通信情報保護學會論文誌
第 7 卷 第 2 號, 1997. 6

# 인터넷 메일 시스템에서의 정보보호 서비스 구현

강 명 희*, 신 효 영**, 유 황 빈***

# An Implementation of the Security Service on Internet Mail System

Myung Hee Kang, Hyo Young Shin, Hwang Bin Ryou

## 요 약

현재 사용되고 있는 대부분의 전자 메일 시스템은 전달되는 메시지의 불법 누출, 불법 변조, 송·수신자의 신원 불분명, 송·수신 행위의 부인 등의 정보보호 위협요소를 가지고 있으며, 이에 대한 대책이 요구되고 있다. 본 논문에서는 인터넷의 메일 시스템을 대상으로 정보보호 서비스를 구현하여 기존의 인터넷 메일 시스템에서의 정보보호에 대한 취약성을 보완하였다. 구현된 메일 시스템에서는 기존의 PEM이나 PGP에서 제공하고 있는 메시지 기밀성, 메시지 무결성, 송신자 신분 인증, 송신 부인 봉쇄 등의 정보보호 서비스를 제공할 뿐만 아니라, 아직까지 PEM이나 PGP에서는 제공하고 있지 못한 메시지 재전송 방지, 내용증명을 통한 수신 부인 봉쇄 서비스를 제공한다. 또한 본 논문에서는 디지털 서명 생성시 서명 블록을 생성하여 서명을 수행함으로써, 디지털 서명에 있어 보다 안전성을 높였으며, 암호화 블록을 생성하여 암호화 키를 암호화함으로써, 암호화 키에 대한 안전성 또한 높였다.

## Abstract

Most of the currently used electronic mail system has the threat of security such as illegal leak of message, forgery, uncertain identity, denial of sending and receiving, and so forth. The security for this system is not satisfied yet, thus we explore these problems. In this thesis, we implement the security services for internet mail system which cover the weakness for traditional mail system. This system provides not only security services which PEM and PGP provides (i.e message confidentiality, message integrity, originator authentication, non-repudiation of origin), but also message replay prevention, and non-denial of recipient using certification of contents. In addition, this system increases security of the

* 백두정보기술/주, EP&C 팀
* * 경성전문대학 사무자동화과
* * * 광운대학교 전자계산학과

digital signature by signing with signature block formatting on the creation of it. And it increases security of the digital enveloping by encrypting with encryption block formatting of message encryption key.

## 1. 서 론

전자 메일 시스템은 개인간의 서신, 문서 교환이나 공고, 안내문 등의 다양한 정보 뿐만 아니라 기업간의 공식적인 문서 교환에 이르기까지 다양한 용도로 이용되고 있다. 그러나 현재 사용되고 있는 전자 메일 시스템에서는 정보의 불법 누출, 불법 변조, 송·수신자의 신원 조작 및 송·수신 행위의 부인 등이 발생할 가능성이 높다.

인터넷에서는 전자 메일 시스템에서의 정보보호에 대한 취약성을 보완하기 위하여 1993년 2월에 IETF(Internet Engineering Task Force)의 PEM(Privacy Enhanced Mail) WG과 IRTF(Internet Research Task Force)의 PSRG(Privacy and Security Research Group)의 공동 연구로 PEM에 대한 RFC 문서를 발표하였다.[1, 6, 8, 9, 10] RFC 문서에는 암호화 기법을 기반으로한 메시지 암호화와 인증 과정, 인증서 기반의 키 관리 및 분배에 대해서 기술되어 있으며, 메시지 기밀성, 메시지 무결성, 송신자 신분 인증, 송신 부인 봉쇄 등의 정보보호 서비스를 제공하고 있다.

본 논문에서 구현한 메일 시스템은 PEM에서 제공하고 있는 정보보호 서비스들과 수신자가 송신자로부터 수신한 데이터를 조작하여 제3자에게 전달하고, 제3자가 송신자로부터 메시지를 수신하였다고 주장하는 메시지 재전송(Message Replay)에 대처할 수 있는 기능 즉, 메시지 재전송 방지 서비스와 내용 증명(Certification of Contents)을 통한 수신 부인 봉쇄(Non-repudiation of Recipient) 서비스를 제공한다.

## 2. 인터넷 메일 시스템의 정보보호

### 2.1 정보보호 서비스

전자 메일 시스템에서의 정보보호 서비스에는 메시지의 불법 누출, 불법 변조 등을 막고, 송·수신자의 신원을 확인할 수 있는 송·수신자 인증과 송·수신 사실에 대한 부인 봉쇄 등이 있다. 또한 수신자가 송신자로부터 수신한 데이터를 조작하여 제3자에게 전달하여, 제3자가 송신자로부터 메시지를 수신하였다고 주장하는 경우에 대처할 수 있는 기능 등이 필요하다. 표 1은 전자 메일 시스템에서 고려될 수 있는 정보보호 서비스를 나타내고 있다.[4, 7, 16]

표 1 메일 시스템에서의 정보보호 서비스

| 정보보호 서비스 | 서비스 기능 |
|---|---|
| 메시지 기밀성 | 메시지 전송중에 발생할 수 있는 메시지의 불법적인 누출을 막기 위하여 메시지를 암호화한다. |
| 메시지 무결성 | 메시지 전송중에 발생할 수 있는 메시지에 대한 불법적인 변조 여부를 검사한다. |
| 송신자 신분 인증 | 메시지 수신자에게 메시지의 송신자 신원을 확인 시켜 준다. |
| 송신 부인 봉쇄 | 메시지 수신자에게 메시지 송신자에 대한 증거를 제공하여 송신자가 메시지의 송신 사실을 부인할 수 없도록 한다. |
| 수신 부인 봉쇄 | 수신자의 메시지 수신 사실을 부인할 수 없도록 한다. |
| 메시지 재전송 방지 | 제3자가 송신자로부터 메시지를 수신하였다고 주장하는 경우에 대처한다. |

## 2.2 PEM

인터넷에서는 SMTP를 사용하는 기존의 메일 시스템에 메시지 기밀성, 메시지 무결성, 송신자 인증, 송신 부인 봉쇄 등의 정보보호 서비스를 제공하기 위하여 PEM (Privacy Enhanced Mail)을 정의하였다.[1, 6, 8, 9, 10, 16] PEM은 TCP/IP프로토콜을 사용하는 각종 기술 지원 및 연구 개발을 담당하는 두 기구인 IRTF와 IETF에서 개발한 권고안으로 RFC 821 SMTP를 사용하는 메일 시스템의 정보보호에 대한 취약성을 보완하기 위한 것이다. 다음 그림 1은 PEM의 구조를 나타낸 것으로, 송신측 UA는 필터링 방식을, 수신측 UA는 통합 방식을 사용한 예이다.[8] 송신측에서는 메시지를 생성하고 PEM 필터를 통하여 메시지를 암호화하거나 디지털 서명 등을 수행하여 기존의 인터넷 메일 시스템의 UA 에 전달한다. UA는 메시지를 인터넷 메일 메시지 형식으로 구성하여 MTA 전달하고, MTA는 수신측에 RFC 821 SMTP를 이용하여 메시지를 전달한다. 수신측에서는 UA와 PEM 모듈이 통합되어 있기 때문에 메시지 복호화, 메시지 검색, 디지털 서명에 대한 검증 등은 UA에서 처리된다.

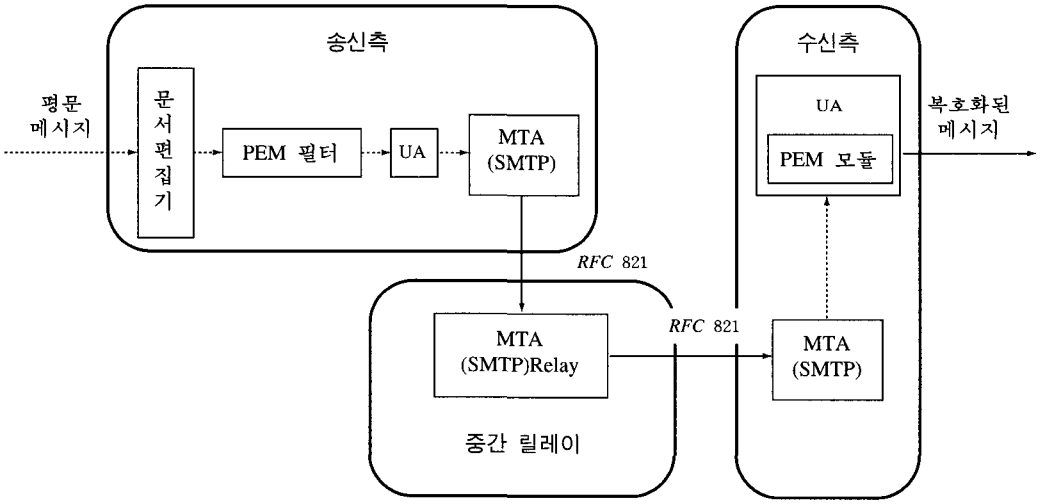



그림 1. PEM의 구조

PEM 필터나 PEM 모듈내에서는 메시지를 암호화 시키거나 디지털 서명 생성, 검증등의 기능을 수행하며 구체적인 과정은 다음과 같다.

• 송신자 A

(1) 생성 메시지를 해쉬함수 h를 이용하여 해쉬코드 h(M)을 생성하고, 해쉬코드 h(M)을 자신의 비밀키 $SK_A$를 이용하여, 생성한 디지털 서명 $E_{SKA}[h(M)]$와, 자신의 인증서 $Cert_A$와 함께 수신자 B에게 전송한다.

(2) 메시지를 DES-CBC 알고리즘을 이용하여 암호화한 $E_K[M]$를 수신자 B에게 전송한다.

(3) 수신자 B가 메시지를 복호화할 수 있도록 세션 DES키 K를 수신자 B의 공개키 $PK_B$로 암호화한 $E_{PKB}[K]$를 수신자 B에게 전송한다.

• 수신자 B

(1) $E_{PKB}[K]$를 자신의 비밀키 $SK_B$로 복호화 한다.

(2) K를 이용하여 $E_K[M]$을 복호화하여 메시지를 검색한다.

(3) 복호화한 메시지를 해쉬함수 h를 이용하여 해쉬코드 h(M')을 생성한다.

(4) 송신자 A의 인증서 $Cert_A$를 이용하여 A의 공개키 $PK_A$를 습득하고, $PK_A$를 이용하여 디지털 서명 $E_{SKA}[h(M)]$을 복호화하여 h(M)을 구한다.

(5) h(M')와 h(M)을 비교하여 디지털 서명에 대한 유효성을 검증한다.

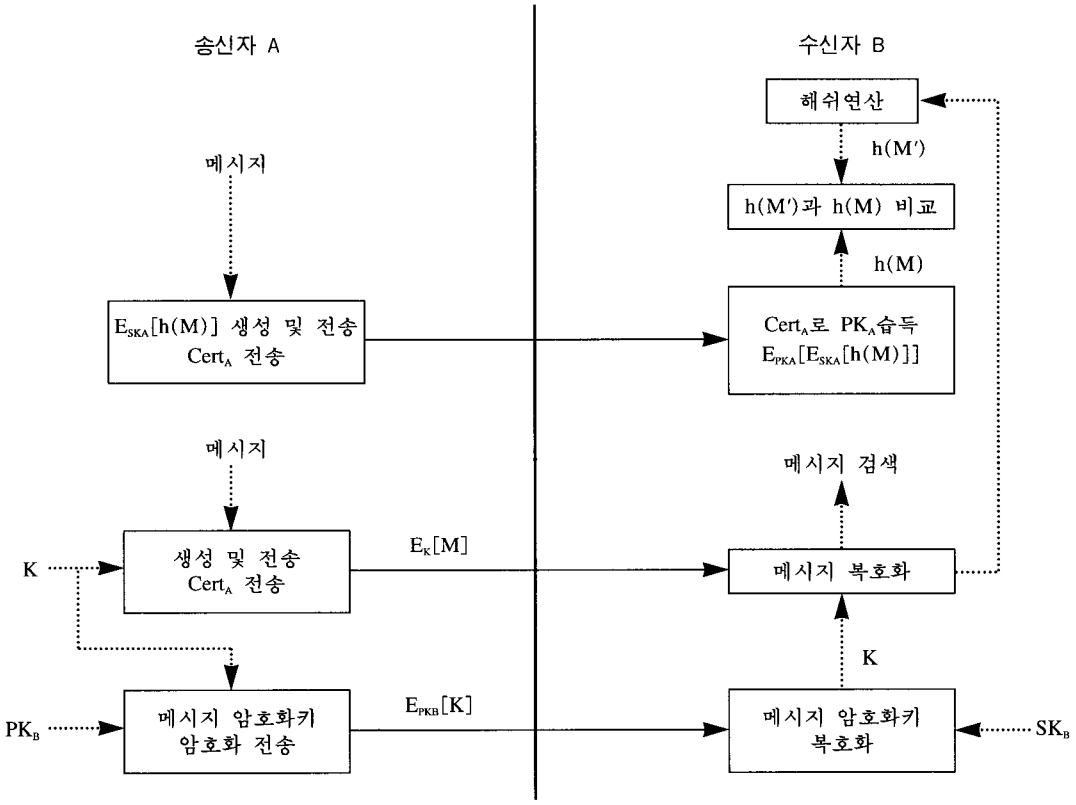



그림 2. PEM에서의 메시지 암호화 및 디지털 서명

## 3. 구현 모델

### 3.1 메시지 재전송 방지

메시지 재전송은 수신자가 송신자로부터 수신한 데이터를 조작하여 제3자에게 알려주고, 제3자는 송신자로부터 메시지를 수신하였다고 주장하는 경우이다. 구체적인 메시지 재전송 과정은 그림 3과 같다.

(1) 수신자 B는 송신자 A로부터 전달받은 데이터중 $E_{PKB}[K]$를 자신의 비밀키 $SK_B$로 복호화 한다.

(2) K, $E_K[M]$, $E_{SKA}[h(M)]$, $Cert_A$를 제3자 C에게 전송한다.

(3) 제3자 C는 자신의 공개키 $PK_C$로 세션 DES 키 K를 다시 암호화한 $E_{PKC}[K]$를 생성하여, 수신자 B로부터 전달받은 데이터[1] 즉 $E_K[M]$, $Cert_A$, $E_{SKA}[h(M)]$와 $E_{PKC}[K]$를 메일 형식에 맞춰 재구성하여 송신자 A로부터 메시지를 수신하였다고 주장한다.

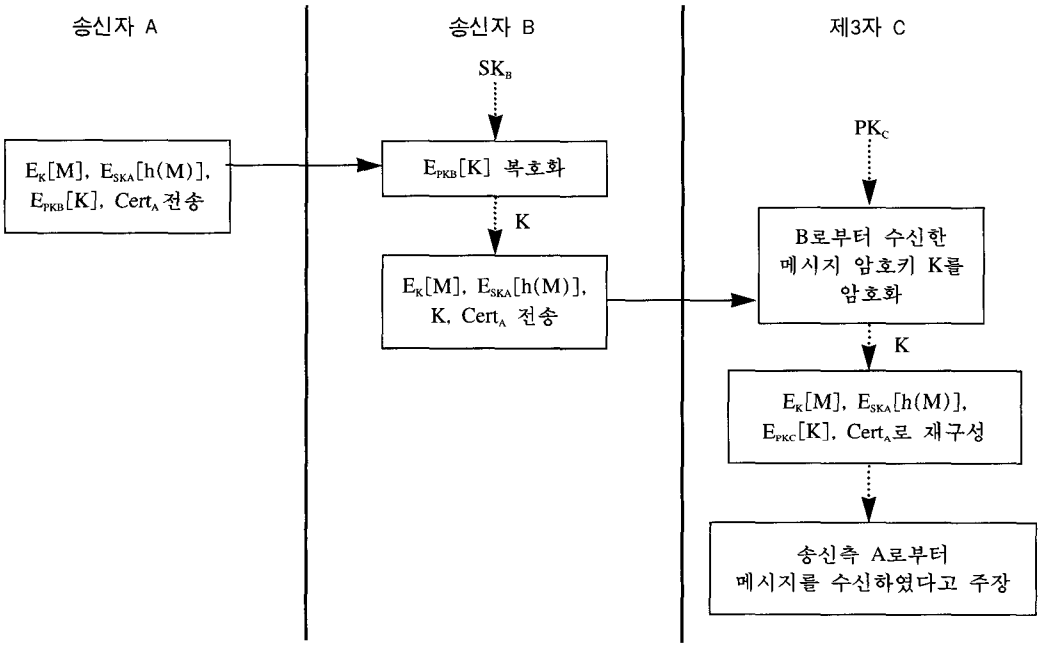



그림 3. 메시지 재전송

본 논문에서는 메시지 재전송 방지[2]를 위해서 송신자 A가 디지털 서명 생성시 메시지 뿐만 아니라 수신자 B의 인증서 또한 해쉬 처리하여 자신의 비밀키로써 디지털 서명을 생성한다. 따라서, 디지털 서명에는 메시지의 수신자가 B임을 증명할 수 있는 해쉬코드 정보가 있다. 이 경우에는 수신자가 제3자에게 자신의 비밀키와 송신자 A로부터 수신한 데이터를 전달하면 제3자는 암호화된 세션 DES 키를 수신자의 비밀키를 이용하여 복호화한 다음 메시지를 검색할 수 있지만, 송신자 A의 비밀키를 알 수 없기 때문에 디지털 서명을 변조할 수 없다. 만약 제3자가 확실히 송신자 A로부터 메시지를 수신하였다면 디지털 서명에는 제3자 C에 대한 인증서의 해쉬코드가 있어야 하는데, 실제로는 수신자 B에 대한 인증서 해쉬코드가 있기 때문에 제3자 C가 송신자 A로부터 메시지를 수신하였다고 주장할 수가 없다. 따라서, 본 논문에서 제안하고 있는 디지털 서명 방법은 메시지와 수신자의 인증서를 해쉬 처리하여 디지털 서명을 생성함으로써 메시지 재전송에 대하여 대처할 수 있다.

1 메시지만을 해쉬 처리한 디지털 서명에는 수신자와 관련된 정보가 없다.

2. 송신자 A로부터 수신한 메시지를 수신자 B가 제3자에게 전송하는 것 자체를 방지하는 것은 아니다.

### 3.2 메시지 암호화 및 디지털 서명

본 논문에서 정보보호 서비스를 제공하기 위해서 사용하고 있는 알고리즘은 표 2와 같다.[1, 2, 3, 5, 6, 8, 9, 10, 13, 14, 16]

표 2. 사용하는 알고리즘

| | |
|---|---|
| 메시지 기밀성 | DES-CBS 알고리즘 |
| 메시지 무결성 | MD5 메시지 다이제스트 알고리즘 |
| 디지털 서명 및 검증 | RSASA-BR 알고리즘 (768 비트 키) |
| 인증서 생성 및 내용증명 통지서에 대한 디지털 서명 | RSASA-BR 알고리즘 (768 비트 키) |
| 난수 생성 | DES-EDE, ANSI X9.17 |
| DES 키 및 초기화 벡터 생성 | ANSI X9.17, MD5 메시지 다이제스트 알고리즘 |
| 메시지 암호화 키 암호화 방법 (Digital enveloping) | RSAES-BRMJ (Optimal Asymmetric Encryption Padding) |

본 논문에서는 DES 키와 초기화 벡터(Initialize Vector)를 생성을 위해 먼저 ANSI X9.17에 명시된 난수(Random Number) 생성 방법을 이용하여 난수를 생성하고, 이 난수에 NULL 데이터 8 바이트를 다시 패딩한 다음, MD5 해쉬연산을 수행하여 해쉬코드의 상위 8 바이트를 DES 키로 사용하고, 하위 8 바이트를 초기화 벡터로 사용한다.[14, 16]

또한 디지털 서명과 메시지 암호화키 암호화(Digital enveloping)를 위해 IEEE P1363 working draft에 따라 입력 데이터를 재구성하여 결정적(deterministic)[3] 방식을 랜덤화시켜 probabilistic한 방식으로 전환하여 보다 안전성을 높이도록 하였다.[2, 3, 5] 다음 그림 4와 5는 디지털 서명 블록과 Digital enveloping을 위한 암호화 블록의 생성 및 검증 방법을 나타내고 있다. Seed는 ANSI X9.17의 난수 생성기를 이용하여 생성하고, G와 H는 MD5 해쉬 알고리즘을 이용하여 난수를 원하는 비트 만큼 추출할 수 있도록 한 만든 함수이다.[2, 3, 5]

그림 4의 디지털 서명 블록 생성 및 검증 과정에 대한 구체적인 내용은 다음과 같다.

• 디지털 서명 블록 생성 과정

(1) ANSI X9.17의 난수 생성기를 통해서 Seed 값을 생성한다.

(2) 서명하고자 하는 메시지 M과 Seed 값을 연결(Concatenation) 시켜 H 함수에 입력시켜 MD(Message Digest) 값을 생성한다.

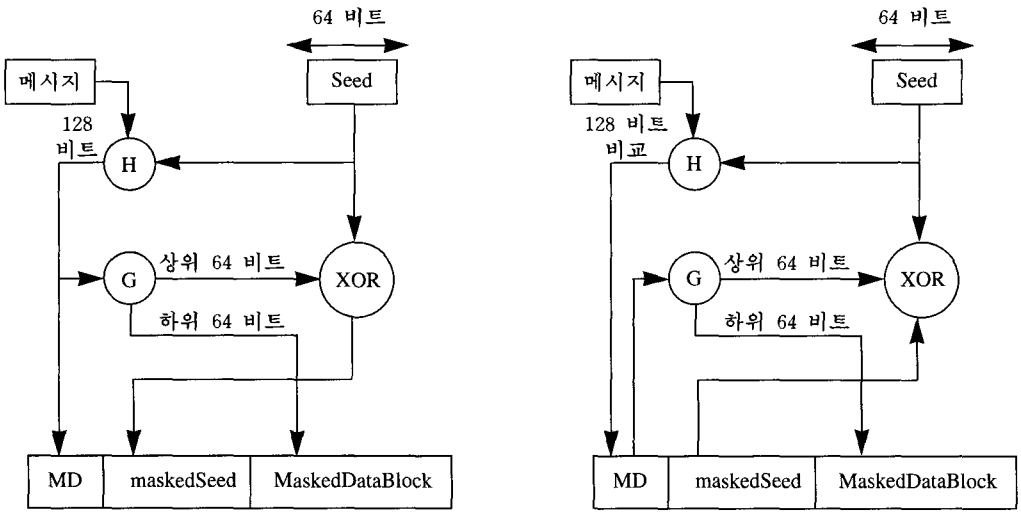
(3) MD 값을 G 함수에 입력하여 얻은 결과값의 하위 64비트를 MaskedDataBlock 으로, 상위 64 비트는 Seed 값과 XOR 연산 결과를 maskedSeed 값으로 생성한다.

(4) MD, maskedSeed , MaskedDataBlock 을 각각 연결하여, 디지털 서명 블록을 생성한다.

• 디지털 서명 블록 검증 과정

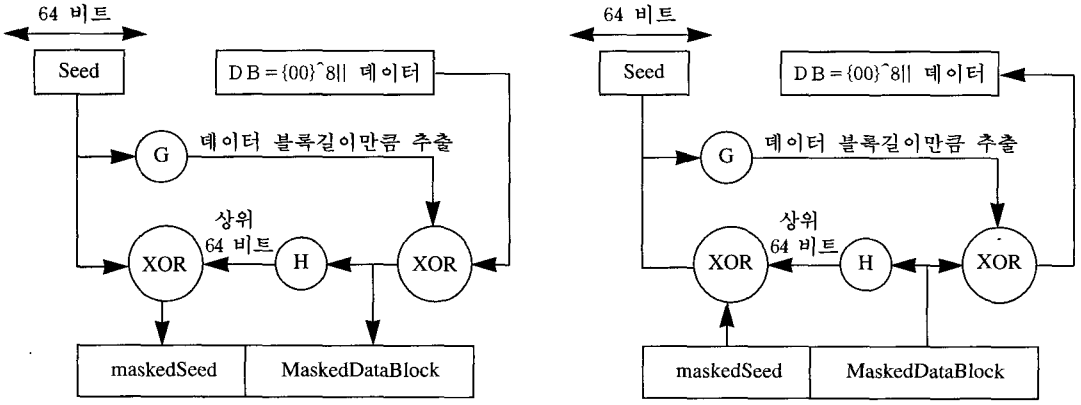
(1) 디지털 서명 블록의 MD 부분을 G 함수

3 입력 데이터와 서명 키가 같으면 항상 같은 서명을 만들어낸다.




(1) 디지털 서명 블록 생성 과정 (2) 디지털 서명 블록 검증 과정

그림 4. 디지털 서명 블록 생성 및 검증 과정




(1) 암호화 블록 생성 과정 (2) 암호화 블록 검증 과정

그림 5. 암호화 블록 생성 및 검증 과정

에 입력시킨 결과값의 하위 64 비트를 디지털 서명 블록의 MaskedDataBlock 과 동일한지 비교한다.

(2) 동일하면, G 함수의 결과값의 상위 64 비트와 디지털 서명 블록의 maskedSeed 와 XOR 연산하여 Seed 값을 구한다.

(3) 검증하고자 하는 메시지 M과 Seed 값을 연결시켜 H 함수에 입력시켜 디지털 서명 블록의 MD 값과 비교하여, 디지털 서명의 유효성을 검증한다.

그림 5의 암호화 블록 생성 및 검증 과정에 대한 구체적인 내용은 다음과 같다.

• 암호화 블록 생성 과정

(1) ANSI X9.17의 난수 생성기를 통해서 Seed 값을 생성한다.

(2) NULL 값 8바이트와 데이터를 연결시켜 데이터 블록을 생성한다.

(3) Seed 값을 G 함수에 입력시킨 결과값을 데이터 블록의 길이 만큼 추출하여 데이터 블록과 XOR 연산을 수행하여 MaskedDataBlock을 생성한다.

(4) MaskedDataBlock을 H 함수에 입력하여 상위 64 비트를 추출하여 Seed 값과 XOR 연산하여 Seed를 생성한다.

(5) MD, maskedSeed, MaskedDataBlock 을 각각 연결하여, 암호화 블록을 생성한다.

• 암호화 블록 검증 과정

(1) MaskedDataBlock을 H 함수에 입력시킨 결과값의 상위 64 비트를 추출하여 Seed 값과 XOR 연산하여 Seed 값을 구한다.

(2) Seed 값을 G 함수에 입력시킨 결과값을 데이터 블록의 길이 만큼 추출하여 암호화 블록의 MaskedDataBlock과 XOR 연산하여 데이터 블록을 구한다.

(3) 데이터 블록의 하위 8바이트가 NULL 값인지 비교하고, 데이터를 검색한다.

논문에서 제공하고 있는 정보보호 서비스인 메시지 기밀성, 메시지 무결성, 송신자 인증, 송신자 부인 봉쇄, 메시지 재전송 방지 서비스를 위한 메시지 암호화 및 디지털 서명 과정은 그림 6과 같다.

• 송신자 A

(1) 수신자 B의 인증서 $Cert_B$를 인증서 관리국에 요청하여 얻는다.

(2) 메시지 M을 그림 4와 같이 디지털 서명 블록 SB(M)을 생성한다.

(3) 메시지 재전송에 대처하기 위해서 수신자 B의 인증서 $Cert_B$[4] 또한 디지털 서명 블록 $SB(Cert_B)$로 구성한다.

(4) 메시지에 대한 디지털 서명 블록 SB(M)과 수신자 B의 인증서에 대한 서명블록 $SB(Cert_B)$를 연결(Concatenation)하여 자신의 비밀키 $SK_A$로 RSA 암호화 연산한 디지털 서명 $E_{SKA}[SB(Cert_B)||SB(M)]$을 생성한다.

(5) 자신의 인증서 $Cert_A$와 $E_{SKA}[SB(Cert_B)||SB(M)]$를 수신자 B에 전송한다.

(6) 메시지를 암호화하기 위해서 필요한 세션 DES키 K를 생성한다.

(7) K로 메시지를 암호화한 $E_K[M]$을 생성하여 수신자 B에 전송한다.

(8) 수신자 B의 인증서 $Cert_B$를 이용하여 B의 공개키 $PK_B$를 습득하고, K를 그림 5와 같이 암호화 블록 EB(K)를 생성한다.

(9) EB(M)을 B의 공개키 $PK_B$로 암호화한 $E_{PKB}[EB(K)]$를 수신자 B에 전송한다.

• 수신자 B

(1) $E_{PKB}[EB(K)]$를 자신의 비밀키 SKB로 복호화한다.

(2) 그림 5와 같이 EB(K)를 암호화 블록 검증 과정을 통하여, K를 얻고 K를 이용하여 메시지를 복호화 한 다음, 메시

4 수신자 B의 인증서 $Cert_B$에는 수신자 B의 신분을 확인할 수 있는 정보가 있다.

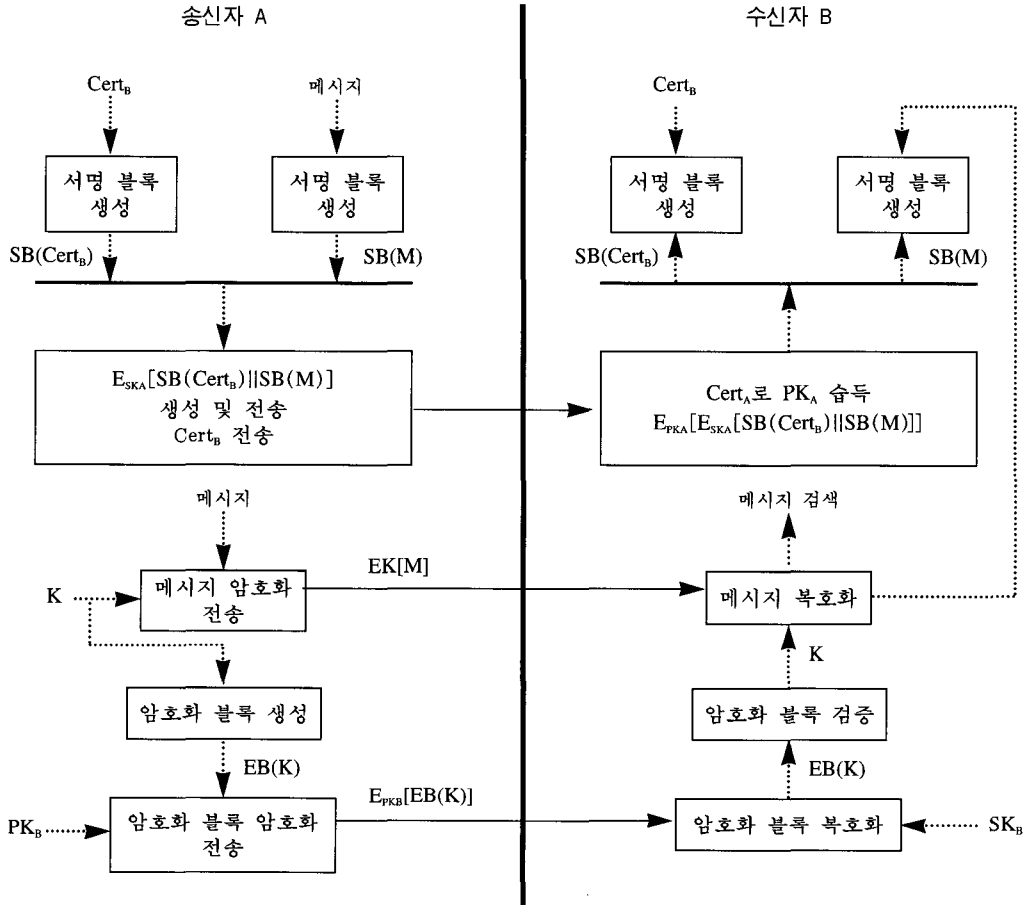



그림 6. 메시지 암호화 및 디지털 서명

지를 검색한다.

(3) 송신자 A의 인증서 $Cert_A$를 이용하여 A의 공개키 $PK_A$를 습득하고, $PK_A$를 이용하여 디지털 서명 $E_{SKA}[SB(Cert_B)||SB(M)]$을 복호화하여 $SB(Cert_B)$, SB(M)를 구한다.

(4) $SB(Cert_B)$와 자신의 인증서 $Cert_B$를 그림 4와 같은 디지털 서명 블록 검증 과정을 통하여 비교하고, SB(M)과 복호화한 메시지 M도 또한 그림 4와 같은 디지털 서명 블록 검증 과정을 통하여 비교하여, 디지털 서명 대한 유효성을 검증한다.

본 논문에서 메시지를 DES-CBC 모드 알고리즘을 사용하여 암호화하여 수신자 B에게 전달하기 때문에 메시지 기밀성을 유지한다. 그리고, 송신측과 수신측에서는 디지털 서명 생성과 검증 작업을 통하여 메시지 무결성, 송신자 신분 인증 서비스를 제공한다. 또한, 송신자 A의 비밀키 SKA는 송신자 A 이외에는 누구도 알 수 없기 때문에 송신자 부인 봉쇄 서비스를 제공한다. 수신자 B는 송신자 A로부터 수신한 데이터(암호화된 메시지, 디지털 서명, 송신자 A의 인증서)를 조작하여 제3자 C에게 알려주어도 송신자 A의 비밀키 SKA를 알지 못하여 디지털 서명을 변조할 수 없고, 디

지털 서명에는 수신자 B의 신원을 알 수 있는 수신자 인증서의 디지털 서명 블록이 있기 때문에 메시지 재전송에 대하여 대처할 수 있다.

그러나 기존의 암호화, 디지털 서명 생성 방법에 비하여, 암호화 블록, 디지털 서명 블록 등의 부가적인 계산상의 오버헤드가 있으며, 특히 특정 사용자 그룹에 본 논문에서 제안한 메시지 재전송 방지 기법을 적용할 경우에는 사용자 그룹에 대한 공개키/비밀키의 생성 및 관리 방안, 사용자 그룹 인증서의 생성 및 관리, 분배 방안이 없는 한, 각각의 사용자의 인증서에 대해서 디지털 서명 블록을 생성하고, 디지털 서명을 생성하여야 하는 문제점이 발생한다.

### 3.3 내용 증명

내용 증명은 언제, 누가, 누구에게 어떠한 내용의 메시지를 송신하였는가를 증명하는 것이다. 본 논문에서는 내용 증명을 통하여 수신 부인 봉쇄 서비스를 제공하고자 한다. 그림 7은 인증서 관리국이 중재자 역할을 담당하여 내용증명 과정을 나타내고 있다.

(1) 송신자 A는 암호화한 메시지, 디지털 서명, $Cert_A$를 각각 인증서 관리국(Certifi-cate Authorities)에 전송하고 분쟁에 대비하여 저장한다.

(2) 인증서 관리국은 분쟁 발생시에 대비하여 A로부터 수신한 데이터에 Time Stamp를 생성하여 수신한 데이터와 함께 저장한다.

(3) 인증서 관리국은 A로부터 수신한 데이터를 B에 전송한다.

(4) 인증서 관리국은 송신자에게 내용증명 통지서를 Cert__Cont__tag를 생성하고, 내용증명 통지서에 대한 디지털 서명을 생성하여 각각 송신자 A에 전송한다.

(5) 수신자 B는 인증서 관리국으로부터 수신한 데이터를 복호화하여 메시지를 검색하고, 디지털 서명 검증을 수행한다.

(6) 송신자 A가 내용증명 통지서 Cert__Cont__tag와 통지서에 대한 디지털 서명 $E_{SKCert}$[SB(Cert__Cont__tag)], 수신자에게 전송한 메일을 인증서 관리국에 전송하여 내용증명 요청한다.

(7) $E_{SKCert}$[SB(Cert__Cont__tag)]에 대한 디지털 서명 검증과정을 통하여 내용증명 통지서의 변조 여부를 검증한다.

(8) 인증서 관리국은 수신한 통지서로 내용증명 메일 서버에 저장된 데이터를 검색하여, 송신자 A로부터 수신한 데이터와 비교함으로써 내용증명을 수행한다.

본 논문에서 제공하고 있는 수신 부인 봉쇄 서비스를 제공하기 위해서는 인증서 관리국의 본래의 기능(인증서의 생성 및 분배, 관리 등) 이외에 내용증명을 위한 대용량의 저장 공간이 필요하며, 내용증명 수행 기능을 담당하는 서버가 필요하게 되며, 인증서 관리국에 대한 좀 더 높은 안전성이 요구된다.

## 4. 설계 및 구현

### 4.1 시스템 구조

본 논문에서 구현한 메일 시스템에서 송·수신자간의 메시지 전송 프로토콜은 RFC 821 SMTP(Simple Mail Transfer Protocol)을 사용하였다. 또한 송신자와 인증서 관리국간의 인증서의 요청, 전송, 내용 증명을 위한 통신 프로토콜은 TCP/IP 프로토콜을 사용하였고, 인

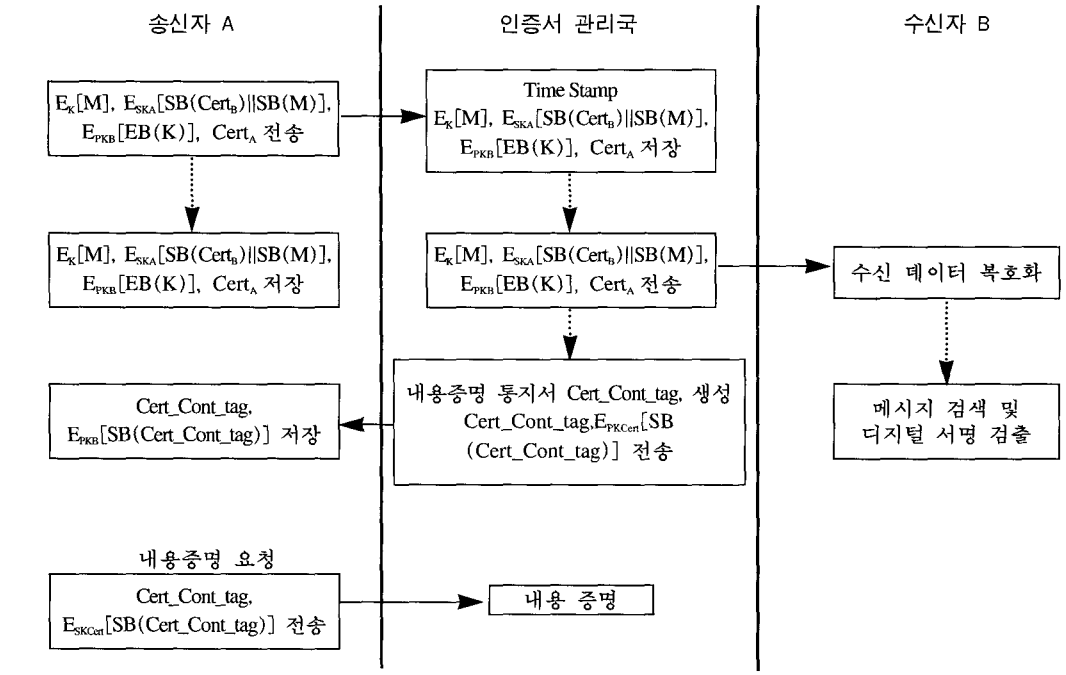



그림 7. 내용증명

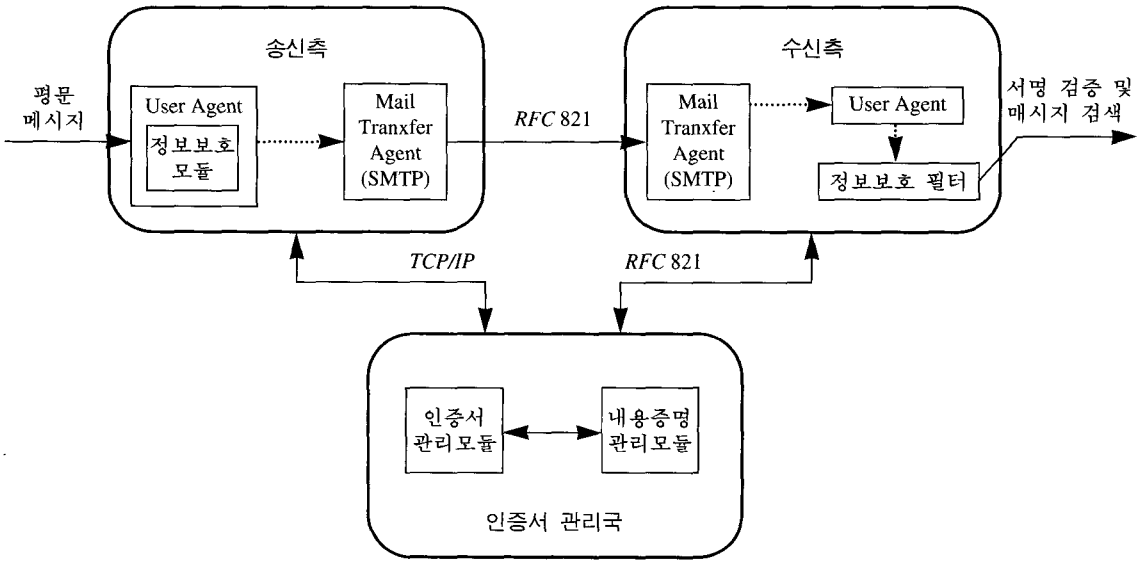



그림 8. 시스템 구조

증서 관리국과 수신측간의 통신 프로토콜은 RFC 821 SMTP를 사용하였다. 송신측의 메일·클라이언트는 정보보호 모듈을 UA(User Agent)와 통합하여 구현하였으며, 수신측은 UA와 정보보호 모듈을 분리하여 기존의 메일 시스템을 사용할 경우에도 정보보호 필터 모듈만 있으면 메시지 검색 및 디지털 서명 검증을 수행할 수 있도록 하였다. 그림 8은 본 논문에서 구현한 메일 시스템의 구조이다.

## 4.2 구현 결과

본 논문에서 구현한 메일 시스템 환경은 SunOS 4.1.3 환경에서 GNU 컴파일러 gcc 2.6.3을 사용하였으며, 사용자 인터페이스는 Motif를 사용하였다. 구현한 메일 시스템은 송신측의 메일 클라이언트 부분과 수신측의 정보보호 필터 부분, 인증서 관리국에서 수행하는 인증서 관리및 분배, 내용증명에 필요한 프로그램 모듈로 나눌 수 있다.

송신측의 메일 클라이언트는 메시지의 생성 및 저장 기능을 수행할 수 있는 부분과 메일 전송 부분, 정보보호 부분으로 구성된다. 사용자 인터페이스와 메시지의 생성, 저장하는 부분은 Motif를 사용하여 구현하였으며, 메일 전송 부분은 TCP 포트 25번을 바인딩(binding)하여 데이터를 전송하였다.

본 메일 시스템의 인증서 관리국 서버 프로그램은 SUN Sparc 20에서 실행하였으며, 송신측 메일 클라이언트 프로그램도 SUN상에서 실행하였다.

송신측에서 수신측의 인증서가 필요할 경우에는 인증서 관리국에게 수신측의 메일 주소를 전달하여 수신측의 인증서를 전달받고 있으며, 인증서 관리국으로부터 수신한 인증서는 송신자의 홈 디렉토리에 .Recipient.Certificate 화일로 저장된다. 또한 사용자에게 융통성있는 서비스를 제공하기 위해서 4가지 형태의 메시지 형태로 메일을 전송할 수 있도록 하였으며, 제공하고 있는 메시지 형태는 다음과 같다.

(1) ENCRYPTED : 메시지를 암호화하고, 디지털 서명을 수행한 메시지 형태이다.

(2) MESSAGE-ENCRYPTED-ONLY : 디지털 서명은 수행하지 않고 메시지만을 암호화한 메시지 형태이다.

(3) MIC-ONLY : 메시지는 암호화하지 않고 디지털 서명만을 수행한 메시지 형태이다.

(4) PLAIN : 기존의 인터넷 메일 메시지와 동일한 메시지 형태이다.

그림 9는 메일을 전송하는 것으로 다이얼로그 박스의 토글 버튼의 조합에 따라 사용자가 융통성있게 메시지 형태를 정하여 수신측에 전송할 수 있다.

그림 10은 수신측에서 ENCRYPTED 형태의 메시지를 수신한 것이다. 메시지 형식은 메시지를 암호화하거나 디지털 서명을 수행할 때 사용한 알고리즘과 해당 정보를 명시하고 있다. 수신측에서 수신한 데이터 형식은 첫부분은 SMTP를 사용하였기 때문에 기존의 메일의 헤더와 동일하다. 다음은 본 메일 시스템에서의 메시지 시작을 나타내는 필드이다. Proc-Type 필드는 메시지의 형태를 나타내는 필드이다. Content-Domain 필드는 SMTP를 사용하는 메일 메시지 형태를 명시하는 필드이다. DEK-Info(Data Encryption Key Information) 필드는 메시지를 암호화하는데 사용된 알고리즘을 명시하는데, 본 논문에서는 DES-CBC 모드 알고리즘을 사용하였기 때문에 초기화 벡터에 대한 정보를 또한 명시하였다. MIC-Info(Message Integrity Code Information) 필드는 송신측에서 메시지에 대한 디지털 서명을 수행한 서명 정보와 사용한 알고리즘을 명시하는 필드이다. Key-Info 필드에는 메시지를 암호화할 때 사용한 세션 DES 키를 수신자의 공개키로 암호화한 정보가 있으며, 다음에 나오는 필드는 송신자가 수신자에게 전송하는 메시지를 DES-CBC 모드 알고리즘으로 암호화한 데이터 부분이다. MESSAGE-ENCRYPTED-ONLY 메시지 형태는 메시지만을 암호화하여 전송하기 때문에 MIC-Info 필드가 필요없다.

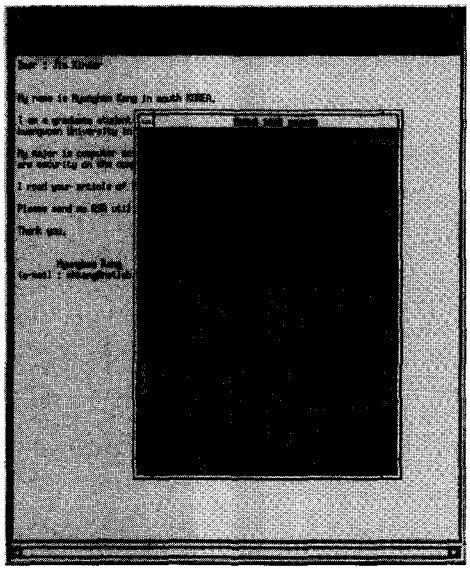


그림 9. 메시지 전송

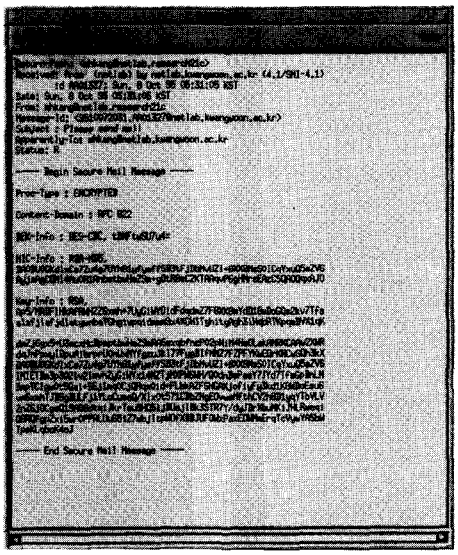


그림 10. 수신한 메시지

따라서, MESSAGE-ENCRYPTED-ONLY 형태는 Proc-Type 필드, Content-Domain 필드, DEK-Info 필드, Key-Info 필드, 암호화된 메시지 필드로 구성된다. MIC-ONLY 메시지 형태는 메시지는 암호화하지 않고 디지털 서명만을 수행하기 때문에 DEK-Info 필드, Key-Info 필드가 없다.

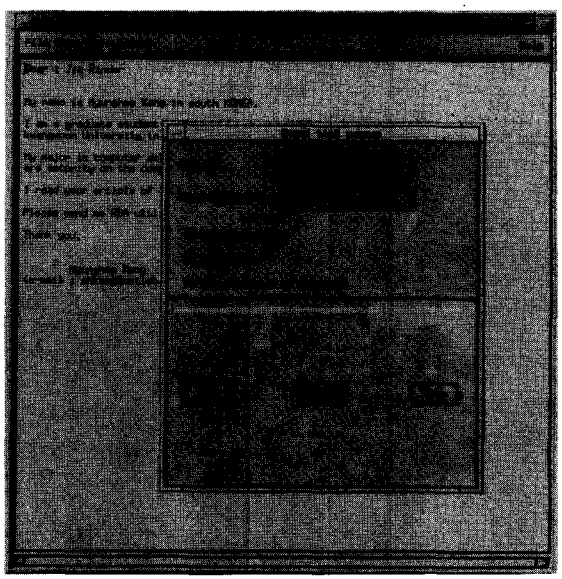


그림 11. 내용 증명을 위한 데이터 전송

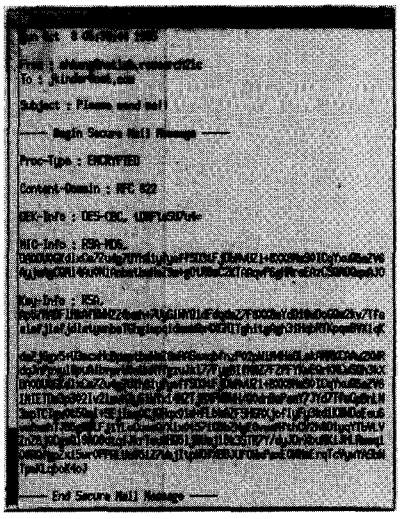


그림 12. 인증서 관리국에서 수신한 데이터

그림 11은 송신측에서 인증서 관리국에 내용증명을 위해서 데이터를 전송하는것으로 ENCRYPTED 형태의 데이터를 전송하는 것이다.

그림 12는 송신측에서 내용 증명을 위해 인증서 관리국에 전송한 데이터이다. 인증서 관리국에서 송신측으로부터 수신한 데이터에는 SMTP 메시지 헤더는 없고 대신에 송신측에서 인증서 관리국에 데이터를 전송한 날짜와 시간, 송신자와 수신자의 주소가 명시되어 있다. 전송한 날짜와 시간, 송·수신자의 주소는 분쟁 발생시에 내용증명을 수행하여 분쟁을 해결하기 위한 것이다.

## 5. 결 론

본 논문에서 구현한 메일 시스템은 인터넷의 메일 시스템을 대상으로 하여 정보보호 서비스를 구현함으로써, 기존의 인터넷 메일 시스템에서의 정보보호에 대한 취약성을 보완하였다. 구현된 메일 시스템에서는 기존의 PEM이나 PGP에서 제공하고 있는 메시지 기밀성, 메시지 무결성, 송신자 신분 인증, 송신 부인봉쇄 등의 정보보호 서비스를 제공할 뿐만 아니라, 아직까지 PEM이나 PGP에서는 제공하고 있지 못한 메시지 재전송 방지, 내용증명을 통한 수신 부인 봉쇄 서비스를 제공한다. 또한 본 논문에서는 디지털 서명 생성시 서명 블록을 생성하여 서명을 수행함으로써, 디지털 서명에 있어 보다 안전성을 높였으며, 또한 암호화 블록을 생성하여 암호화 키를 암호화함으로써, 암호화 키에 대한 안전성을 높였다. 그리고 제공하는 정보보호 서비스의 유형에 따라 다양한 메시지 형태로 전송할 수 있어 사용자에게 융통성 있게 정보보호 서비스를 제공할 수 있다.

## 참 고 문 헌


[1] D. Balenson, Privacy Enhancement for Internet Electronic Mail, Part III : Algorithms, Modes, and Identifiers, Request for Comments (RFC) 1423, Internet Activities Board, 1993.

[2] Mihir Bellare and Phillip Rogaway, The Exact Security of Digital Signatures - How to Sign with RSA and Rabin, Advances in Cryptology - Eurocrypt 96 Proceedings, LNCS 1070, Ueli Maurer ed, Springer-Verlag Berlin Heidelberg 1996.

[3] Mihir Bellare and Phillip Rogaway, Optimal Asymmetric Encryption, Advances in Cryptology - Eurocrypt 94 Proceedings, LNCS 950, A. De Santis ed., Springer-Verlag, 1994.

[4] Warwick Ford, Computer Communications Security : Principles, Standard Protocols and Techniques, pp. 325-376, Prentice Hall, 1994.

[5] IEEEP1363 Working Draft, Standard of RSA, Diffie-Hellman and related public-key cryptography, 1996

[6] B. Kaliski, Privacy Enhancement for Internet Electronic Mail, Part IV : Key Certification and Related Services, Request for Comments (RFC) 1424, Internet Activities Board, 1993.

[7] Kaufman, Perlman, and Speciner, Network Security : Private Communication in a PUBLIC World, pp. 329-397, Prentice Hall, 1995.

[8] Stephen T. Kent, Internet Privacy Enhanced Mail, Communications of the ACM, Vol. 36, No. 8, pp. 48-60, Aug. 1993.

[9] S. Kent, Privacy Enhancement for Internet Electronic Mail, Part II : Certificate-Based Key Management, Request for Comments (RFC) 1422, Internet Activities Board, 1993.

[10] J. Linn, Privacy Enhancement for Internet Electronic Mail, Part I : Message Encryption and Authentication Procedures, Request for Comments (RFC) 1421, Internet Activities Board, 1993.

[11] Master Card and Visa, Secure Electronic Transactions, Feb 23. 1996.

[12] J.B. Postel, Simple Mail Transfer Protocol, Request for Comments (RFC)

821, Internet Activities Board, Aug. 1982.

[13] RSA Laboratories, 'PKCS #1 : RSA Encryption Standard, Version 1.1, Nov. 1993.

[14] RSA Laboratories, PKCS #5 : Password-Based Encryption Standard, Version 1.1, Nov. 1993.

[15] R. Rivest, The MD5 Message-Digest Algorithm, Request for Comments (RFC) 1321, Internet Activities Board, Apr. 1992.

[16] William Stallings, Network and Internetwork Security : Principle and Practice, pp. 102-103, pp. 360-411, Prentice Hall, 1995.

## □ 著者紹介

강 명 희(康 明 熙)

1994년 2월 : 광운대학교 수학과 졸업(이학사)
1996년 2월 : 광운대학교 대학원 전자계산학과 졸업 (이학석사)
1996년 2월 - 현재 : 백두정보기술/주, EP&C팀

※ 관심분야 : 네트워크 보안, 전자상거래, 스마트 카드 등

신 효 영(申 孝 泳)

1986년 2월 : 광운대학교 이과대학 전자계산학과(이학사)
1988년 2월 : 광운대학교 대학원 전자계산학과(이학석사)
1996년 2월 : 광운대학교 대학원 전자계산학과 박사과정 수료
1988년~1993년 : LG 소프트웨어(주)
1994년~현재 : 경성전문대학 사무자동화과 전임강사

※ 관심분야 : 컴퓨터네트워크, 컴퓨터통신 정보보호, 멀티미디어 통신

유 황 빈(柳 惶 彬)

1975년 2월 : 인하대학교 전자공학과 (공학사)
1977년 7월 : 연세대학교 산업대학원 전기전자공학과(공학석사)
1989년 2월 : 경희대학교 전자공학과 (공학박사)
1994년 2월-1995년 2월 : University of California at SanDiego 교환교수
1981년-현재 : 광운대학교 전자계산학과 교수
1995년-현재 : 광운대학교 신기술 연구소 연구원

※ 관심분야 : ATM, B-ISDN, 네트워크 보안, 멀티미디어 네트워크