



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2012년04월04일
(11) 등록번호 10-1133093
(24) 등록일자 2012년03월28일

(51) 국제특허분류(Int. Cl.)
H04L 9/14 (2006.01) H04L 9/32 (2006.01)
H04L 9/28 (2006.01)

(21) 출원번호 10-2010-0116598

(22) 출원일자 2010년11월23일
심사청구일자 2010년11월23일

(56) 선행기술조사문헌
R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Communications of ACM, Volume 21, Issue 2, pp. 120-126
KR1020100024605 A
KR1020040092031 A
US20070016785 A1

(73) 특허권자
세종대학교산학협력단
서울특별시 광진구 능동로 209 (군자동, 세종대학교)

(72) 발명자
권태경
서울특별시 강남구 도곡동 아카데미스위트 3709호

(74) 대리인
특허법인엠에이피에스

전체 청구항 수 : 총 11 항

심사관 : 이형일

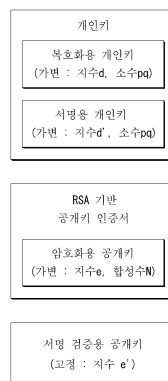
(54) 발명의 명칭 하나의 인증서를 이용하여 암호화와 전자 서명을 제공하는 방법

(57) 요약

하나의 인증서로 RSA 암호화와 전자 서명을 모두 제공하는 방법이 개시된다.

본 발명의 일 실시예에 따르면, 전자 서명 검증용 공개키의 지수(e')를 미리 결정하는 단계, 암호화용 공개키의 합성수(N)와 지수(e)를 선택하고, 복호화용 개인키 지수(d)를 산출하는 단계, 상기 합성수(N)와 지수(e')를 이용하여 전자 서명용 개인키 지수(d')를 산출하는 단계를 포함한다. 여기서, 상기 전자 서명 검증용 공개키 지수(e')는 모든 사용자에게 공개된 고정값이다.

대 표 도 - 도2



특허청구의 범위

청구항 1

하나의 인증서를 이용하여 RSA 암호화와 전자 서명을 제공하는 방법에 있어서,
전자 서명 검증용 공개키의 지수(e')를 미리 결정하는 단계;
암호화용 공개키의 합성수(N)와 지수(e)를 선택하고, 복호화용 개인키 지수(d)를 산출하는 단계;
상기 합성수(N)와 지수(e')를 이용하여 전자 서명용 개인키 지수(d')를 산출하는 단계를 포함하되,
상기 전자 서명 검증용 공개키 지수(e')는 상기 합성수(N)와 무관하게 모든 사용자에게 공개된 고정값인 것을 특징으로 하는 방법.

청구항 2

제 1 항에 있어서,
상기 지수(d)를 이용하여 복호화용 개인키를 생성하는 단계 및
상기 지수(d')를 이용하여 전자 서명용 개인키를 생성하는 단계를 더 포함하는 방법.

청구항 3

제 2 항에 있어서,
상기 공개키의 합성수(N)와 지수(e)는 송신될 메시지 또는 대칭키를 암호화하는데 사용되며,
상기 공개키의 합성수(N)와 지수(e')는 수신된 메시지의 전자 서명을 검증하는데 사용되는 것인 방법.

청구항 4

제 2 항에 있어서,
상기 복호화용 개인키를 이용한 제1암호화 방식과 상기 전자 서명용 개인키를 이용한 제2암호화 방식은 서로 상이한 것인 방법.

청구항 5

제 4 항에 있어서,
상기 제1암호화 방식은 OAEP(Optimal Asymmetric Encryption Padding) 인코딩을 이용하는 공개키 암호 방식이며, 상기 제2암호화 방식은 PSS(Probabilistic Signature Scheme) 전자 서명 방식인 것인 방법.

청구항 6

제 1 항에 있어서,
상기 합성수(N), 지수(e)에 기초하여 공개키 인증서를 생성하는 단계를 더 포함하는 방법.

청구항 7

제 6 항에 있어서,

상기 공개키 인증서에 인증기관의 전자 서명을 수행하는 단계를 더 포함하는 방법.

청구항 8

RSA 공개키 인증서를 이용하여 전자 서명을 수행하는 방법에 있어서,

송신자의 RSA 공개키의 합성수(N_A)와 미리 결정된 공개키 지수(e_A')를 이용하여 전자 서명용 개인키 지수(d_A')를 산출하는 단계; 및

상기 전자 서명용 개인키 지수(d_A')를 이용하여 메시지 또는 해쉬값을 암호화하여 서명하는 단계를 포함하되,

상기 전자 서명 검증용 공개키 지수(e_A')는 상기 합성수(N_A)와 무관하게 수신자에게 공개된 고정값인 것을 특징으로 하는 전자 서명 방법.

청구항 9

제8항에 있어서,

상기 전자 서명용 개인키 지수(d_A') 및 전자 서명 검증용 공개키 지수(e_A')는 SSL/TSL 보안 기법에서 record 프로토콜을 이용하여 제공되는 것인 전자 서명 방법.

청구항 10

RSA 공개키 인증서를 이용하여 전자 서명을 검증하는 방법에 있어서,

수신자의 RSA 공개키로 암호화된 메시지 또는 세션키를 수신자의 복호화용 개인키(d_B)를 이용하여 복호화하는 단계;

상기 복호화용 개인키(d_B)에 의해 복호화된 메시지로부터 송신자의 전자 서명을 검출하는 단계;

상기 전자 서명을 송신자의 RSA 공개키의 합성수(N_A)와 미리 정해진 공개키 지수(e_A')를 이용하여 복호화하는 단계; 및

상기 복호화된 전자 서명을 이용하여 서명 검증을 수행하는 단계를 포함하되,

상기 미리 정해진 공개키 지수(e_A')는 상기 합성수(N_A)와 무관하게, 공개된 고정값인 것인 전자 서명 검증 방법.

청구항 11

제10항에 있어서,

상기 전자 서명용 개인키 지수(d_A') 및 전자 서명 검증용 공개키 지수(e_A')는 SSL/TSL 보안 기법에서 record 프로토콜을 이용하여 제공되는 것인 전자 서명 검증 방법.

명세서

기술 분야

본 발명은 공개키 기반 구조(PKI: Public Key Infrastructure)를 이용한 암호화 및 전자 서명 방법에 관한 것이다.

[0001]

[0002] 더욱 구체적으로, 본 발명은 하나의 공개키 인증서를 이용하여 메시지를 암호화하는 것뿐 아니라 전자 서명을 수행 및 검증할 수 있는 방법에 관한 것이다.

배경 기술

[0003] 최근, PKI의 보급과 함께, SSL/TLS (Secure Socket Layer/Transport Layer Security) 보안 기법 등과 같이 공개키 암호화를 사용하는 보안 기법들이 널리 활용되고 있다. SSL/TLS는 인터넷과 응용 계층(application layer)와 전달 계층(transport layer) 사이에서 인증과 키 분배, 그리고 암호를 제공하기 위한 보안 계층 및 프로토콜에 해당한다.

[0004] 도 1은 SSL/TLS 보안 기법의 동작을 설명한 신호 흐름도이다.

[0005] 클라이언트(1)와 서버(2) 사이에는 인터넷 쇼핑, 경매, बैंक, 증권 등의 전자 상거래가 이뤄질 수 있다. 이 때 클라이언트(1)와 서버(2)사이의 송수신 되는 텍스트 등의 데이터는 암호화되어 타인에 의해 해독되어서는 안 된다.

[0006] 이를 지원하기 위해서, 서버(2)가 SSL/TLS 보안 프로토콜을 지원하는 경우에는 클라이언트(1)와 서버(2) 사이의 세션을 통해 전송되는 데이터를 세션키를 암호화할 수 있다. 이러한 세션키를 주고 받기 위해서, 세션키를 암호화하는 공개키를 인증서를 이용하여 인증한다.

[0007] 이에 대해 보다 상세히 설명하면, 클라이언트(1)와 서버(2)는 단계(S1) 암호 방식에 대해서 상호 협상한다. 암호 방식 협상은 클라이언트(1)이 지원 가능한 암호화 방식, 서명 방식, 압축 방식을 서버(2)에 알리고, 서버(2)는 이에 대해 응답하고 세션 ID를 할당하게 된다.

[0008] 단계(S2)에서는 클라이언트(1)은 공개키 인증서를 이용하여 서버(2)를 인증한다. 공개키 인증서에서는 서버(2)에 관한 정보 및 공개키가 기록되어 있으며, 이는 전자 서명되어 클라이언트(1)에 의해 검증된다.

[0009] 단계(S3)에서는 동일한 방식으로 서버(2)가 클라이언트(1)을 인증한다. 상기 클라이언트 인증이 필요 없는 경우에는 단계(S3)은 생략될 수 있다.

[0010] 인증이 완료되면, 단계(S4)에서 클라이언트(1)과 서버(2) 사이의 세션키가 확보된다. 상기 세션키는 일회용 대칭키로서 메시지를 암호화하는데 사용되고, 상기 세션키 자체는 서버(2)의 공개키로 암호화되어 전송될 수 있다(S5).

[0011] 이러한 일반적인 SSL/TLS 보안 프로토콜에서는 별도의 인증서 없이 부인 봉쇄 기능을 제공하지는 못한다.

[0012] 부인 봉쇄란, 송신자가 자신의 정보를 정확하게 상대방에게 전송하였다고 할지라도 수신자가 이를 부인하거나, 수신자가 정확한 정보를 받았음에도 불구하고 송신자가 자신이 보낸 정보가 아니라고 주장하는 것을 방지하는 기능이다.

[0013] 이러한 부인 봉쇄 기능은 온라인 금융 거래 등에 있어서는 필수적인 기능이며, 이러한 전자 서명 기법에 의해 될 수 있다.

[0014] 전자 서명은 송신자를 인증하면서도 전송되어온 메시지가 변조되지 않았음을 증명하는 디지털 정보이며, RSA 암호화 공개키 이외에 별도의 공개키 인증서가 별도로 필요하다.

[0015] 따라서, SSL/TLS 보안 기법에 있어서, 별도의 인증서를 요구하지 않으면서도 수정 수준을 최소화한 상태에서 전자 서명을 제공하는 방법이 절실히 요구된다.

발명의 내용

해결하려는 과제

[0016] 본 발명의 일부 실시예들은 하나의 공개키 인증서를 이용하여 RSA 암호화와 전자 서명의 수행 및 검증이 가능한 방법을 제공한다.

과제의 해결 수단

- [0017] 상술한 기술적 과제를 달성하기 위한 기술적 수단으로서, 본 발명의 제 1 측면은 전자 서명 검증용 공개키의 지수(e')를 미리 결정하는 단계, 암호화용 공개키의 합성수(N)와 지수(e)를 선택하고, 복호화용 개인키 지수(d)를 산출하는 단계 및 상기 합성수(N)와 지수(e')를 이용하여 전자 서명용 개인키 지수(d')를 산출하는 단계를 포함하되, 상기 전자 서명 검증용 공개키 지수(e')는 모든 사용자에게 공개된 고정값인 것을 특징으로 하는 하나의 인증서를 이용하여 RSA 암호화와 전자 서명을 제공하는 방법을 제공할 수 있다.
- [0018] 본 발명의 제 2 측면은 송신자의 RSA 공개키의 합성수(N_A)와 미리 결정된 공개키 지수(e_A')를 이용하여 전자 서명용 개인키 지수(d_A')를 산출하는 단계 및 상기 전자 서명용 개인키 지수(d_A')를 이용하여 메시지 또는 해쉬값을 암호화하여 서명하는 단계를 포함하되, 상기 전자 서명 검증용 공개키 지수(e_A')는 수신자에게 공개된 고정값인 것을 특징으로 하는 RSA 공개키 인증서를 이용하여 전자 서명을 수행하는 방법을 제공할 수 있다.

발명의 효과

- [0019] 전술한 본 발명의 과제 해결 수단 중 하나에 의하면, 하나의 공개키 인증서를 이용하여 복호화용 개인키와 전자 서명용 개인키가 생성된다. 따라서, 하나의 공개키 인증서를 이용하여 사용자는 RSA 암호화뿐 아니라, 전자 서명 및 검증을 이용할 수 있다.

도면의 간단한 설명

- [0020] 도 1은 SSL/TLS 보안 기법의 동작을 설명한 신호 흐름도이다.
- 도 2는 본 발명의 일 실시예에 따른 공개키와 개인키를 도시한 도면이다.
- 도 3은 본 발명의 실시예에 따른 키 생성 방법을 도시한 흐름도이다.
- 도 4는 본 발명의 실시예에 따른 전자 서명 및 검증 프로세스를 도시한 신호 흐름도이다.

발명을 실시하기 위한 구체적인 내용

- [0021] 아래에서는 첨부한 도면을 참조하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 본 발명의 실시예를 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시예에 한정되지 않는다. 그리고 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.
- [0022] 명세서 전체에서, 어떤 부분이 다른 부분과 "연결"되어 있다고 할 때, 이는 "직접적으로 연결"되어 있는 경우뿐 아니라, 그 중간에 다른 소자를 사이에 두고 "전기적으로 연결"되어 있는 경우도 포함한다. 또한 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있는 것을 의미한다
- [0023] 본 발명의 실시예를 설명하기에 앞서, 우선 RSA 암호화를 위한 공개키 및 개인키 생성 방법을 설명한다.
- [0024] 공개키 (N, e) 에서, N 은 소수 p 와 q 의 곱($N = pq$)으로 이루어진다.
- [0025] 여기서, $\phi(N) = (p-1)(q-1)$ 이라고 할 때, N 과 서로 소(relatively prime)인 e 를 선택한다. (여기서, $\phi(N)$ 는 N 의 Euler's totient 값임)
- [0026] 한편, 개인키를 위하여 선택된 e 로부터, $de = 1 \bmod \phi(N)$ 를 만족하는 수 d 를 계산한다.
- [0027] 여기서, 합성수 N 과 지수 e 는 공개키의 요소로서 공개키(N, e)의 형태로 공개되고, 계산된 d 는 개인키 지수로서 보관하게 된다.
- [0028] 이와 같이 공개키(N, e)와 개인키 (d)가 생성되면, 메시지 (M)은 이하와 같이 암호화될 수 있다.
- [0029] $C = M^e \bmod N$

- [0030] 암호문 (C)는 개인키 (d)를 이용하여 이하와 같이 복호화 될 것이다.
- [0031] $M = C^d \bmod N$
- [0032] 이미 설명한 바와 같이, N은 이미 공개된 값이기 때문에 송신자 및 수신자 모두 사용이 가능하다.
- [0033] 다음은 전자 서명의 과정에 대해서 설명한다.
- [0034] 전자 서명에 사용되는 개인키와 공개키는 암호화에 사용되는 개인키와 공개키와 다른 값을 가질 수 있지만 설명의 편의를 위하여 동일한 부호 (N,e), (d)를 사용하여 설명한다.
- [0035] 서명값 S는 이하와 같이 정의된다.
- [0036] $S = H(M)^d \bmod N$
- [0037] 여기서 H(M)은 메시지 M의 해쉬값이며, 상기 해쉬값은 개인키 (d)로 암호화(서명)되어 메시지(M)과 함께 송신된다.
- [0038] 이러한 서명 S로부터 H(M)은 이하와 같이 검증 된다.
- [0039] $H(M) = S^e \bmod N$
- [0040] 여기서 서명값 S와 함께 전송된 해쉬값(H(M))은 함께 전송된 메시지(M)의 해쉬값과 비교되어 무결성을 검토하는데 사용된다.
- [0041] 무결성이 확인되고 나면 해쉬값(H(M))과 서명을 검증(복호화)한 값을 상호 비교하여 송신자의 전자 서명이 맞는지 확인한다. .
- [0042] 이를 통해 송신자가 송신한 메시지의 무결성이 입증되고, 부인 봉쇄를 실현할 수 있다.
- [0043] 여기서, 수신자는 송신자의 개인키로 암호화한 서명을 복호화하기 위하여 송신자의 공개키가 필요하며, 이를 위해서는 송신자의 공개키를 인증하는 별도의 인증서가 필요할 것이다.
- [0044] 본 발명에서는 전자 서명 및 검증에 필요한 별도의 인증서 또는 별도의 웹 브라우저 플러그 인이나 Active-X 없이도 RSA 암호와 서명을 동시에 할 수 있는 방법을 제시한다.
- [0045] 본 발명이 제시하는 방법은 별도의 공개키 인증서의 요구 단계를 없애고, SSL/TLS 계층에 대한 수정을 record protocol만으로 최소화한다.
- [0046] 도 2는 본 발명의 일 실시예에 따른 공개키와 개인키를 도시한 도면이다.
- [0047] 도 2와 같이, 개인키와 공개키는 이하와 같이 정의될 수 있다.
- [0048] 암호화용 공개키 (합성수 N, 지수 e)
- [0049] 서명 검증용 공개키 (지수 e)'
- [0050] 복호화용 개인키 (지수 d, 소수 p, q)
- [0051] 서명용 개인키 (지수 d' , 소수 p, q)
- [0052] 여기서, 소수 p, q 및 N의 값은 암호/복호화 또는 서명/검증에 있어서 동일한 값이다.
- [0053] 하지만, 지수 e와 지수 e' 는 상이하며, 지수 d와 지수 d' 는 상이하다.
- [0054] 또한, 지수 e' 를 제외한 다른 값들은 사용자에게 따라 가변적인 값을 가질 것이다.
- [0055] 하지만, 지수 e' 는 사용자에게 상관없이 고정 값을 가지며, 여기서 고정 값인 지수 e' 는 모든 사용자에게 공개되어 공유될 수 있다.

- [0056] 이러한 특징을 이용하여, 본 발명의 일 실시예에 따르는 경우 별도의 인증서 없이 RSA 암호화와 전자 서명을 동시에 제공할 수 있다.
- [0057] 도 3은 본 발명의 실시예에 따른 키 생성 방법을 도시한 흐름도이다.
- [0058] 도 2와 같이 정의되는 경우, RSA 공개키를 생성함에 있어서, 기존과 같이 $N = pq$ 를 구한 후에, 암호화용 공개키 지수 e 를 선택한다(S100).
- [0059] 암호화용 공개키 지수 e 가 선택되면, 복호화용 개인키 지수 d 가 이하의 수식으로부터 얻어질 수 있다(S110).
- [0060] $de = 1 \bmod \phi(N)$
- [0061] 이와 함께 고정값인 서명 검증용 공개키 지수 e' 로부터 서명용 개인키 지수 d' 를 이하의 수식으로부터 구한다(S120).
- [0062] $d' e' = 1 \bmod \phi(N)$
- [0063] 여기서, e' 값은 고정되어 있지만, p, q 의 값이 가변적이기 때문에 d' 는 사용자마다 상이한 값을 가질 수 있다. 하지만, e' 는 고정되어 있으며 그 값이 모든 사용자에게 공개되어 있으므로, 모든 사용자가 서명 검증에 이용할 수 있을 것이다.
- [0064] 한편, 여기서 암호화용 공개키 지수 e 는 이미 알려진 서명 검증용 공개키 지수 e' 와는 상이한 값으로 선택되어야 한다.
- [0065] 이후, 합성수 N 과 지수 e 를 이용하여 RSA 공개키 인증서 및 복호화용 개인키 및 서명용 개인키가 생성된다(S130). 상기 RSA 공개키 인증서 소유자는 복호화용 개인키 지수로서 d 를 사용하고, 전자 서명용 개인키 지수로서 d' 를 사용한다.
- [0066] 여기서, 공개키 암호와 전자 서명을 위한 인코딩 방식은 서로 다르도록 할 수 있다. 예를 들어, 공개키 암호의 경우에는 OAEP(Optimal Asymmetric Encryption Padding)방식을 사용하고, 전자 서명에서는 PSS(Probabilistic Signature Scheme) 방식을 사용할 수 있다.
- [0067] 상기 RSA 공개키 인증서에 대한 검증자는, 인증서에 포함된 인증 기관(CA; Certification Authority)의 서명을 검증한 후, 인증서에 포함된 암호화용 공개키를 이용해서, 인증서의 소유자만이 복호화할 수 있는 암호문을 구성할 수 있을 뿐 아니라, 해당 인증서 소유자가 서명한 서명에 대해 검증할 수 도 있다.
- [0068] 도 4는 본 발명의 실시예에 따른 전자 서명 및 검증 프로세스를 도시한 신호 흐름도이다.
- [0069] 도 4에서는 송신 단말 A가 수신 단말 B에 세션키로 암호화한 메시지를 전송하는 상황이 도시되어 있다. 도 4는 세션키로 메시지를 암호화하고 공개키로 세션키를 암호화하는 하이브리드 방식이 설명되어 있지만, 이는 단지 발명을 설명하기 위한 예시일 뿐이며, 대칭키 암호화 방식이나 비대칭 암호화 방식 모두에 본 발명이 적용될 수 있다.
- [0070] 송신 단말 A(10)는 복호화용 개인키 d_A , 서명용 개인키 d'_A , 암호화용 공개키 (N_A, e_A) 및 서명 검증용 공개키 (N_A, e'_A) 를 구비하고 있다.
- [0071] 수신 단말 B(10)는 복호화용 개인키 d_B , 서명용 개인키 d'_B , 암호화용 공개키 (N_B, e_B) 및 서명 검증용 공개키 (N_B, e'_B) 를 구비하고 있다.
- [0072] 여기서, 서명 검증용 공개키 e'_A 와 e'_B 동일한 고정값이다. 하지만, N_A 와 N_B 는 상이한 값이며, CA(30)의 인증서를 통해서 획득될 수 있다.
- [0073] 단계(S200)에서 송신 단말 A(10)는 송신 메시지(M_A)의 해쉬값($H(M)_A$)의 값을 생성한다. 이후, 서명용 개인키 d'_A 를 이용하여 축약된 해쉬값($H(M)_A$)을 암호화하여 서명값 S_A 를 생성한다.
- [0074] 생성된 서명값(S_A), 해쉬값($H(M)_A$), 메시지 (M_A) 전체는, 대칭키인 세션키로 암호문(C)로 암호화된다. 세션키는 수신 단말 B(20)의 공개키(N_B, e_B)로 암호화되어, 암호문(C)와 함께 수신 단말 B(20)로 전송된다(S210).
- [0075] 이후, 수신 단말 B(20)는 자신의 복호화용 개인키(d_B)로 세션키를 복호화한다(S230). 복호화된 세션키는 암호

문(C)를 서명값(S_A), 해쉬값($H(M)_A$), 메시지 (M_A)로 복호화하는데 이용된다.

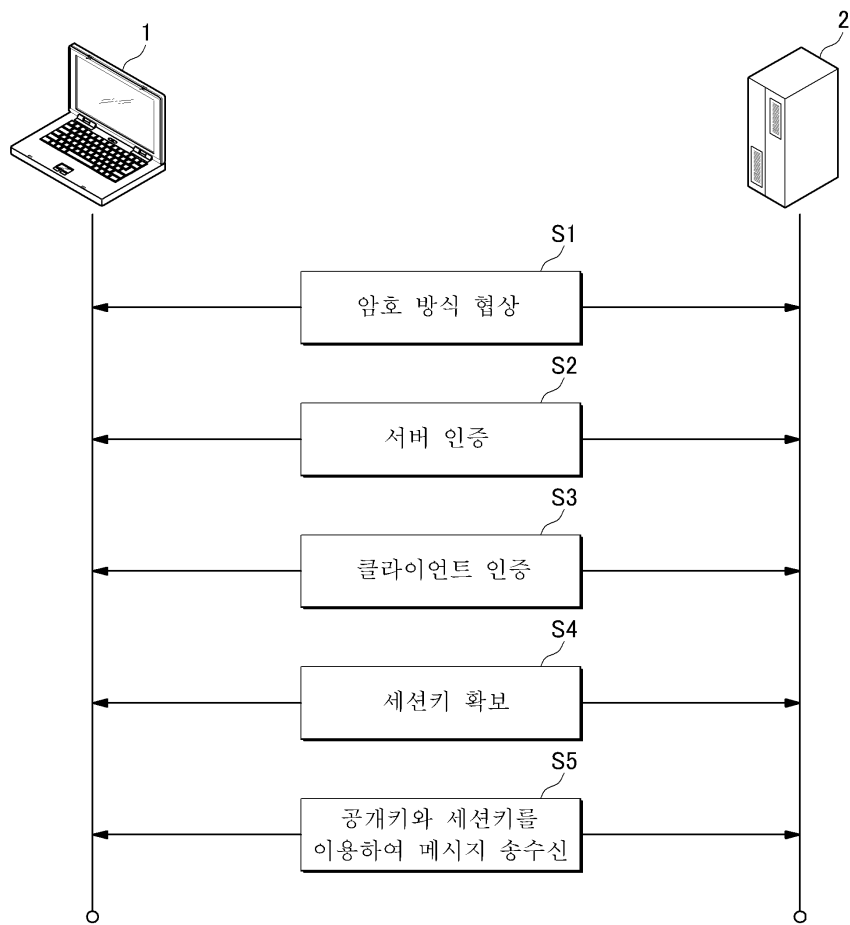
- [0076] 이후 수신 단말 B(20)는 메시지(M_A)의 해쉬값을 생성해서, 송신된 해쉬값($H(M)_A$)과 비교하여 데이터 무결성을 체크한다(S240).
- [0077] 무결성에 문제가 없는 경우, 수신 단말 B(20)는 송신 단말 A(10) 공개키 합성수 (N_A)와 서명 검증용 공개키 지수 (e_A')를 이용하여 서명값(S_A)를 복호화하고, 복호화한 값과 해쉬값($H(M)_A$)을 비교하여 서명을 검증한다(S250).
- [0078] 여기서, 서명 검증용 공개키 지수 (e_A')는 고정값이며, 서명 검증시에도 암호화용 공개키 합성수 N_A 값을 그대로 이용하기 때문에, 별도의 인증서 없이도 RSA 암호화와 전자 서명/검증을 모두 수행할 수 있다.
- [0079] 따라서, 본 발명의 실시예에 의한 경우 SSL/TSL 를 사용하는 시스템에서도 SSL/TSL 계층의 수정을 record protocol 수정 수준으로 최소화하면서도 전자 서명을 이용할 수 있는 안전한 통신을 제공할 수 있다.
- [0080] 본 발명의 일 실시예는 컴퓨터에 의해 실행되는 프로그램 모듈과 같은 컴퓨터에 의해 실행가능한 명령어를 포함하는 기록 매체의 형태로도 구현될 수 있다. 컴퓨터 판독 가능 매체는 컴퓨터에 의해 액세스될 수 있는 임의의 가용 매체일 수 있고, 휘발성 및 비휘발성 매체, 분리형 및 비분리형 매체를 모두 포함한다. 또한, 컴퓨터 판독 가능 매체는 컴퓨터 저장 매체 및 통신 매체를 모두 포함할 수 있다. 컴퓨터 저장 매체는 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈 또는 기타 데이터와 같은 정보의 저장을 위한 임의의 방법 또는 기술로 구현된 휘발성 및 비휘발성, 분리형 및 비분리형 매체를 모두 포함한다. 통신 매체는 전형적으로 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈, 또는 반송파와 같은 변조된 데이터 신호의 기타 데이터, 또는 기타 전송 매커니즘을 포함하며, 임의의 정보 전달 매체를 포함한다.
- [0081] 전술한 본 발명의 설명은 예시를 위한 것이며, 본 발명이 속하는 기술분야의 통상의 지식을 가진 자는 본 발명의 기술적 사상이나 필수적인 특징을 변경하지 않고서 다른 구체적인 형태로 쉽게 변형이 가능하다는 것을 이해할 수 있을 것이다. 그러므로 이상에서 기술한 실시예들은 모든 면에서 예시적인 것이며 한정적이 아닌 것으로 이해해야만 한다. 예를 들어, 단일형으로 설명되어 있는 각 구성 요소는 분산되어 실시될 수도 있으며, 마찬가지로 분산된 것으로 설명되어 있는 구성 요소들도 결합된 형태로 실시될 수 있다.
- [0082] 본 발명의 범위는 상기 상세한 설명보다는 후술하는 특허청구범위에 의하여 나타내어지며, 특허청구범위의 의미 및 범위 그리고 그 균등 개념으로부터 도출되는 모든 변경 또는 변형된 형태가 본 발명의 범위에 포함되는 것으로 해석되어야 한다.

부호의 설명

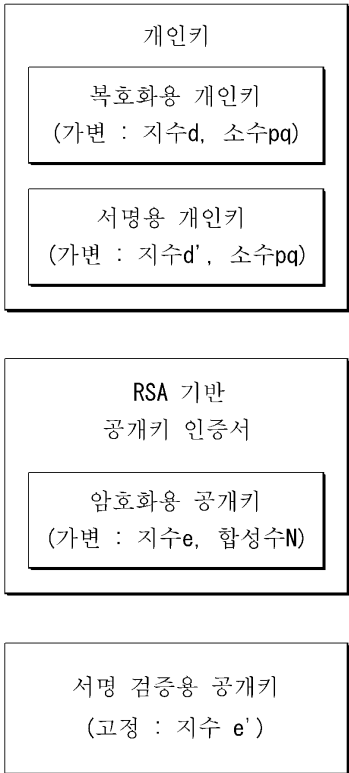
- [0083]
- | | |
|-----------|-----------|
| 1: 클라이언트 | 2: 서버 |
| 10: 송신 단말 | 20: 수신 단말 |
| 30: CA | |

도면

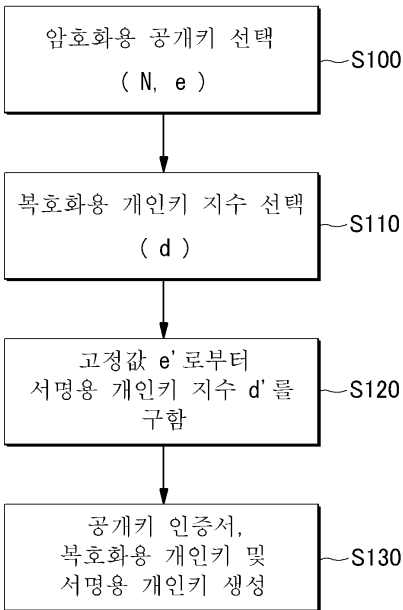
도면1



도면2



도면3



도면4

