ECC 암호시스템을 활용한 강력한 암호시스템의 구축 및 사례연구

최병선, 황영철, 이원구, 이재광
한남대학교 컴퓨터공학과

Study on Research of Secure Crypto System Using a ECC Crypto System

Byoung-Son Choi, Young-Chul Hwang, Won-Goo Lee, Jae-Kwang Lee
Dept. of Computer Engineering, Hannam University

요 약

인터넷은 전 세계를 연결하는 매체로서, 그 사용자가 매년 폭발적으로 증가하고 있다. 이러한 인터넷 사용자간의 자료 교환 수단으로서 전자우편은 표준이라 말할 수 있을 만큼 많이 사용되고 있다. 일반 편지에서부터 상업광고 목적의 전자우편에 이르기까지 다양한 분야에서 사용되고 있다. 하지만 이러한 전자우편에도 많은 문제가 존재한다. 기존의 전자우편은 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 전자우편 시스템의 개발이 시급하다. 본 논문에서는 기본적인 정보보호 서비스 외에 기존의 전자우편 시스템에서는 제공되지 않는 배달 증명 및 내용 증명 기능을 제공하고 자바 암호 API를 사용하여 안전한 키 교환이 가능하도록 하였다.

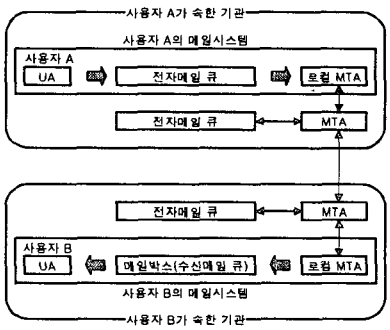
1. 서론

인터넷은 전 세계를 연결하는 매체로서 그 사용자가 매년 폭발적으로 증가하고 있다. 인터넷을 사용하는 사용자들 간의 의사 교환수단으로서 전자메일은 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 전자메일을 이용하여 상호 교환되지 못하고 있다. 그 이유는 전자메일이 가지는 보안적인 문제점 때문이다. 첫째는 전자메일 양식상의 문제점이고, 둘째는 프로토콜 상의 문제점이다. 본 논문에서 구현한 전자메일은 공개키 암호화 방식을 이용하여 이러한 문제점을 해결하였다.[1]

2. 전자 메일 시스템

2.1 전자 메일 시스템의 구조

전자메일 시스템은 [그림 1]과 같이 여러 개의 UA(User Agent)와 MTA(Mail Transfer Agent) 등으로 구성되며, 사용자 A가 사용자 B에게 메일을 전송하려 한다면 다음과 같은 과정을 거치게 된다[2].



[그림 1] 기존의 전자메일 시스템

2.2 정보보호 서비스

2.2.1 내용 기밀성 (Content Confidentiality)

기밀성은 권한이 없는 사용자들에게 메시지가 노출되어지는 것을 막는 것을 의미한다.

2.2.2 내용 무결성 (Content Integrity)

* 본 연구는 한국과학재단 지역협력연구센터(R12-2003-02004-0) 지원으로 수행되었음

메시지 스트림을 대상으로 하는 연결형 무결성 서비스는 메시지가 원래 송신된 대로 즉, 복사, 추가, 수정, 순서변경 또는 재 전송되지 않고 수신됐음을 확인한다.

2.2.3 발신자 인증(Message Origin Authentication)

발신자 인증은 통신이 신뢰성을 갖도록 보증한다. 발신자 인증 서비스는 메시지가 자기라고 주장하는 실체의 출처로부터 전송되었음을 수신자에게 확인시키는 서비스이다.

2.2.4 부인방지(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)

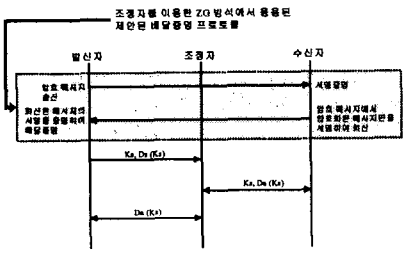
메시지를 송신한 후에, 송신자가 실제로 수신자에 의해서 이 메시지가 수신됐었다는 것을 확인할 수 있게 한다. 이러한 수신 부인방지 서비스의 예로는 배달 증명과 내용 증명 서비스가 있다. [4,5]

3. 부인방지 서비스

3.1 배달 증명 서비스

3.1.1 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 ZG(Zhou and Gollmann) 방식[3]을 응용하여 배달 증명 서비스를 제공하는 프로토콜을 수용하였다. [그림 2]는 조정자를 이용한 ZG 방식을 응용하여 제안한 배달 증명 프로토콜을 기술하고 있다.

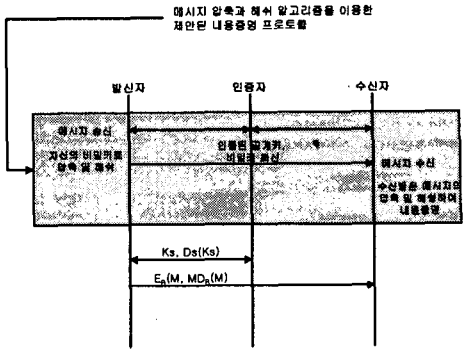


[그림 2] 제안된 배달증명 프로토콜

3.2 내용 증명 서비스

3.2.1 제안된 방식

내용 증명 서비스를 제공하기 위해, 메시지 압축과 해쉬를 이용함으로서, 수신자가 발신자로부터 온 메시지가 변경되지 않았다는 것에 대해 신뢰할 수 있게 된다. 아래 [그림 3]에서는 이러한 내용 증명 서비스를 제공하기 위한 전체적인 프로토콜을 보여준다.

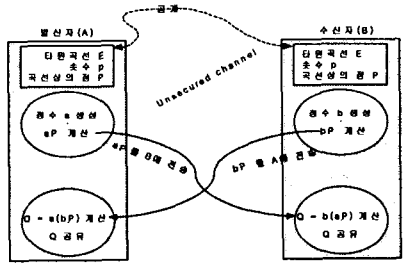


[그림 3] 제안된 내용증명 프로토콜

4. 안전한 전자 메일 시스템의 설계

4.1 안전한 키교환 모델

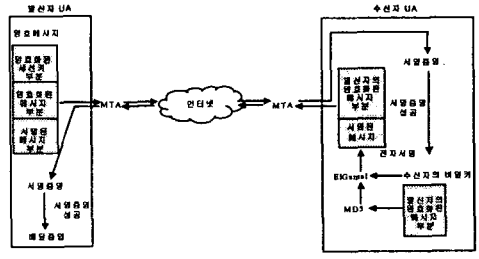
발신자와 수신자가 안전하게 메일을 주고받기 전에, 반드시 상호 키 교환이 필요하게 된다. 본 논문에서는 이러한 안전하게 키 교환을 하기 위해 ECDH(Elliptic Curve Diffie-Hellman) 알고리즘을 이용한 키 교환 모델을 구현하였다. 이러한 키 교환 과정을 구현한 모델은 다음의 [그림 4]와 같다.[6]



[그림 4] ECDH 알고리즘을 이용한 키 교환 모델

4.2 안전한 배달증명 모델

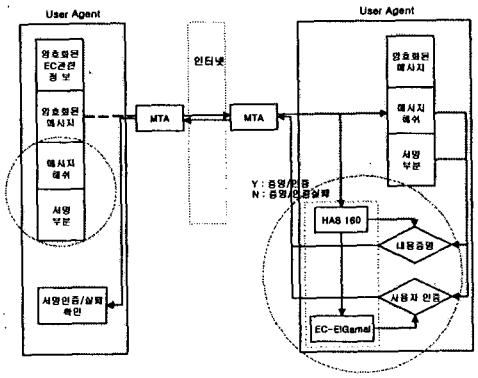
아래 [그림 5]는 앞에서 제안된 배달증명 방식을 기반으로 한 배달증명 모델을 통해서 의도된 수신자가 올바르게 메일 메시지를 수신하였음을 확인하는 과정을 보여주고 있다.



[그림 5] 배달증명 모델

4.3 안전한 내용증명 모델

앞에서 제안된 내용 증명 방식을 기반으로 한 내용 증명 모델을 통해서 수신자는 발신자가 보낸 메시지가 변조되지 않고 전달되었다는 것을 확인하는 과정이 [그림 6]에 보여지고 있다.



[그림 6] 암호화 알고리즘을 이용한 배달 증명 모델

4.4 안전한 암호화 모델

4.4.1 암호화 알고리즘

(1) 메시지 암호화 알고리즘 : SEED 알고리즘

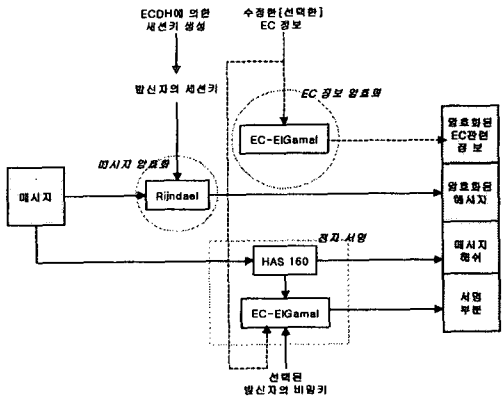
SEED 알고리즘은 널리 사용되는 관용 암호 알고리즘이며, 데이터를 128비트 키를 이용한다. 관용 암호 알고리즘이기 때문에 암호화와 복호화에 사용되는 키가 하나이고 속도가 빠르다.

(2) 전자 서명 알고리즘 : EDCSA(Elliptic Curve Digital Signature Algorithm) 알고리즘

ECDSA는 DSA를 타원곡선으로 변형시킨 것이다. ECDSA와 DSA의 중요 차이점은 r의 생성에 있다. DSA는 r을 임의의 $g^k \bmod p$를 선택/계산한 후, $\bmod q$를 계산하여 얻는다. 그러나 ECDSA에서 r은 임의의 점 kP의 x 좌표를 $\bmod n$하여 얻는다. ECDSA가 160비트 q와 1024비트 p를 가진 DSA와 비슷한 안전도를 갖기 위해서는 매개변수 n이 약 160비트이면 된다. 이 경우 DSA와 ECDSA는 같은 서명길이(320비트)를 갖는다.

4.4.2 메시지 암호화 모델

발신자가 메시지를 암호화하여 생성하는 암호 메시지는 암호화된 세션키 부분, 암호화된 메시지 부분, 그리고 서명 부분으로 구성된다. [그림 7]은 다음에 기술한 메시지 암호화 과정을 거쳐 암호 메시지를 생성하는 과정에 대해 보여주며, 설계에 대한 구현 코드를 기술한다.



[그림 7] Rijndael 알고리즘을 이용한 메시지 암호화 모델

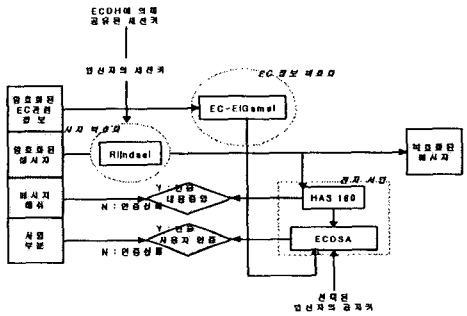
① 메시지를 Rijndael 알고리즘을 사용해서 발신자의 세션키로 메시지를 암호화한다. 그리고 이탤릭체와 함께 진하게 강조된 글자는 사용된 알고리즘을 보여주고 있다.

② 메시지 암호화에 사용된 Rijndael 세션키(선택된 EC 정보)를 EC-ElGamal 알고리즘을 사용해서 암호화한다.

③ HAS160 알고리즘을 사용해서 메시지 다이제스트를 생성하고, 이 메시지 다이제스트를 ElGamal 알고리즘으로 암호화하여 전자 서명을 생성한다.

4.4.3 메시지 복호화

수신된 암호 메시지는 메시지의 각 부분별로 복호화 및 서명을 증명하는데, [그림 8]은 이러한 과정을 보여주고 있다.



[그림 8] Rijndael 알고리즘을 이용한 복호화 모델

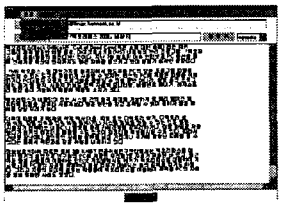
① EC-ElGamal 알고리즘을 사용해서 Rijndael 세션키(선택된 EC 정보)를 복호화한다.

② Rijndael 알고리즘을 사용해서 복원된 Rijndael 세션키(선택된 EC 정보를 가지고 암호문을 복호화 한다.

③ 복원된 평문 메시지를 HAS160 알고리즘을 사용해서 메시지 다이제스트로 변환하고, ECDSA[EC ElGamal] 알고리즘을 사용해서 전자 서명을 증명하게 된다.

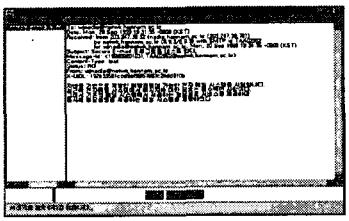
5. 암호 메일 테스팅

5.1 메시지 작성 및 송신 테스팅



[그림 9] 메시지 작성

[그림 9]에서는 메시지 작성 윈도우의 메뉴 바에서 '보안 기능 사용' 메뉴와 '배달 증명 사용', 그리고 '내용 증명 사용' 메뉴를 선택하여 기본 보안 기능과 배달증명 서비스, 그리고 내용증명 서비스를 제공받을 수 있도록 설정하였다.



[그림 10] 메시지 암호화 및 서명

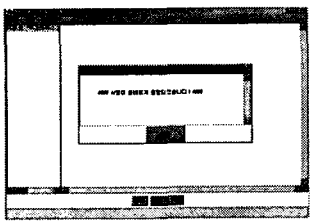
[그림 11]은 메시지 암호화 및 서명을 통해서 생성된 암호 메시지 자체를 출력한 것으로 배달 증명을 요청하기 위해서 "Certification of Repudiation" 태그를 암호 메시지의 맨 처음에 첨부하였다.

Certification of Repudiation:bAd3am5hZssJG+j
lkklJJUAAgxuZrsq5+dATONIEZxAiqudx7ppYs+7
4RARd9H8L6rmjPTuyaDMpm+SOE+pLUI4+BNK
2FfwawgzcjdgWGGrrdBvN7lz18yDhazbTIYsdvA
0MtRxsnB5y7dojkuKVQf8R09327yVGW4VAAP/3
pIPgYXxJuYLAAAAgFur8S7UYEW7aU5qh556yj
wvHSmZUiZ3Yxyg2ZNRf9VKR6lz22ZBDJAVmE
HNNr9L+CYFRgKIm/yxfycwC ……

[그림 11] 암호화된 메시지

5.2 메시지 수신 및 서명 증명

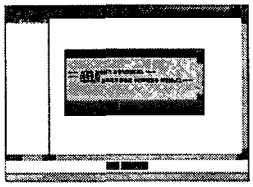
메시지를 수신한 수신자의 메일 프로그램은 배달 증명과 내용 증명을 요구하는 메시지임을 메시지 내의 플래그를 인지하여 확인하고, 서명을 증명하여 [그림 12]와 같이 서명이 올바르게 증명되었음을 다이얼로그 박스에 출력한다.



[그림 12] 수신된 메시지의 서명 증명

5.3 메시지 회신 및 부인방지

회신 메시지를 수신한 발신자는 메시지에 붙어있는 두 플래그가 배달 증명과 내용 증명에 대한 회신 메시지를 나타냄을 확인한다. 그리고 수신된 메시지의 서명을 증명하여 배달증명과 내용 증명이 확인되었음을 나타내는 다이얼로그 박스를 [그림 13]과 같이 출력한다.



[그림 13] 회신된 메시지의 배달증명

6. 결론

현재 네트워크 환경에서 널리 사용되고 있는 전자메일 시스템은 많은 보안상의 취약점에 노출되어 있다. 이러한 전자메일의 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 배달증명 서비스와 내용이 변경되지 않았음을 증명하는 내용증명 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 부인방지 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.

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] Scott Oaks, "Java Security", O' REILLY, 1998