論 文

공개키 암호방식을 이용한 화일전송 모델의 연구

正會員 崔 鎭 卓* 正會員 宋 榮 宰**

A Study of Model on File Transfer Using Public-key Cryptography

Jin Tag CHOI* Young Jae SONG** *Regular Members*

要 約 본 논문은 화일전송 시스템에서 데이타 보호방법에 대하여 연구 하였다. 기존의 화일전송 시스템에서는 보호기법으로 시스템 사용 권한통제(password) 및 화일 접근통제방법(ACL)이 사용되고 있지만 데이타 자체 보호는 하지 못하고 다만 허가되지않은자의 접근을 통제하여 준다. 이러한 보호기법을 컴퓨터 침입자로 하여금 많은 위협을 받고있다. 제안된 시스템 구성은 높은 수준의 비밀유지보호(데이타 자체보호, 송신자 인증 등)를 위하여 화일전송에서 공개키 방법중 RSA 암호방식을 사용하여 최상의 비밀유지를 이룩할 수 있고 또한 이방법을 데이타 베이스에서 처럼 여러가지 문서취급에 쉽게 적용할 수 있는 새로운 대체 시스템에 대하여 연구 하였다.

ABSTRACT This paper is concerned with the file protection in the file transfer systems. In the existing file transfer systems, passwords are used in the protection but do not provide any data protection and can only provide some protection against unauthorized access. Even provided with this protection, we cannot be free form computer hackers. In order to achieve higher standards of protection for our privacy (protection for data themselves, authentication of senders…) analternative technical system should be developed in using of public key cryptography by choosing the public key method(RSA public key) in the file transfer. A new system suggested in the paper can achieve some higher standards of protection for our privacy. We a result this system will be easily applied to various document handling systems as in the data base.

Ⅰ. 서 론

현대사회가 정보화 사회로 변환되어 가고 있고 또한 많은양의 정보를 생산, 사용하고 있어 정보를 보호하기위한 방법으로 암호화 시스템에 대하여 많은 연구를 하고있다.[1-8] 정보통신의 고도화와 다양화로 인하여 과거 집중처리 방식에서는 별로 문제가 되지않았던 자료의 보호가 컴퓨터를 이용한 정보의 처리및 사용에 있어 편리해진 반면에 자료의 노출이 상대적으로 심하여져 비밀을 요하는 자료의 전송과정에서 보안문제가 매우 중요한 필수적인 문제로 부각되고 있다.[2] 정보의 전달과정에 있어서 여러가지 방법으로 상대방에

*仁川大學校 電子計算學科
Dept. of Computer Science, Incheon Univ.
**慶熙大學校 電子計算工學科
Dept. of Electronic Engineering, Kyunghee University.
論文番號 : 90-56(接受1990. 2. 15)

게 전달되는데 일반적으로 평문으로 전달되기도 하지만 자료의 보호가 요구되는 비밀사항의 메시지나 화일은 암호화 방법으로 전달이 되어지고 있다.[6] 정보의 전달수단이 손으로쓴 편지에 의하여 상대방에게 전달되던 시대의 암호알고리즘은 문자대치 알고리즘이나 위치교환 알고리즘이 주로 사용되었다. 컴퓨터의 발달로 모든 정보의 전달방법은 컴퓨터시스템의 데이타통신망을 통하여 정확하고 신속하게 전달되어지고 있다. 이러한 컴퓨터 시스템들이 데이타 통신망을 통하여 정보를 교환할때 처리및 송수신되는 과정에서 예기치않은 외부 침입자로 하여금 여러가지 수단에의하여 도청, 재수신, 위조전문의 삽입 등 컴퓨터의 보안에 위협을 받고있기 때문에 데이타의 보안을 요구하는 화일전송시 일반적인 암호체계가 갖고있는 제문제를 해결할 수 있는 새로운 암호 화일 전송 시스템이 요구된다.[9] 정보보호란 정보시스템 혹은 통신시스템내에 각종자료나 화일 및 소프트웨어 등과 같은 고가의 정보를 제삼자의 침해로부터 보호하는것을 말하며 또한 전달과정에서도 보호되어야 한다.

현재 컴퓨터네트워크를 이용한 화일전송 시스템에서는 일반적으로 터미널끼리 서로 평문으로 화일을 교환하고 있다. 정보전송에 있어서 외부의 침입을 막기위한 일반적인 보호정책으로 정보자체의 접근을 통제하는 접근제어 방법이 있는데 이는 사용자의 신원 또는 공유자원의 특성을 고려해서 암호(password)를 사용하여 허가되지 않은 사용자로 하여금 접근을 통제하는 방법이다.[3 11] 이 방법은 사용자의 암호(password)가 단순하기 때문에 침입자에 의해 침해될 우려가 있다. 일단 침해당하면 데이타는 원시화일 그대로 공개될 수 있어 데이타의 소멸, 파괴, 변조, 허위문서전송 등의 침해가 우려되며 그래서 자원자체의 사용이나 접근을 통제하는것 외에 데이타 내용 자체를 암호화하여 허락된 사용자만이 그내용의 진의를 파악할 수 있으며 허락되지않은 침입의 경우에도 비밀의 데이타가 보호될 수 있는 방법으로 내용을 암호화하는 Cryptography가 등장하였다.[1] 여기에는 여러가지 방법으로 내용을 암호화하여 (Encryption) 전송하면 특정한 권리를 부여 받은자만이 내용을 해독(Decryption) 할 수 있다.

본 논문에서는 종래의 화일전송 시스템에서는 비밀을 요하는 사항의 화일을 전송하거나 보관하는데있어서 화일 자체를 보호하기 어려우며 또한 전송과정에서 도청, 위조전문 삽입등의 침해가 우려되었다. 따라서 이러한 단점을 보완하기 위하여 공개키를 이용한 방법으로 화일전송 시스템서비스에서 사용자의 모든 공개키를 관리하며 화일전송 시스템 서비스와 가입자간에 두개의 공개키와 비밀키를 이용 상대방을 인증한 상태에서 워크 스테이션(work station)을 이용하여 내용을 암호화하여 전송하며 수신측에서 해독역시 워크스테이션에서 공개키와 개인비밀키를 이용하여 해독하고 처리되므로 전송 과정에서의 도청, 변조, 허위문서 삽입 등의 침해를 방지할 수 있다. 제안된 시스템 설계에서는 공개키 암호방법중 RSA 암호방식을 응용 적용하여 데이타 자체보호는 물론 종래 방법에서 확인하기 곤란한 인증, 디지탈 서명, 비밀유지 등을 해결할 수 있는 새로운 시스템을 제시하였다. 또한 응용으로 비밀정보나 데이타 베이스 화일에서 특정 데이타를 보호하는데도 쉽게 적용할 수 있다.

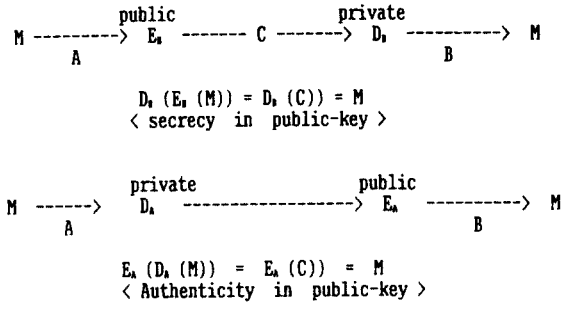
Ⅱ. 공개키 암호시스템

Ⅱ.1 기본개념과 인증

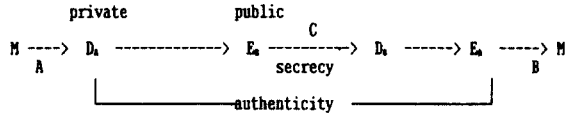
모든통신에서 상대방을 확인하는 인증문제가 매우 중요하다. 서류를 매체로 직접적인서명 인장의 날인 지문의 수단으로 인증하는 방법이 통신시스템에서는 다른형태로 구현되어져야 한다. 공개키 암호방식이 인증방법을 구체적으로 실현 시킨다. 공개키 암호방법에서 대표적인 RSA방법의 기본개념과 인증 방법은 다음과 같다.[6 12]

공개키의 개념은 1976년 Diffie와 Hellman에 의해 소개되었다. 어떤 통신시스템의 두가입자를 A와 B로 나타내면 가입자 A는 공개키(E_A)와

개인의 키(D_A) 두개를 가지고있다. 공개키 시스템 가입자 A는 공용 디렉토리에서 암호화 과정 E_A는 공개키 이고 해독화 과정 D_A는 개인 비밀키 이다.[1] 공개키 시스템에서 가입자 A가 가입자 B에게 메시지를 전달한다고 하면 A는 B의 공개키 E_B를 알고 있어야 한다. 그래서 가입자 A는 메시지 M을 암호화 ($E_B(M)$)해서 암호문 C를 가입자 B에게 보낸다.[5 6]



위에서는 한사람의 키를 사용해서 메시지를 전달하였지만 다음은 두사람의 키를 이용하여 가입자A가 메시지 M을 B에게 보내기를 원한다면 가입자 A는 암호화하여 $E_B(D_A(M))=C$를 사용자 B에게 보낸다. 가입자 B는 받아서 해독하면 $E_A(D_B(C))=E_A(D_B(E_B(D_A(M))))=M$이 된다.[10]



Ⅱ.2 지수를 이용한 효과적인 RSA 암호방식

Pohlig과 Hellman이 1978년 지수계산을 기초로 한 암호작성법을 발표하였고 같은 시기에 R. Rivest, A. Shamir과 L. Adleman에 의해서 고안된 RSA 암호방식은 정보 데이타를 정수로 나타내고 이들 정수를 멱승하여 다른 정수로 암호화 하는 방법을 말한다.[4]

$C=M^e \bmod n$

(e와 n은 암호화하는 키 이다)

M은 다시 C에다 평문화 하는 다른 키 d를 지수연산에 사용하여 만든다.

$M=C^d \bmod n$

(d와 n은 복호하 하는 키이다.)

RSA 암호방식에서 (e,n)은 공개하여 공용할 수 있도록 하고 (d,n)은 비밀로 한다. n은 p와 q의 곱이고 p,q는 솟수(prime number)이다.
정해진 (e,n)에 대한 복호화키 (d,n)의 d는 e의 역수 $d=e^{-1} \bmod \phi(n)$으로 구한다. $\phi(n)=\phi(p)\ \phi(q)=(p-1)(q-1)$
그러나 (e,n)을 알고 d를 구하기는 매우 어렵다. $\phi(n)$을 알아야 하는데 n을 소인수 분해하여 p와 q를 알아야 하는것과 같다. n의 자리가 200개 이상이면 암호분석이 현실적으로 수행될 수 없는것으로 되어있다. 이를 해독하기 위해서는 성능이 우수한 컴퓨터로 수천만년이 걸리게 되기 때문이다. 지수계산을 빠른방법으로 하기위하여 fastexp라는 알고리즘을 사용한다.

C=fastexp(M,e,n)
M=fastexp(C,d,n)

암복호화를 함께 하면

$(M^e \bmod n)^d \bmod n = M$
$M^{de} \bmod n = M$

이러한 대칭때문에 RSA 암호방식은 공개키 조직에서 가장 대표적이며 p,q의 길이에 따라서 일반적인 암호화 방법에 비하여 시스템의 안전성이 매우높고 비밀을 유지할 수 있는 암호화 방법이다.

Ⅲ. 확장된 화일전송 시스템설계

컴퓨터와 단말기들이 지역적으로 분산되어 있어서 컴퓨터 통신망은 크게 컴퓨터 시스템, 데이타 통신 시스템으로 구분할 수 있다. 여기서 컴퓨터통신망의 특징은 같은 설비를 여러사람이 공통으로 사용하고 많은사람이 손쉽게 사용하도록 구성되어야 한다. 이러한 사용자의 장점은 보안의 측면에서는 큰 부담이 아닐수 없다. 특히 화일전송 시스템에서 사용자간의 데이타나 화일 전송에 있어서 정당성 여부, 자료의 불법적 사용, 데이타의 불법적 액세스변경및 합법적 활동의 도용 등을 방지할 수 있는 시스템이 설계되어야 한다. 일반적 전송 방법은 안전장치가 되어 있지않은 통신로를 통하여 평문 그대로 전송되며 또한 컴퓨터 소유자의 입장에서도 관할밖의 영역이기 때문에 취약부분으로 문제시되고 있는 실정이다. 그래서 컴퓨터 시스템에 수록되어 있거나 화일전송 시스템을 통하여 전달되고있는 데이타에 대하여 여러가지 위협에 대처할 수 있는 방법으로 제안된 모델은 공개키 암호방식을 이용하여 화일전송 시스템 서비스 패키지 제어하에 키의 전송이 이루어지고 보호해야할 화일은 일반 통신선로를 통하여 암호화하여 전송된다. 전송과정에서 보안의 문제점을 없게하기 위하여 암호해독의 처리를 화일전송 시스템 서비스에서 하지않고 각자 워크 스테이션을 사용하여 처리하는것으로 설계하여 비밀을 요하는 데이타나 화일을 보다 안전하게 전달할 수 있는 암호통신 시스템을 설계 하였다. 기본적인 개념은 그림 3-1과 같다.

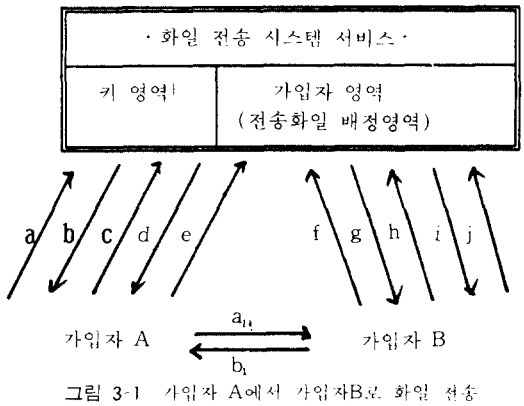


그림 3-1 가입자 A에서 가입자B로 화일 전송

a. 암호(password)로 패키지 주컴퓨터에 연결
b. 컴퓨터 공개키를 가입자 A에 전송
c. 송신자, 수신자명을 암호화 하여 전송
d. 확인후 필요한키 전송
e. (송신자+time stamp+비밀화일)을 암호화하여 전송
a1. 직접통로를 통하여 (송신자, timestamp, file length)를 암호화하여 전송
f. 암호(password)로 패키지 주 컴퓨터에 연결
g. 컴퓨터 공개키를 B에 전송
h. 고유명(수신자명)을 암호화 하여 전송
i. 확인후 도착 화일이 있으면 필요한 키와 함께 화일 전송
j. 해독한 화일 time stamp와 a1을 통한 time stamp 비교 같으면 확인응답 보고
b1. 틀리면 재송신요청

Ⅲ.1 가입자 A에서 가입자 B로 비밀의 화일 전송시 작업순서

1) 용어 정의

S:송신 R:수신 M:화일 C:암호문
GA:가입자 E:암호화 D:해독화 e:공개키 d:비밀키 A,B:가입자명 H:패키지가있는 주 컴퓨터
DL:data length T:time stamp

2) 가입자 A의 처리순서 (송신자)

① 일반적인 방법으로 암호(password)나 전화번호를 이용 패키지 주 컴퓨터와 네트워크 연결

② · 화일전송 시스템 서비스 패키지(package) 개방
· 개방과 동시 화일전송 시스템 서비스 공개키($e_{H,n}$)를 전송 받는다.

③ · 송수신자 고유명을 개인 비밀키와 화일전송 시스템 서비스 공개키로 암호화하여 화일전송 시스템 서비스가 있는 컴퓨터로 보낸다.

$S_A=E_H(D_A(GA_A))$

$R_B=E_H(D_A(GA_B))$

· S_A, R_B를 화일전송 시스템 서비스 컴퓨터에 전송하며 여기서 D_A는 디지탈 서명에 해당

④ 화일전송 시스템 서비스는 비밀키를 이용하여 A,B 가입자명 확인, 즉 인증후 배정

영역 확보

⑤ 암호화에 필요한 키(e_B, n)를 전송 받음

⑥ 전송받은 키를 이용 송신자, timestamp, 화일을 암호화하여 함께 화일전송 시스템 서비스에 전송

$C=E_B(D_A(GA_A+T+M))$

⑦ 화일전송 시스템 서비스는 받은 C를 가입자B 배정영역에 저장하게 된다.(GA_A 첨가:발신자 확인)

3) 가입자B 처리순서 (수신자)

① 일반적인 방법으로 암호(password)나 전호번호를 이용패키지 주 컴퓨터와 네트워크 연결

② 화일전송 시스템 서비스 패키지(package) 개방

· 개방과 동시 화일전송 시스템 서비스 공개키(e_H, n)를 전송 받는다.

③ 수신신청을 위하여 화일전송 시스템 서비스 공개키와 개인비밀키로 자신의 가입자명(수신자명)을 암호화하여 화일전송 시스템 서비스에 전송

$R_B=E_H(D_B(GA_B))$

④ 화일전송 시스템 서비스는 비밀키를 이용하여 해독하고 가입자를 인증후 도착비문화일이 있으면 가입자 A의 공개키와 비문을 전송한다. (e_A, n)와 C를 B에 전송

⑤ 가입자 B는 받은키를 이용 해독하여 수신된 화일을 확인

$GA_A+T+M=E_A(D_B(C))$

⑥ 직접 통로를 통하여온 송신자, time stamp, file length를 ⑤에서 해독한것과 비교하여 이상 없으면 확인응답 보고한다.

⑦ 비교하여 이상이 있으면 GA_A에 재송신 요청한다.

4) 화일전송 시스템 서비스 컴퓨터에서의 처리순서

① 송신자와 네트워크 연결이 되면 화일전송 시스템 서비스 공개키(e_H, n)을 보낸다.

② 송신자를 확인후 송신자에 필요한 공개키(e_B,n)을 보낸다.

$E_A(D_H(S_A))$=〉 가입자 A 확인(인증)

$E_A(D_H(R_B))$=〉 가입자 B 확인(인증)

③ 보내온 암호문을 수신자의 영역에 저장한다.

④ 수신 요청이 오면 도착된 비문화일의 여부를 확인후 해독에 필요한 공개키(e_H, n)와 암호문을 전송해 준다.

⑤ 수신완료 확인응답 보고가 있으면 해당영역에서 삭제한다.

Ⅳ. 시스템에 사용되는 키 관리

암호화의 보안성은 키를 얼마나 잘 보호할 수 있느냐에 달려있다. 키 관리는 키의 생성에서부터 파괴까지 여러측면을 포함 하는데 특히 키의 분배와 저장은 매우 중요하다. 키를 통신 네트워크를 통하여 전송할때는 또 다른 키를 이용하여 암호화 되어야 한다. 키는 넓은 의미로 공개키와 비밀키로 나눌수 있으며 화일전송 시스템 서비스 컴퓨터를 비롯 사용자 모두가 각각 공개키와 비밀키를 가지고 있다. 키 관리에 있어서는 공개키는 모두 화일전송 시스템 서비스가 관리하며 보호하고 있다가 필요시만 전송하여 준다. 공개키라 하더라도 누구에게나 함부로 공개되지 않으며 화일전송 시스템 컴퓨터가 인증후 필요한 공개키만 그때 그때 전달하며 키의변경 의뢰가 있을 경우 이를 받아들여 수정하여준다. 결국 화일전송 시스템 서비스 컴퓨터는 키의 유지관리및 모든 사용자 통제를 한다. 개인 비밀키는 각자가 보관하고 있다. 또한 키가 파괴되거나 노출되었을때는 변경이 가능하며 화일전송 시스템 시비스에도 알려야 한다. 그룹키는 한 그룹 구성원 모두가 같은 키값을 갖고있다. 비밀키 보호의 강도를 높이려면 chip card나 H/W에 저장으로 구현할 수 있으며 또한 이것을 오랫동안 정확하게 기억하기는 쉬운일이 아니므로 ID 카드로 대신하면 더욱 효과적이다. 공개키 역시 화일전송 시스템 서비스 master key에

의하여 관리보호되며 제안 시스템에 사용되는 키의 종류는 표4-1과 같다.

표 4-1. 사용되는 키의 종류

가입자 개인	공개키	(e_A,n)	화일전송 시스템 서비스가 보관
	비밀키	(d_A,n)	memory chip이나 ID카드로 저장
화일전송 시스템	공개키	(e_H,n)	화일전송 시스템 서비스가 보관
	비밀키	(d_H,n)	〃
그룹	공개키	(e_G,n)	〃
	비밀키	(d_G,n)	그룹 모든구성원이 보관

V. 제안 시스템의 처리 모델

가입자 A가 가입자 B에게 데이타 "SECURITY", time stamp=9001일때 전송의 예를 들어 보자. 일반적으로 RSA 암호방식에서 키의 길이가 100자리이상 정도되면 안전 하다고 할 수 있다. 그렇지만 본 논문에서는 간단한 키를 이용하여 표5-1과 같이 하여 실제 적용하여 보면

표 5-1. 두개의 공통키 값

	고유번호	P	Q	e	d	n
가입자A	A01	11	29	83	27	319
가입자B	B07	13	53	137	41	689
화일전송 시스템		23	47	399	279	1081

가입자A는 화일전송 시스템 서비스와 네트워크 연결상태에서 $E_H(e_H,n)=(399, 1081)$를 부여받아 송수신자 고유명을 암호화하여 화일전송 시스템 서비스 컴퓨터로 보낸다. 이때 모든문자를 숫자화 할때 여러가지 알고리즘을 이용하여 변환할 수 있지만 여기서는 ASCII코드값으로 변환한다.

$S_A=E_H(D_A("A01"))=E_H(D_A(65\ 48\ 49)$
: 문자를 ASCII 코드값으로 변환
$=E_H(54\ 258\ 190)$:A의 디지탈 서명
$=627\ 884\ 538$:암호화

같은 방법으로

$R_B=E_H(D_A("B07"))=E_H(D_A(66\ 48\ 55))$
$=E_H(11\ 258\ 77)$
$=411\ 884\ 466$

S_A, R_B를 전송하면 화일전송 시스템 서비스 주 컴퓨터는 이를 해독하고, A에 필요한 공개키 $(e_A, n)=(83, 319)$, $(e_H, n)=(137, 689)$를 가입자A에 전송한다. 이제 메시지를 암호화하여 화일전송 시스템 서비스로 보낼때 송신자이름, time stamp, 화일을 함께 암호화 하여 C를 보낸다.

$C=E_B(D_A("A01"-"9001"-"SECURITY"))$
$=E_B(D_A(65\ 48\ 49\ 45\ 57\ 48\ 48\ 49\ 45\ 83\ 69\ 67\ 85\ 82\ 73\ 84\ 89))$
:ASCII 코드화
$=E_B(54\ 258\ 190\ 78\ 260\ 258\ 258\ 190\ 78\ 239\ 240\ 100\ 101\ 168\ 292\ 193\ 276)$
:디지탈 서명
$=266\ 501\ 73\ 221\ 533\ 501\ 501\ 73\ 221\ 330\ 57\ 4\ 328\ 56\ 90\ 171\ 345\ 555$
:화일 암호화

화일전송 시스템 서비스 컴퓨터는 수신자명을 확인후 B의 영역에 저장하여 둔다. 가입자B는 시간적여유가 있을시 화일전송 시스템 서비스와 연결공개키 (e_A, n)을 받아

$R_B=E_H(D_B("B07")=E_H(D_B(66\ 48\ 55)$:ASCII 코드값 변환
$=E_H(222\ 575\ 516)$:B의 디지탈서명
$=178\ 552\ 563$:암호화

R_B를 화일전송 시스템 서비스에 전송한다. 화일전송시스템 서비스는 확인후 전송할 내용이 있으면 도착된 암호문과 필요한 공개키(e_H,n)를 B에 전송한다. B는 개인 비밀키와 공개키를 이용

C를 해독하게된다.

$M=E_A(D_B(C))$
$=E_A(D_B(266\ 501\ 73\ 221\ 533\ 501\ 501\ 73\ 221\ 330\ 574\ 328\ 56\ 90\ 171\ 345\ 555)$
$=E_A(54\ 258\ 190\ 78\ 260\ 258\ 258\ 190\ 78\ 239\ 240\ 100\ 101\ 168\ 292\ 183\ 276)$
$=65\ 48\ 49\ 45\ 57\ 48\ 48\ 49\ 45\ 83\ 69\ 67\ 85\ 82\ 73\ 84\ 89$
A 0 1 - 9 0 0 1 - S E C U R I T Y

위의 전과정에서 알 수 있듯이 중간에 암호문 C의 내용을 다른 경로를 통하여 입수 하더라도 키의 값을 알수 없기 때문에 해독하기가 어렵게 된다. 직접통로를 통하여 전송된 송신자, time stamp와 암호문 해독에서 얻은 송신자, time stamp를 비교하여 확인하면 정보의 전달과정에서 생길수 있는 데이타의 추가및 삭제를 확인할 수 있고 송신자 인증문제도 확인된다. 또한 침해자가 도청하여 암호문을 가로 채더라도 침해자가 복호 알고리즘 키를 알지 못한다면 암호문으로부터 평문을 얻을 수 없게되어 데이타에 대한 프라이버시를 보증할 수 있게된다.

Ⅵ. 결 론

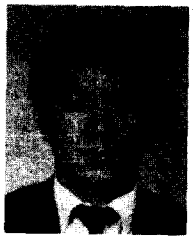
정보화 시대에 각 정보의 보호가 점차 요구됨에 따라 컴퓨터 시스템에 저장되어 있거나 데이타 통신 시스템을 통하여 전송되는 과정에서 비밀을 요하는 화일이 불법적으로 노출, 변조, 파손에, 대비하는 데이타 보호책이필요하다. 종래 방식은 암호(password)를 이용하여 사용자의 권한을 제한하지만 데이타 자체는 보호되지 않는 방법이다. 제안된 시스템에서는 노출된 데이타나 화일을 도청장치 등으로 정보를 획득 하더라도 정보 자체가 암호화되어 있어 암호 해독이 어려우며 또한 암호화 및 해독의 처리가 모두 각자의 워크스테이션에서 처리되기 때문에 더욱 완벽하게 비밀의 보호를 받을 수 있다. 화일전송 시스템의 암호화 방법에서 공개키 암호방식을 채택함으로써 현재 정보통신에 요구되고 있는 비문의 전송에 있어 디지탈 서명을하여 전송하고 상대방의 인증도 가능하게 되어 화일의 비밀유지 및 암호의 강도를 높일 수 있는 시스템을 설계하여 실제 적용하여 보았다. 화일전송 시스템 서비스 패키지에서는 암호문을 유지 관리만하고 해독을 하지 않기때문에 여러 가입자에게 공개될 염려가 없다. 또 어떤 한 그룹의 모든 구성원에게 화일을 전송할때는 그룹키를 이용, 한번에 여러 가입자에게 전송할 수 있어 제안된 예와 같은 화일의 비밀 보호를 받게된다. 계속 연구가 필요한 분야는 처리속도 향상 효율적인 키관리방법이 요구된다.

참 고 문 헌

1. Dorothy E.Denning, Cryptography and Data Security, Adison Wesley Publishing Company, pp.101-147, 1982.
2. Dorothy E.Denning and Peter J.Denning, "Data Security", Computing Surveys Vol.11, No.3, pp.227-245, Sep.1979.
3. Robert Morris and Ken Thompson, "Password Security", Commu. ACM, Vol.22, No.11, pp.594-597, Nov. 1979.
4. R.L. Rivest, A.Shamir and L.Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems", Comm. ACM, Vol.21, No.2, pp.120-126, Feb. 1978.
5. Dorothy E.Denning, "Secure Personal Computing in An Insercure Network", Commu.ACM, Vol.22, No. 8, pp.476-482, Aug. 1979.
6. Leslie Lamport, "Password Authentication with Insecure Communication", Commu.ACM, Vol.24, No.11, pp.770-772, Nov.1981.
7. R.W.Hamming, Coding and Information Theory, Prentcehall, Englewood Cliffs, N.J., 1980.
8. A.G.Konheim, Cryptography, John Wiley and Sone, N.Y., 1981
9. J.Vandewalle, "Implementation Study of Public Key Cryptographic Protection in An Existing Electronic

Mail and Document Handling System", Advance in Cryptology EUROCRTYPT, Vol.219, pp.43-49, Apr. 1985.

10. S.Weinstein, "Smart Credit Cards; the Answer to Cashless Shopping", IEEE Spectrum, Vol.21, No.2, pp.43-49, Feb. 1984.
11. D.Chaum, "Untracable Electronic Mail, Return Address, and Digital Pseudonyms", Comm.ACM, Vol.24, pp.84-88, Feb. 1981.
12. R.Merkle and M. Hellman, "Hiding Information and Signatures in Trapdoor Knapsacks", IEEE Trans. Inform. Theory, Vol.24. pp.525-530, Sep. 1978.



崔 鎭 卓 (Jin Tag CHOI) 正會員
1953年 4 月 8 日生
1977年 2 月：東國大學校 數學科 卒業
1982年 8 月：東國大學校 大學院 電子計算學科 卒業
1987年 2 月：慶熙大學校 大學院 電子工學科 博士課程 修了
1987年～現在：仁川大學校 電子計算學科 助教授로 在職中.

宋 榮 宰 (Young Jae SONG) 正會員
1947年 4 月20日生
1969年 2 月：仁荷大學校 電子工學科 卒業
1972年10月：日本 Toyo Seiko研究員
1976年 3 月：日本Keio Univ. 大學院 卒業
1979年 8 月：明知大學院 卒業(工學博士)
1980年 1 月：工業振興庁 工業標準 審議委員
1982年 8 月：美國Univ. of Maryland 객원教授
1985年 ：韓國情報科學會 平委員
1986年 1 月：大韓電子工學會 電子計算研究會 專門委員長
1986年 1 月～現在：IEEE Computer Society 한국지회副會長
1987年 6 月～現在：全國大學電算所長協議會 總務理事, 副會長
1976年～現在：慶熙大學校 電子計算工學科 教授
• 關心分野：소프트웨어 엔지니어링, 데이타베이스 시스템 Object-oriented Programming & Systems.