(19)대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。Int. Cl.[7]
H04L 9/30

(11) 공개번호 특2003-0047148
(43) 공개일자 2003년06월18일

(21) 출원번호 10-2001-0077555
(22) 출원일자 2001년12월08일

(71) 출원인 학교법인대우학원
경기 수원시 팔달구 원천동 산5번지

(72) 발명자 조민호
경기도 성남시 분당구 이매동 동신아파트 904-804

민복기
서울특별시강남구역삼1동648-9번지힐코트404호

김형도
경기도성남시분당구구미동무지개마을LG(아)203동503호

(74) 대리인 진천웅
조현실

심사청구 : 있음

(54) ＲＳＡ를 이용한 클라이언트/서버 기반의 메신저 보안 방법

요약

본 발명은 RSA를 이용한 클라이언트/서버 기반의 메신저 보안 방법에 관한 것이다.

이러한 본 발명은 RSA 알고리즘을 메신저에 적용하여 클라이언트-서버-클라이언트 간에 송수신하는 메시지의 외부 유출을 방지하는 보안 방법에 있어서, 서버에서 공개키와 개인키를 생성하여, 공개키는 상기 서버로부터 기 인증처리된 제 1, 2클라이언트에 배분하고 개인키는 서버내 레지스터에 저장하는 단계; 공개키를 배분받은 제 1 클라이언트에서 송신할 메시지를 공개키로 암호화하여 상기 서버로 송신하는 단계; 상기 서버에서 수신한 메시지를 개인키로 복호화하는 단계; 상기 서버에서 복호화된 메시지를 개인키로 암호화하여 공개키를 배분받은 제 2클라이언트로 송신하는 단계; 및 상기 제 2클라이언트에서 수신한 메시지를 공개키로 복호화하는 단계를 포함한 것을 특징으로 한다.

본 발명에 따르면, 서버에서 메시지의 복호화와 암호화의 연속된 프로세서를 수행함으로써 메시지를 송신하거나 수신하는 양쪽의 클라이언트가 대칭구조처럼 공개키만을 사용하여 메신저의 메시지에 대한 암호화와 복호화를 처리할 수 있다.

대표도

도 3

색인어

RSA, 암호화, 복호화, 클라이언트, 서버, 메신저, 보안

명세서

도면의 간단한 설명

도 1은 본 발명을 실시하기 위한 바람직한 보안 시스템 개념도,

도 2는 본 발명에 따른 클라이언트/서버간의 키 생성 및 배분을 나타내는 순서도,

도 3은 본 발명에 따라 메시지의 암호화/복호화를 이용한 메시지 전송을 나타내는 순서도이다.

*도면의 주요부분에 대한 부호의 설명

10 : 제 1 클라이언트

20,40 : 네트워크망

30 : 서버

50 : 제 2 클라이언트

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 RSA를 이용한 클라이언트/서버 기반의 메신저 보안 방법에 관한 것으로서, 특히 인터넷이나 인트라넷 등의 네트워크망을 통해 클라이언트/서버 시스템하의 메신저를 사용하여 전송되는 메시지의 외부유출을 방지할 수 있는 보안 방법에 관한 것이다.

현재, 컴퓨터 기술의 급속한 발전과 통신 기술의 발달로 인해 네트워크망을 통한 정보 전달은 정보 제공자와 정보 수신자 사이에서 시간과 공간의 제약을 받지 않고 이루어질 수 있다는 점에서 많은 산업분야에 널리 이용되고 있다.

한편, 네트워크망을 통해 메시지를 주고받기 위해 널리 사용하는 대다수 클라이언트/서버 시스템 기반의 메신저 프로그램들과 피어투피어(Peer To Peer)방식의 메신저 프로그램들은 일반적으로 암호화 기능을 구비하고 있지 않다. 그런데, 회사나 기관에서 주로 이용하는 인트라넷상이나 일반 대중이 이용하는 인터넷상의 클라이언트/서버 시스템하에서 메신저를 통한 많은 중요한 정보들의 교환이 이루어지고 있기 때문에 회사나 기관의 중요한 비밀정보나 대중의 개인정보가 외부로 유출되는 문제점을 갖고 있다.

발명이 이루고자 하는 기술적 과제

이에 본 발명은 상기와 같은 문제점을 해결하기 위하여 안출된 것으로서, 인터넷이나 인트라넷 등의 네트워크망을 통해 클라이언트/서버 시스템하의 메신저를 사용하여 전송되는 메시지의 외부유출을 방지할 수 있는 RSA를 이용한 클라이언트/서버 기반의 메신저 보안 방법을 제공하는데 그 목적이 있다.

상기와 같은 목적을 달성하기 위하여 본 발명에 따른 RSA 알고리즘을 메신저에 적용하여 클라이언트-서버-클라이언트 간에 송수신하는 메시지의 외부유출을 방지하는 보안 방법에 있어서, 서버에서 공개키와 개인키를 생성하여, 공개키는 상기 서버로부터 기 인증처리된 제 1, 2클라이언트에 배분하고 개인키는 서버내 레지스터에 저장하는 단계; 공개키를 배분받은 제 1 클라이언트에서 송신할 메시지를 공개키로 암호화하여 상기 서버로 송신하는 단계; 상기 서버에서 수신한 메시지를 개인키로 복호화하는 단계; 상기 서버에서 복호화된 메시지를 개인키로 암호화하여 공개키를 배분받은 제 2클라이언트로 송신하는 단계; 및 상기 제 2클라이언트에서 수신한 메시지를 공개키로 복호화하는 단계를 포함하여 바람직하게 실시할 수 있다.

발명의 구성 및 작용

이하, 첨부된 도면을 참조하여 본 발명을 상세히 설명하기로 한다.

도 1은 본 발명을 실시하기 위한 바람직한 보안 시스템 개념도로서, 제 1 클라이언트(10), 서버(30), 및 제 2 클라이언트(50)가 네트워크망(20,40)을 통해 연 결된다. 본 발명에서는 RSA(Rivert,Shamir,Adleman) 알고리즘을 이용하여 클라이언트-서버-클라이언트 간의 주고받는 메시지에 암호화 및 복호화 과정을 거치게 함으로써 메시지의 보안을 유지시킨다. 상기 네트워크망(20, 40)은 주로 회사나 기관에서 이용하는 인트라넷망이나 일반대중이 이용하는 인터넷망 등을 포함한다. 상술한 개념도는 설명의 편의를 위한 것이며, 상기 서버(30)에는 다수의 클라이언트가 연결될 수 있다.

한편, 본 발명의 이해를 돕기 위해 상기 RSA 알고리즘에 대하여 설명하기로 한다. RSA 암호법은 암호키의 안전한 분배 및 관리문제를 해결하기 위해 널리 이용되고 있으며, 140자리 이상으로 자리수가 비슷하지만 두 수의 차가 큰 서로 다른 두 소수 p, q (n=pq)를 이용한다. 사용자는 mod Φ(n) = (p-1)(q-1)에 관해 서로소인 e를 개인 공개키로 선택하고 e와 n을 공개한다. 만약에 사용자가 p, q를 알고 있다면, 유클리드 알고리즘을 이용하여 e*d ≡1 (mod (p-1)(q-1)) 인 정수 d를 개인 비밀키로 선택할 수 있고, 이들을 이용하여 암호화와 복호화를 구현한다. 암호화 구현과정을 설명하면, 문자를 숫자로 바꿔 이어놓고 나서, 적당한 숫자블럭으로 나누어서 각 블럭을 mod n에 관해 공개키 e로 거듭제곱한다. 복호화 구현과정을 설명하면, 개인만이 알고있는 비밀키 d를 사용하여 mod n에 관해 거듭제곱하면 원래의 숫자가 나온다.

도 2는 본 발명을 실시하기 위한 클라이언트/서버간의 키 생성 및 배분을 나타내는 순서도이다. 먼저, 서버(30)에서 공개키(Public key)와 개인키(Private key)를 생성하여 구분한다(S100,S110). 이어서, 개인키는 서버(30) 내의 레지스터에 저장하고(S120), 공개키는 서버(30)로부터 기 인증처리된 제 1, 2클라이언트(10,50)에 배분한다(S130). 이때, 인증처리된 클라이언트가 복수개라면 각각의 클라이언트가 공개키를 배분받을 수 있다. 상기 공개키를 각각 배분받은 제 1클라이언트(10)와 제 2클라이언트(50)는 메시지의 암호화와 복호화에 대해 대칭구조처럼 사용된다.

한편, 상기 키 생성 및 배분 과정을 이해하기 위해 RSA 알고리즘 동작에 대하여 구체적으로 설명하자면, 먼저 RSA 공개키 암호에 사용될 공개키{E,N}와 개인키{D,N}를 생성하기 위해서는 다음의 작업을 순차적으로 수행하여야 한다.

첫째로, 두 개의 큰 소수 p와 q를 선정한 다음에 Modulus N = p * q와 PI(N)을 계산한다. 둘째로, 공개키 E는 PI(N) = (p - 1)(q - 1)과 서로소의 관계가 되게 임의로 선정한다. 셋째로, E * D mod PI(N) = 1의 관계에 있는 개인키 D를 '확장된 유클리드 알고리즘'으로 구한다. 넷째로, {E,N}을 공개키로 공개하고, {D,N}을 개인키로 안전하게 보관한다.

다음으로, RSA 암호의 암호화를 위해서는 먼저 암호화된 메시지를 수신할 수신자의 공개키{E, N}을 취득한 후에 암호화할 평문 M을 정수 M으로 전환하여 아래의 수학식 1과 같은 암호화 작업을 수행한 결과인 암호문 C를 수신자에게 보내고, 수신자는 자신의 개인키{D, N}를 이용하여 아래의 수학식 2와 같은 복호화 작업을 통해서 원래의 평문 M을 복원하게 된다.

수학식 1

$$RSA\text{암호화} : E(M) = M \hat{} E \bmod N = C$$

수학식 2

도 3은 본 발명에 따라 메시지의 암호화/복호화를 이용한 메시지 전송을 나타내는 순서도로서, RSA 알고리즘을 메신저에 적용하여 클라이언트-서버-클라이언트 간에 송수신하는 메시지의 외부유출을 방지하는 방법을 나타낸다.

먼저, 서버(30)로부터 기 인증처리되어 공개키를 배분받은 제 1 클라이언트(10)에서는 송신할 메시지를 공개키를 이용해 암호화하고 암호화된 메시지를 서버(30)로 송신하면(S200,S210), 상기 서버(30)에서는 수신한 암호화된 메시지를 개인키를 이용하여 복호화한다(S220).

이어서, 상기 서버(30)에서는 복호화된 메시지를 개인키를 이용해 암호화하여 공개키를 배분받은 제 2클라이언트(50)로 송신하면(S230,S240), 상기 제 2클라이언트(50)에서는 수신한 메시지를 공개키를 이용하여 복호화하여(S250), 암호화하기 전의 메시지를 확인할 수가 있다.

한편, 생성된 공개키를 상기 서버(30)로부터 기 인증처리된 복수의 클라이언트에 배분하고서, 메시지 송신 클라이언트와 메시지 수신 클라이언트가 1 : N, 또는 N : N 으로 통신하는 형태에도 본 발명에 따른 메신저 보안 방법을 적용할 수 있다. 즉, 하나의 클라이언트에서 메시지를 암호화하여 송신하면 서버를 거쳐 복수의 클라이언트에서 암호화된 메시지를 복호화할 수 있다. 또한, 복수의 클라이언트에서 메시지를 암호화하여 송신하면 서버를 거쳐 복수의 클라이언트에서 암호화된 메시지를 복호화할 수 있다.

발명의 효과

본 발명에 따르면, 사내 인트라넷 또는 인터넷상에서 주고받는 메신저 메시지의 외부유출을 방지할 수 있다. 또한, 서버에서 메시지의 복호화와 암호화의 연속된 프로세서를 수행함으로써 메시지를 송신하거나 수신하는 양쪽의 클라이언트가 대칭구조처럼 공개키만을 사용하여 메신저의 메시지에 대한 암호화와 복호화를 처리할 수 있다. 아울러 키관리의 용이함과 전자서명의 사용가능 등 비대칭키의 장점들을 이용할 수가 있다.

(57) 청구의 범위

청구항 1.

RSA 알고리즘을 메신저에 적용하여 클라이언트-서버-클라이언트 간에 송수신하는 메시지의 외부유출을 방지하는 보안 방법에 있어서,

서버에서 공개키와 개인키를 생성하여, 공개키는 상기 서버로부터 기 인증처리된 제 1, 2클라이언트에 배분하고 개인키는 서버내 레지스터에 저장하는 단계;

공개키를 배분받은 제 1 클라이언트에서 송신할 메시지를 공개키로 암호화하여 상기 서버로 송신하는 단계;

상기 서버에서 수신한 메시지를 개인키로 복호화하는 단계;

상기 서버에서 복호화된 메시지를 개인키로 암호화하여 공개키를 배분받은 제 2클라이언트로 송신하는 단계; 및

상기 제 2클라이언트에서 수신한 메시지를 공개키로 복호화하는 단계를 포함한 것을 특징으로 하는 RSA를 이용한 클라이언트/서버 기반의 메신저 보안 방법.

청구항 2.

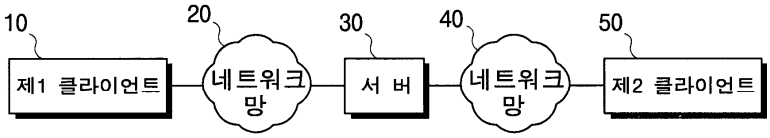
제 1항에 있어서,

생성된 공개키를 기 인증처리된 복수의 클라이언트에 배분하되,

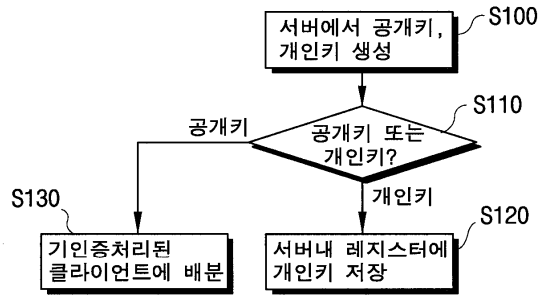
메시지 송신 클라이언트와 메시지 수신 클라이언트가 1 : N, 또는 N : N 으로 통신하는 형태에 적용하는 것을 특징으로 하는 RSA를 이용한 클라이언트/서버 기반의 메신저 보안 방법.

도면

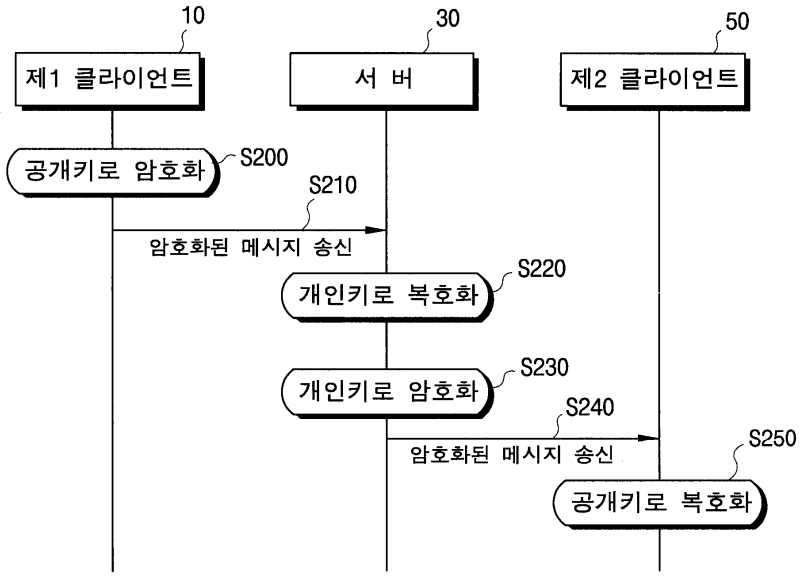
도면1



도면2


서버에서 공개키, 개인키 생성
S100
공개키 또는 개인키?
S110
공개키
개인키
S130
기인증처리된 클라이언트에 배분
서버내 레지스터에 개인키 저장
S120

도면3


10
30
50
제1 클라이언트
서 버
제2 클라이언트
공개키로 암호화
S200
S210
암호화된 메시지 송신
개인키로 복호화
S220
개인키로 암호화
S230
S240
암호화된 메시지 송신
S250
공개키로 복호화