약점에 노출되어 있다. 이러한 전자 메일의 취약점을 극복하기 위해서 다양한 보안 메일 시스템들이 소개되고 있는 추세이지만 사용자에게 만족스런 서비스를 제공하지 못하고 있다. 본 논문에서는 기존의 메일 시스템에서 제공되는 기본 보안 서비스를 제공하며, 의도된 수신자가 메시지를 올바르게 수신하였음을 증명하는 배달 증명 서비스와 내용이



(그림 14) 수신된 메시지의 서명 증명



(그림 15) 회신된 메시지의 부인증명

변경되지 않았음을 증명하는 내용 증명 서비스, 그리고 메시지 교환 이전에 안전하게 키를 교환하기 위한 키 교환 모델을 설계·구현하였다. 구현은 자바 암호 API를 기반으로 하였으며, 이를 포함한 자바 플랫폼은 네트워크 및 보안 서비스를 제공하는 데 필수적인 모든 요소들을 클래스로 갖추고 있기 때문에 개발자에게 프로그램의 작성을 용이하게 한다.

향후 보안 메일 시스템에서는 부인 방지 서비스 및 안전한 키 교환 서비스를 제공하면서도, 기존의 시스템(암호화하지 않은 채, 메일을 전송하는 시스템)과 전송속도 차이가 나지 않는 메일 시스템을 구현함으로써, 상호간에 신뢰하면서도 빠른 메일 서비스를 제공하는 방법을 모색해야 할 것이다.

Acknowledgement

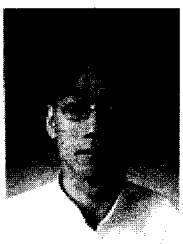
이 논문은 본 학회 2001년도 "춘계학술발표대회" 최우수 논문임

참 고 문 헌

[1] 최용락, 소우영, 이재광, 이임영, "통신망 정보 보호", 그린출판사, 1995

[2] 조한진, 김봉한, 이재광, "정보보호 서비스를 위한 Secure E-mail 시스템 설계", 한남대학교 산업기술연구소, 1998
[3] 손진욱 편저, "Java 2 Programing Bible", 정보문화사, 1999
[4] 박춘식, "배달 및 내용 증명이 가능한 전자메일", 통신정보보호학회지, 제7권 제2호, 1997. 6.
[5] 강명희, "인터넷 메일 시스템에서의 정보 보호 서비스 구현", 광운대학교 전자계산학과 석사학위 논문, 1995
[6] 이재용, 이기수, 장춘서, "PGP를 이용한 WWW 메일 시스템의 설계 및 구현", 한국정보과학회 가을 학술발표논문집, 제24권 제 2호, 1997
[7] 홍주영, 윤이중, 김대호, "전자우편 시스템의 보호 방식 분석", 통신정보보호학회지 Vol.4 No.2, 1994. 6
[8] J.Zhou and D. Gollmann, "Observations on Non-repudiation", Advances in Cryptology, Proceedings of ASIACRYPT '96, Spring-Verlag, 1996
[9] Elliotte Rusty Harold, "Java Network Programing", O' REILLY, 1997
[10] Jonathan Knudesen, "Java Cryptography", O' REILLY, 1998
[11] J.Zhou and D. Gollmann, "A Fair Non-repudiation Protocol", Proc. of the 1996 IEEE Symposium on Security and Privacy, 1996
[12] Scott Oaks, "Java Security", O' REILLY, 1998
[13] Bruce Schneier, "Applied Cryptography", John Wiley & Sons Inc., 1996
[14] Sun Microsystems, "Java 2 SDK, Standard Edition Documentation", 1999

◐ 저 자 소 개 ◑



이 원 구
2000년 한남대학교 컴퓨터공학과 (공학사)
2000년 한남대학교 대학원 컴퓨터공학과 석사과정
관심분야 : 컴퓨터네트워크, 정보통신 정보보호
E-mail : wglee@netwk.hannam.ac.kr

김 성 준
2000년 한남대학교 컴퓨터공학과 (공학사)
2000년 한남대학교 대학원 컴퓨터공학과 석사과정
관심분야 : 컴퓨터네트워크, 정보통신 정보보호
E-mail : sjkim@netwk.hannam.ac.kr

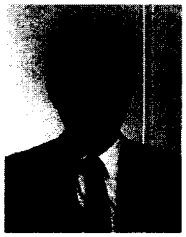
◐ 저 자 소 개 ◑

이 희 규

1998년 우송대학교 컴퓨터과학과 (공학사)
2000년 한남대학교 대학원 컴퓨터공학과 (공학석사)
2000년 현재 한남대학교 대학원 컴퓨터공학과 박사과정
관심분야 : 컴퓨터네트워크, 정보통신 정보보호
E-mail : june@netwk.hannam.ac.kr

조 한 진

1997년 한남대학교 컴퓨터공학과 (공학사)
1999년 한남대학교 대학원 컴퓨터공학과 (공학석사)
1999년 현재 한남대학교 대학원 컴퓨터공학과 박사과정
관심분야 : 컴퓨터네트워크, 정보통신 정보보호
E-mail : hjcho@netwk.hannam.ac.kr



이 재 광

1984년 광운대학교 전자계산학과 (이학사)
1986년 광운대학교 대학원 전자계산학과(이학석사)
1993년 광운대학교 대학원 전자계산학과(이학박사)
1986년 1993년 군산전문대학 전자계산학과 부교수
1997년~1998년 University of Alabama 객원교수
1993년~현재 한남대학교 컴퓨터공학과 부교수
관심분야 : 컴퓨터 네트워크, 정보통신 정보보호
E-mail: jklee@netwk.hannam.ac.kr