韓國通信情報保護學會誌
第1卷, 第1號, 1991. 4

암호시스템을 이용한 디지탈 서명시스템

남 길 현*

1. 서 론

가. 디지탈 서명(digital signature)의 필요성

컴퓨터산업의 급속한 발전과 정보화사회 구현을 위한 각종 전산망이 확대 보급되어 운영되고 있는 현 시점에서 대량의 중요한 정보들이 컴퓨터를 통하여 저장 및 처리되고 컴퓨터 통신망을 이용한 정보교환이 신속하게 이루어지고 있다.

그러나 컴퓨터를 이용함으로써 많은 장점이 있는 반면 권한이 없는 불법적인 침입자로부터 개인이나 조직의 중요한 자료들을 보호하고 컴퓨터 통신망을 통해 전송되는 자료의 불법적인 도청이나 내용의 변조를 방지하기 위한 보안대책이 매우 중요한 문제점으로 나타나고 있다. 특히 국가에서 추진중인 국가 5대 기간 전산망과 같은 사업에서는 이미 자료의 적극적인 보안대책이 요구되고 있는 실정이다.

또한 종래의 종이서류에 의한 문서 수발 업무등이 컴퓨터 통신망을 통해 빠르고 경제적으로 이루어지고 있으나, 이와 함께 메세지전송시 상대방의 신분을 확인하거나 사용자의 정당성을 인증하고 송수신자간에 일어날 수 있는 제반분쟁을 해결할 수 있도록, 통상적인 인감도장과 같은 역할을 해줄 수 있는 제도나 절차가 필연적으로 요구된다.

이는 제반 문서처리와 마찬가지로 어떤 메세지를 컴퓨터 통신망을 통하여 전송하였을 때, 수신자가 고의적으로 메세지 내용을 자신에게 이롭도록 고칠 수도 있고, 또 비양심적인 송신자가 메세지를 보내지 않았다고 부인하거나 혹은 메세지 내용을 수신자가 위조해서 자신이 보낸 내용과 틀리다고 주장한다면 결국 송수신자 사이에 분쟁이 발생하게 되며 이를 근본적으로 해결할 방법이 있어야 되는 것이다. 또한 이와 같은 것은 수신자가 메세지 접수시 마다 메세지 내용의 진위여부를 확인할 것을 요구하게 되며, 메세지 내용이 수신자로 하여금 일련의 응답조치 및 행동을 요구한 것이라면, 송신자는 메세지가 확실히 신뢰할 수 있는 것이라는 것을 믿게 할 필요가 있는 것이다.

이와같이 컴퓨터 통신망을 통하여 메세지 전송시 필요한 메세지 서명방법을 디지탈 서명(digital signature)이라고 하며, 최근에는 디지탈 서명을 실제로 구현하는데 암호시스템(crypto system)을 이용하는 방안에 대하여 많은 연구가 진행되고 있다.

본고에서는 이러한 암호시스템을 이용하여 메세지 서명기능을 수행하는 디지탈 서명시스템에 대해서 살펴보기로 한다.

* 종신회원, 국방대학원

나. 프로토콜의 형태

암호시스템이란 자료에 대한 도청이란 변조 또는 정보의 누출을 방지하기 위해서 자료를 암호화시켜 저장하거나 전송함으로써 비밀키를 알고 있는 인가된 사람이 아니면 해독할 수 없도록 하는 체제로서, 일반적으로 보통문을 암호문으로 변형하고 필요시 암호문을 본래의 보통문으로 복호화하는 체제로 구성되며 관용키(또는 개인키)(private key) 암호시스템과 공중키(또는 공개키)(public key) 암호시스템으로 크게 분류할 수 있다[1].

디지탈 서명시스템은 관용키 암호시스템, 공중키 암호시스템 또는 관용키와 공중키를 조합한 암호시스템을 이용하여 디지탈 서명이 요구하는 특성을 충족시켜 주도록 구현할 수 있다.

보통 디지탈 서명에는 서명을 어떻게 수행하느냐에 따라서 서로 다른 프로토콜이 적용될 수 있는데 이는 첫째, 다른 매개수단을 통하지 않고 송수신자간에 직접 문자와 서명을 송수신하는 당사자 서명방법과 둘째, 송수신자간에 제 3 자의 중재자를 통하여 문서를 송수신함으로써 중재자에 의해서 송신자의 서명이 인증되는 중재자 서명방법이 사용될 수 있으며,셋째로는 당사자 서명방법과 중재자 서명방법을 혼용한 복합형 서명방법이 사용될 수 있다[2].

한편, 서명할 메세지의 크기와 용도에 따라서 서명을 어떻게 할것인가가 고려되어야 한다. 즉, 암호화단위 크기마다 서명을 하거나 전체 메세지 끝에 서명을 첨가하는 방법 등 다양한 방법이 고려될 수가 있다. 메세지와 서명이 분리되어 있는 경우에는, 송신자가 서명은 맞지만 메세지가 자신이 보낸 메세지가 아니라고 거부하거나 수신자가 보내온 메세지 내용을 변경하여 송신자의 서명과 함께 조작된 메세지를 주장할 경우에는 진위 판단이 어려워 진다.

따라서, 이와 같은 경우를 대비하기 위해서는 디지탈 서명의 내용에 메세지의 중요한 내용을 요약하여 포함시키는 방법을 고려할 수 있다. 즉 디지탈 서명내용에 송수신자의 성명과 메세지의 일련번호 뿐만 아니라 메세지의 요약(condensed message)을 추가하거나 특정위치에서 추출된 데이타를 집약시켜 줌으로써 메세지의 임의 변경을 어렵게 할 수 있다.

2. 디지탈 서명의 특성

일반적으로 암호시스템이 추구하고자 하는 기본 목표는 비인가자에게 자료가 노출되는 것을 보호하는 비밀성(secrecy)과 비인가자가 자료를 변형할 수 없도록 보호하는 인증성(authenticity)에 있다[1]. 이러한 인증성은 자료를 보내는 송신자와 보내온 메세지를 신뢰한다는 의미가 되며 암호시스템을 이용한 디지탈 서명시스템도 동일한 기본 목표를 지니게 된다.

특히, 컴퓨터 통신망을 이용하여 서명된 메세지를 보낸다고 함은 기본적으로 수신자는 송신자를 확인할 수 있어야 하며, 송신자는 추후에 보낸 메세지를 부인할 수 없어야 하는 것이다.

즉, 디지탈 서명은 개인의 고유성과 정당성을 제공하고 메세지의 인증과 송수신자 사이에 발생하는 제반 문제점을 해결해 주어야 하기 때문에 다음과 같은 요구조건이 충족되어야 한다[1,3]. 송신자에 의해서 메세지가 디지탈 서명되어 수신자에게 전송되었다면,

첫째, 수신자는 메세지의 서명을 보고 송신자를 확인할 수 있어야 한다.

둘째, 수신자를 포함한 어느 누구도 메세지 내용을 변조하거나 송신자의 서명을 위조할 수 없어야 한다.

세째, 만약 송신자가 메세지의 내용이나 서명을 부인할 경우에는 심판자(제 3 자)가 송신자와 수신자의 분쟁을 해결해 줄 수 있어야 한다.

즉, 위와 같은 요구조건이 충족되면 수신자는 메세지를 받아 볼 때 송신자가 누구인가를 확인함으로써 송신자의 고유성을 부여할 수 있게 되며, 아무도 송신자의 서명을 위조할 수 없음으로써 수신자는 보내온 메세지에 대한 정당성을 인증하게 하고, 송신자가 메세지 송신을 부인하게 될 경우에 위증을 가려 잘못의 책임소재를 분명히 할 수 있

음으로써 디지탈 서명의 기능을 수행하는 시스템이 될 수 있는 것이다.

디지탈 서명이 종이에 서명하는 방법과 틀린점은 종이에 하는 서명이 아무리 복잡해도 비교적 쉽게 위조가 가능하지만 디지탈 서명은 사용하는 방법에 따라 위조할 확율을 줄일 수 있고, 종이에 하는 서명은 사람에 따라 일정하여 모든 문서에 동일하지만 디지탈 서명은 각 메세지마다 서명이 상이하게 할 수 있는 점이라 하겠다[2].

본래 디지탈 서명은 메세지의 비밀성을 반드시 필요로 하는 것은 아니지만 본고에서는 전달되는 메세지의 비밀성도 함께 보장되는 서명시스템을 고려하기로 한다.

3. 공중키 암호시스템을 이용한 당사자 서명시스템

공중키 암호시스템에서는 사용자가 두개의 키인 비밀키와 공개키를 사용하여 보통문을 암호문으로 암호화하고, 암호문을 보통문으로 복호화한다. 이때 각 사용자의 공개키는 공유된 장소에 저장하여 사용할 수 있는 공개된 키이며 비밀키는 각 사용자만 알고 있는 키로서 비밀로 유지된다.

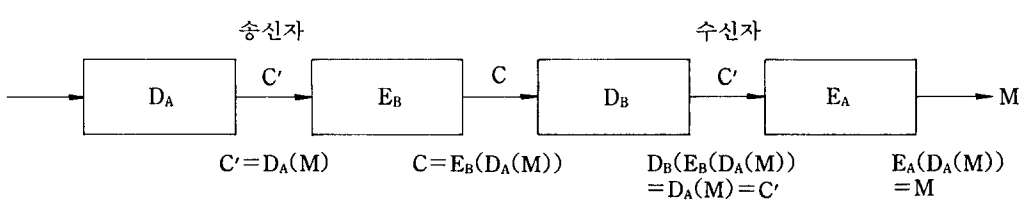
당사자 서명시스템은 평상시에 제3자를 필요로 하지 않기 때문에 가장 바람직한 프로토콜의 형태라고 할 수 있다.

그러면 공중키 암호시스템을 먼저 살펴보고 이러한 공중키 암호시스템이 어떻게 당사자 서명시스템으로 이용될 수 있는가를 살펴보기로 하자.

송신자가 수신자에게 메세지를 송신할 때 가장 간단한 방법은 수신자의 공개키로 메세지를 암호화하여 전송하고 수신자는 전송된 암호문을 자신의 비밀키로 복호화하는 것이다. 그러나 이 경우에는 비밀성이 보장되는 메세지를 보낼 수는 있으나, 특정한 송신자가 메세지를 보냈다는 것을 증명하지는 못한다. 왜냐하면 수신자의 공개키를 알고 있는 사용자 누구라도 메세지를 암호화하여 보낼 수 있기 때문이다.

특정 송신자가 메세지를 보냈다는 것을 나타내기 위해서는, 송신자의 비밀키로 메세지를 암호화하여 전송하고 수신자는 암호문을 자신의 공개키로 메세지를 얻을 수 있다. 그러나 이 경우에는 특정한 송신자가 수신자에게 메세지를 보냈다는 것은 인증할 수는 있으나 수신자의 공개키를 알고 있는 누구라도 암호문을 해독할 수 있기 때문에 비밀성이 보장되지는 못한다.

따라서, 비밀성과 인증성이 보장되는 메세지를 보내게 하기 위해서 송신자는 메세지를 자신의 비밀키를 이용하여 암호화한 후, 이를 수신자의 공개키를 이용하여 재 암호화해서 전송하고, 수신자는 보내온 암호문을 자신의 비밀키를 이용하여 복호화한 후 송신자의 공개키를 이용하여 재 복호화함으로써 메세지를 얻을 수 있다. 이와 같은 절차를 도식해 보면 그림 1과 같다.



(수신자는 C 또는 C′를 서명으로 보관함)

M : 메세지 C : 암호문

D_A, D_B : A 또는 B의 비밀키에 의한 암호와 절차

E_A, E_B : A 또는 B의 공개키에 의한 암호와 절차

그림 1. 공중키 암호시스템을 이용한 당사자 서명시스템

위와 같은 체계를 디지탈 서명의 요구특성과 비교하면 송신자의 비밀키를 이용한 암호화 과정은 오직 송신자만이 수행할 수 있으므로 이를 송신자의 서명이라고 간주할 수 있고 이렇게 생성된 서명은 아무도 위조할 수 없는 것이므로 추후 자신의 비밀키와 송신자의 공개키를 이용하여 보내온 암호문으로부터 복호화해서 메세지를 얻을 수 있으므로 송신자의 공개키를 사용한다는 것은 송신자의 서명을 확인하는 것이 되며, 암호문만 보관하고 있으면 송신자와 수신자의 사이에서 일어나는 제반 논쟁을 해결할 수 있게 된다. 따라서 디지탈 서명 시스템의 요구조건을 충족하게 된다.

이와 같이 공중키 암호시스템은 디지탈 서명기능을 수행할 수 있다고 하지만 모든 공중키 암호시스템이 이에 적합한 것은 아니다. 왜냐하면 암·복호화 기능이 서로 역(inverse)관계에 있어야 하기 때문이다. 이런 종류의 대표적인 공중키 암호시스템으로서는 RSA시스템이 있다[4]. 그러나 RSA 시스템은 10^{200}되는 큰 정수 연산을 필요로 하기 때문에 시간이 많이 소요되는 단점을 무시할 수 없다.

한편 공중키 암호시스템을 사용하여 중재자를 이용한 디지탈 서명시스템을 구현할 수도 있으나 이는 암호시스템의 특성에 비추어 볼 때 장점을 기대하기 어렵기 때문에 본고에서는 생략하기로 한다.

4. 관용키 암호시스템을 이용한 중재자 서명시스템

관용키 암호시스템에서는 송수신자가 동일한 비밀키를 사용하여 보통문을 암호문으로 암호화하고 암호문을 보통문으로 복호화한다.

이러한 관용키 암호시스템을 이용하는 디지탈 서명시스템에서는 동일한 비밀키를 사용하기 때문에 앞에서 기술한 당사자 서명시스템과 같이 사용할 경우에는 메세지를 위조하여 수정하고 다시 암호화해서 이를 본래의 서명된 메세지라고 허위 주장을 하거나 아예 본래의 메세지가 아니라고 할 수가 있기 때문에 송수신자 사이에 제반 분쟁의 소지가 생길 우려가 있다.

따라서, 관용키 암호시스템을 이용하는 디지탈 서명시스템은 관용키 암호시스템을 공중키 암호시스템과 비슷한 역할을 수행하도록 사용하는 방법, 메세지나 서명의 신뢰성 여부를 나중에 검증할 수 있는 자료를 제3자에게 보내어 보관하는 방법 및 중재자를 통하여 메세지나 서명을 주고 받음으로써 오직 중재자의 도움으로 서명이 만들어지거나 증명되는 방법들이 연구되어 왔다[5].

제3자가 메세지나 서명이 신뢰성있음을 표시하는 검증자료를 유지하고 있을 경우에 송수신자사이에 분쟁이 발생할 때는 수신자의 접수된 메세지와 보관하고 있는 검증자료를 비교함으로써 쉽게 송신자의 서명과 일치여부를 확인할 수 있다.

그러나 이 방법은 송수신자가 문서를 송수신하기전에 중재자에게 검증자료를 송수신하여 보관해야 되기 때문에 중재자가 많은 정보를 저장하여야 한다는 단점과 검증자료의 암호화를 위한 비밀키를 매 문서마다 다르게 사용해야 됨으로 비효율적이다.

또한, 관용키 암호시스템을 이용하는 당사자 서명시스템도 무척 복잡하고 송수신되는 정보의 양과 저장량이 너무 많기 때문에 비효율적이라고 볼 수 있다. 따라서 본고에서는 중재자를 통한 디지탈 서명방식만을 생각해 보기로 한다.

중재자 서명시스템을 이용한 관용키 암호시스템에서는 신뢰성있고 안전한 중재자를 필요로 한다. 왜냐하면, 일반적으로 중재자를 이용한 디지탈 서명방법은 송신자가 수신자에게 전송하려는 서명된 메세지를 중재자에게 먼저 보내면, 중재자는 메세지의 서명의 진위여부를 확인하고 메세지 서명확인 증명을 본래의 메세지에 첨가하여 수신자에게 전달하는 것으로 생각할 수 있다. 이는 추후 초래될 수 있는 제반분쟁을 중재자가 근본적으로 해결해야만 되는 아주 민감하고 중요한 역할을 맡게 됨으로써, 중재자는 모든 사용자에게 신뢰되고 안전해야만 하는 것이다.

이러한 중재자를 통한 디지탈 서명절차는 다음과 같이 생각할 수 있다.

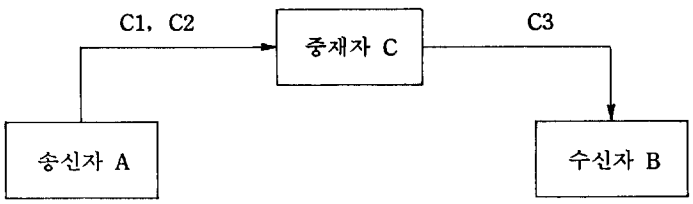
송신자는 수신자에게 보재고자 하는 메세지를 작성하고, 중요한 메세지와 메세지 내용의 요약을

추출한다. 그리고 송신자와 중재자만이 공유하는 비밀키로 메세지와 메세지 내용의 요약을 암호화해서 중재자에게 보낸다. 이때 메세지 내용의 요약에 대한 암호문은 송신자의 메세지에 대한 서명으로 취급된다.

중재자는 보내온 암호문을 복호화해서 메세지와 메세지 내용의 요약을 구하고, 메세지와 메세지 내용 요약의 일치여부를 확인할 수가 있다. 중재자는 확인된 메세지와 메세지 서명에 수신시간 및 서명확인여부를 증명하는 자료를 첨가해서 수신자와 중재자가 공유하는 비밀키로서 암호화하여 수신자에게 보낸다.

수신자는 중재자가 보내온 암호문을 복호화해서 메세지와 중재자의 메세지 수신시간 및 서명확인여부를 구하고 송신자의 메세지 서명을 보관하게 된다.

이와 같은 방법은 분쟁이 발생할 경우, 보관중인 메세지 서명 즉 메세지 내용의 요약을 송신자와 중재자가 공유한 비밀키로 암호화한 것과 본래의 메세지를 심판자에게 제출하면, 심판자는 서명을 복호화할 것을 중재자에게 지시하고 복호화된 내용과 메세지 요약의 일치여부로 쉽게 진위여부를 판가름 할 수 있다. 이와 같은 절차를 도식해 보면 그림 2와 같다.



(수신자는 C2를 서명으로 보관함)

$C1=E_{KAC}(M)$, $C2=E_{KAC}(W)$, $C3=E_{KBC}(M+C2+Time+서명확인)$

$D_{KBC}(C3)=M+C2+Time+서명확인$

E : 암호화 절차　　M : 메세지

D : 복호화 절차　　W : 메세지 M의 요약

$_{KAC}$: 송신자와 중재가가 공유하는 비밀키

$_{KBC}$: 수신자와 중재자가 공유하는 비밀키

그림 2. 관용키 암호시스템을 이용한 중재자 서명시스템

그러나 위와 같은 디지탈 서명방법은 보내고자 하는 메세지가 중재자에게 노출되므로 중재자에 대한 절대적인 신뢰성에 크게 의존하게 되는 것이다. 만일, 중재자에게 메세지를 노출함이 없이 송수신하고자 한다면 다음과 같은 방법으로 해결할 수 있다.

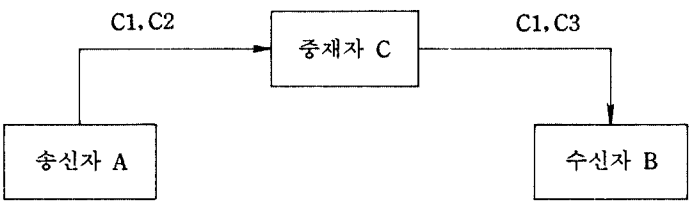
먼저, 송신자는 보내고자 하는 메세지를 송수신자만이 공유하는 비밀키로 암호화하고, 작성된 암호문에 대한 요약을 추출한다. 추출된 암호문 요약을 송신자와 중재자가 공유하는 비밀키로서 암호화한 후에 이 두가지 암호문 즉 메세지 암호문과 메세지 암호문 요약의 암호문을 중재자에게 보낸다. 이때, 메세지 암호문 요약의 암호문은 송신자의 서명으로 취급한다.

중재자는 보내온 암호문 요약에 대한 암호문을 복호화하고, 수신자에게 전달될 메세지 암호문과 복호화한 암호문 요약과의 일치여부를 확인하게 된다. 이는 중재자가 메세지 서명확인 절차를 수행하더라도 메세지 본래의 내용은 노출되지 않는 것이다. 그러나 암호문으로부터 요약을 추출하기

때문에 요약을 만드는 함수가 적합하게 선정되어야 하며 메세지의 일부가 수정되면 요약문도 변경되도록 하여야 한다.

중재자는 서명확인된 메세지 서명에 수신시간 및 서명확인을 첨가해서 수신자에게 보내고, 수신자는 메세지 암호문은 송수신자 공유의 비밀키로 적용하여 메세지를 얻고 중재자가 서명확인하여 다시 작성한 암호문은 중재자와 수신자 공유의 비밀키로 복호화하여 서명확인 여부를 판단하고 이를 보관한다.

이러한 방법을 사용하면 송신자는 서명된 메세지를 중재자에게 내용 노출없이 수신자에게 전달할 수가 있게 되는 것이다. 이를 도식해 보면 그림 3과 같다.



(수신자는 C2를 서명으로 보관함)

$C1 = E_{KAB}(M)$, $C2 = E_{KAC}(W)$, $C3 = E_{KBC}(C2 + Time + 서명확인)$

$D_{KBC}(C3) = C2 + Time + 서명확인$, $D_{KAB}(C1) = M$

E : 암호화 절차　　M : 메세지

D : 복호화 절차　　W : 암호문 C1에 대한 요약

$_{KAB}$: 송수신자가 공유하는 비밀키

$_{KAC}$: 송신자와 중재자가 공유하는 비밀키

$_{KBC}$: 수신자와 중재자가 공유하는 비밀키

그림 3. 중재자에게 메세지 내용을 노출하지 않는 관용키 암호시스템을 이용한 중재자 서명시스템

5. 복합적인 서명시스템

지금까지 살펴본 공중키 암호시스템을 이용한 당사자 서명시스템과 관용키 암호시스템을 이용한 중재자 서명시스템을 비교해 보면, 전자는 메세지의 서명이 명확하게 인증되나 공중키 암호시스템의 특성으로 인해 처리속도가 느리고, 후자는 관용키 암호시스템의 특성으로 인해 서명을 중재자를 통하여 수행함으로써 중재자의 역할비대 뿐만 아니라 통신량이 배가되는 단점이 있다.

또한 일반적으로 보내고자 하는 메세지를 서명하기 위하여 메세지 전체를 서명하는 방법보다는 메세지 요약에 대한 서명방법이 서명량이 적기 때문에 메세지는 당사자가 직접 송수신하고 서명만을 중재자를 통하도록 하는, 즉 당사자 서명시스템과 중재자 서명시스템을 절충한 복합 서명시스템을 생각할 수 있다.

이때 사용되는 암호시스템은 공중키 암호시스템과 관용키 암호시스템 모두가 사용될 수 있으나 본고에서는 관용키 암호시스템의 빠른 처리속도를 고려해서, 관용키 암호시스템을 이용한 서명방법을 살펴 보기로 한다.

송신자는 메세지를 송수신자가 공유하는 비밀키로서 암호화하여 직접 수신자에게 전송하며, 암호

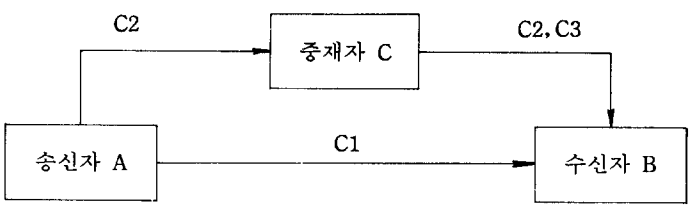
문 요약을 송신자와 중재자가 공유한 비밀키로 암호화하여 이를 서명으로서 중재자에게 전송한다.

중재자는 수신한 서명을 복호화하고 이를 다시 중재자와 수신자가 공유하는 비밀키로 재암호화하여 이를 서명 확인으로서 취급하고, 수신자에게 송신자가 보낸 서명과 자신이 작성한 서명 확인을 전송한다.

수신자는 암호문을 송수신자가 공유하는 비밀키를 사용하여 복호화하고 중재자의 서명확인을 복호화하여, 복호된 내용과 송신자가 보내온 메세지를 요약해서 일치여부를 확인함으로써 송신자의 서명을 인증하게 되며 송신자의 서명은 보관을 한다.

만일 송수신자간에 분쟁이 발생한 경우에는 중재자는 수신자가 보관한 서명과 송신자가 수신자에게 보낸 메세지를 재공받아 서명을 복호화하고 이를 메세지와 비교해서 일치여부를 판단함으로써 해결할 수 있다.

이러한 방법은 메세지에 대한 암호문이 송수신자간에 직접 송수신되므로 높은 보안성을 유지할 수가 있으면서 서명에 비하여 큰 정보량을 갖는 암호문이 중재자를 통하지 않고 송수신되기 때문에 전송비용 뿐만 아니라 시간도 절감할 수 있다. 이와 같은 절차를 도식해 보면 그림 4와 같다.



(수신자는 C2를 서명으로 보관함)

$C1 = E_{KAB}(M)$, $C2 = E_{KAC}(W)$, $C3 = E_{KBC}(W)$

$D_{KBC}(C3) = W$, $D_{KAB}(C1) = M$

E : 암호화 절차　　M : 메세지

D : 복호화 절차　　W : 메세지 M에 대한 요약

$_{KAB}$: 송수신자가 공유하는 비밀키

$_{KAC}$: 송신자와 중재자가 공유하는 비밀키

$_{KBC}$: 수신자와 중재자가 공유하는 비밀키

그림 4. 당사자 서명시스템과 중재자 서명시스템을 혼합시킨 복합 서명시스템

지금까지 몇가지 대표적인 디지탈 서명시스템의 구현방안을 제시해 보았지만 이러한 방안들은 사용되는 암호시스템이나 환경에 따라 여러가지 형태로 변형되어 응용될 수 있으리라 생각된다.

6. 문제점 및 발전 방향

디지탈 서명시스템이 컴퓨터 통신망을 이용하여 중요한 메세지를 전송할 수 있는 아주 유용한 도구임에는 틀림없으나 실용화되기 위해서는 좀더 적극적으로 관련분야에 대한 전문적인 연구와 제도적인 뒷받침이 선행되어야 한다.

첫째, 디지탈 서명시스템을 구현할 수 있는 실용성있는 공중키 또는 관용키 암호시스템의 개발이 이루어져야 한다.

당사자 서명시스템에서 활용될 수 있는 RSA 시

스템이 매우 큰 정수 연산을 필요로 하므로 메세지 전체를 암·복호화하는데 많은 시간이 소요된다는 단점을 극복할 수 있는 방안을 개발하거나, 중재자 서명시스템을 구현할 수 있는 관용키 암호시스템을 개발하여야 한다.

둘째, 비밀키의 생성, 분배 및 관리 방안 및 중재자 운용방안에 대한 연구가 필요하다.

다른 일반적인 암호시스템도 마찬가지이지만 디지탈 서명시스템은 메세지에 관련된 책임한계가 분명해야 되기 때문에 이와 관련된 비밀키의 관리 문제는 더욱 중요한 몫을 차지하게 된다. 특히, 중재자 서명시스템의 경우에는 신뢰성있고 효율적으로 운용될 수 있는 중재자를 설정하고 여러가지 비밀키를 관리하는 문제가 실용성있도록 연구되어야 한다. 이를 위해서는 IC 카드를 이용하는 하드웨어적인 해결방안도 함께 연구되어야 할 것이다.

세째, 디지탈 서명시스템을 실용화할 수 있는 관계법 제정과 제도적인 뒷받침이 선행되어야 한다.

디지탈 서명의 기본특성은 메세지 작성자를 확인하고 책임을 갖도록 하는 것이기 때문에 법적 효력을 갖을 수 있도록 이와 관련된 소프트웨어 및 하드웨어 뿐만 아니라 운용절차에 대하여 법적으로 제도적인 뒷받침이 될 수 있도록 관계법을 제정하여야 한다. 특히, 비밀키와 관련된 적절한 방안이 명시될 수 있어야 한다.

이와 같은 여러 문제점들을 해결할 수 있도록 적극적인 연구가 이루어지고 디지탈 서명시스템이 실용화된다면 정보화사회를 실현하는데 중요한 몫을 하게 될 것이다.

참 고 문 헌

1. D.E.Denning, Cryptography and Data Security, Addison Wesley, 1982.

2. S.G.Akl, "Digital Signatures : A Tutorial Survey," Computer Vol. 16 No. 2, FEB., 1983.

3. D.W.Davis and W.L.Price, Security for Computer Network, Wiley Press, 1984.

4. W.Diffie and M.Hellman, "New Directions in Cryptography," IEEE Trans. Information Theory, Vol. IT-22, No. 6, NOV., 1976.

5. C.H.Meyer and S.M.Matyas, Cryptography : A New Dimension in Computer Data Security, John Wiley, 1983.

□ 著者紹介

남 길 현(正會員)

陸軍士官學校 卒
서울工大 土木科 卒
美海軍 大學院(電算學 碩士)
위스콘신(메디슨) 州立大(電算學 碩士)
루이지아나州立大(電算學 博士)

陸軍士官學校 教授部 勤務, 現在 國防大學院 副教授