「經營情報硏究」 第6號
大韓經營情報學會
2001年 6月

전자상거래에서의 인증 알고리즘에 관한 연구

김 영 선*

〈목 차〉

Ⅰ. 서 론

최근 정보통신 및 인터넷 기술의 비약적인 발전으로 전자상거래(Electronic Commerce)가 인터넷 마케팅 또는 사이버 마케팅이라는 새로운 비즈니스 모델로 활성화되고 있다. 전자상거래를 보다 활성화하기 위해서는 전자상거래의 안전성과 신뢰성을 확보할 수 있는 보안 기술이 필수적인 선결과제이다. 전자상거래 사업의 전망이 밝은 반면에 이에 따르는 법적·제도적 환경 정비 및 고속 통신 인프라, 소비자와 기업이 안전하게 거래할 수 있는 보안체제 등이 이루어지지 않고는 인터넷 전자상거래의 발전은 어려운 상황이다. 특히, 안전한 거래 및 소비자의 지불체제가 전자상거래의 핵심과제로 등장하고 있다. 전자상거래를 위협하는 보안 문제는 다음

* 대림대학 경영정보계열 전임강사

과 같다.

첫째, 디지털 환경의 컴퓨터를 통한 거래가 이루어지므로 동일한 파일이나 데이터를 복제, 모조할 수 있다.

둘째, 인터넷은 네트워크 환경이므로 거래 당사자의 진위 여부 확인이 어렵고, 사용자의 신용카드번호, 비밀번호, 은행계좌번호, 직불카드번호 등의 금융정보가 유출될 가능성이 높다.

셋째, 하나의 거래를 위해 다수의 시스템 또는 거래와 관련 있는 사용자 및 쇼핑몰, 전자지불서버, 인증기관 등과 연계되어 있어 서로 간의 의사소통에 오류가 발생할 수 있다.

넷째, 전자상거래의 지불방법 및 소비자보호를 위한 장치가 미비한 상황이다.

인터넷을 통하여 정보를 교환하는 방법은 암호화 기법을 사용하여 발생될 수 있는 각종 위협들을 미연에 방지할 수 있도록 상호 신분 인증을 통하여 상대방과의 정확한 연결을 확인 후에 정보를 교환하여야 한다. 메시지 및 사용자에 대한 인증기능과 동시에 메시지의 전송사실을 부인할 수 없게 하는 부인방지기능을 갖는 일반적인 전자서명은 각종 보안 서비스에서 필수적으로 사용된다. 그래서, 누구나 메시지의 진위 여부를 확인할 수 있는 자체 인증기능을 갖는 일반적인 전자서명이 유용하게 사용된다[11].

본 논문은 전자상거래의 개념 및 전자상거래의 인증에 대한 알고리즘을 이해하여 체계적이고 표준적인 보안시스템을 인터넷에서 안전하게 구축하는 방안을 제시하는 데 목적을 두고 있다.

Ⅱ. 관련 연구

1. 전자상거래의 개념

전자상거래는 일반적으로 기업, 정부기관과 같은 독립적인 조직과 개인 간의 다양한 전자적 매체를 이용하여 상품이나 용역을 교환하는 것을 의미한다. 인터넷을 통한 전자상거래는 PC통신이 국내의 PC사용자만을 고객으로 확보하여 상거래를

행하는데 반해 전세계인과 시간과 장소에 관계없이 상거래를 할 수 있는 통신방법인 인터넷을 활용하므로 있으므로 주목받고 있다. 여러 선진국들에서는 이를 통한 새로운 비즈니스 환경인 전자상거래가 급속히 개발되고 있으며, 이는 종래의 컴퓨터 네트워크가 비즈니스 거래를 측면 지원하는 것과는 현격한 차이를 갖는다. 쇼핑이나 금융 등의 상거래가 컴퓨터와 네트워크의 가상 공간을 통해 공간적·시간적 한계를 벗어나 사람이 최소한으로 개입된 가운데 구현되며, 보다 빠르고 값싼 경영방식은 기업에게 위협 요인이자 동시에 새로운 기회로 다가오고 있다.

1.1 전자상거래 절차

전자상거래는 일반적으로 인터넷 쇼핑몰에서의 상품 검색부터 배달까지 일반적으로 8단계를 거쳐 이루어진다.

① 소비자는 우선 컴퓨터로 컴퓨터 통신망이나 인터넷의 가상상점에 들어가 매장을 돌아다니며 그곳에 진열돼있는 상품 가운데 원하는 것을 고른다.
② 필요한 상품을 고른 소비자가 거래 신청서를 통해 가상상점 운영자에게 팔 것을 요청하면, 운영자는 인증국에 거래 요청자가 본인이고 믿을 만한 사람인지를 가려줄 것으로 요구한다.
③ 인증국은 가상상점 운영자와 소비자의 정당성과 신용을 법적으로 보증해주는 곳으로, 국가의 관리를 받는다.
④ 인증국으로부터 소비자에 대한 신용인증이 떨어진다.
⑤ 상점 운영자는 소비자의 거래 요청을 승낙한 뒤 대금을 지불할 것을 요구한다.
⑥ 물품 대금 지불은 대부분 신용카드를 통해 이뤄지고 있으며, 가상은행에서 발생하는 전자화폐를 이용하기도 한다.
⑦ 소비자가 신용카드 번호를 입력하는 방법으로 대금 지불을 끝낸다.
⑧ 상품이 소비자에게 배달된다.

1.2 전자상거래 범위

전자상거래는 응용범위에 따라 다음과 같은 유형으로 분류할 수 있다[11].

① EDI(Electronic Data Interchange)

국제 간 또는 국내기업 간의 컴퓨터통신을 통해 표준화된 거래문서(Invoice, 주문서, 계산서)를 전자적으로 상호 교환하는 방식으로 인터넷과 무관하게 추진되어 온 것으로 표준서식을 이용하여 주로 기업 간 상거래에 활용된다.

② CALS(Commerce At Light Speed)

제품의 설계, 개발, 생산에서 유통, 폐기에 이르기까지 수명주기 전반에 관련된 데이터를 통합, 공유, 교환하여 생산성 향상을 추구하는 개념으로 동시병행적인 작업을 가능케 하며, 향후 가상기업의 모델로 발전되고 있다.

③ Cyber Business

인터넷에 홈페이지, 가상상점(virtual shopping mall) 등을 개설하여 일반소비자를 대상으로 마케팅, 판매활동을 수행하는 것으로 일반적으로 Cyber Business를 협의의 전자상거래라고도 한다.

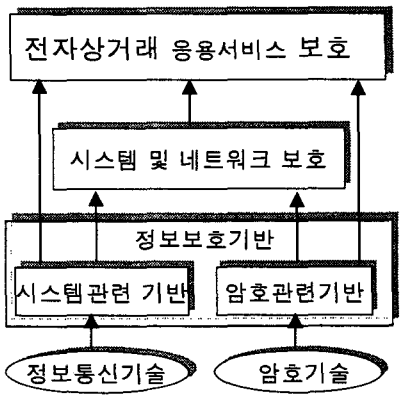
2. 전자상거래 보안

전자상거래는 통합적으로 자동화된 정보체제 환경에서 기업과 기업, 기업과 정부, 기업과 개인 등의 거래관계의 모든 측면에서 생산, 구매, 대금 지불, 수송, 행정, 서비스 등의 제반 비즈니스를 네트워크를 통해 전자적으로 행하는 것을 말한다[2].

네트워크의 발달에 따라 개방형 통신망(open network)에 있어서 각 개인이나 기업 또는 정부의 각종 정보들이 인터넷을 통하여 손쉽게 상대방에게 전달되고 있다. 이렇게 다수의 정보들을 다른 사람이 인터넷을 통하여 손쉽게 접근할 수 있다는 것을 의미한다. 웹 기술의 발달은 일반 사용자들도 이러한 정보를 쉽게 접근이 가능해짐에 따라 인증이나 개인의 사생활 및 개인정보 등의 전자상거래 보안 문제는 더욱 더 중요한 과제가 되고 있다.

전자상거래에서는 인터넷 보안 문제를 반드시 고려하고, 인터넷상의 정보보호 문제를 포함한 보안 문제를 해결하기 위한 제반 장치가 마련되지 않는다면 전자상거래의 안전성과 신뢰성을 기대할 수 없다. 이러한 정보보호 문제를 해결하기 위한 근본적인 방법 중의 하나가 네트워크상에서 송·수신 메시지나 거래 내용에 관한

정보를 암호화 및 복호화 하여 사용하여야 한다.



〈그림 1〉 전자상거래 보안 계층

전자상거래 보안 기술은 네트워크 보호, 컴퓨터 보호 기술로 구분할 수 있다. 네트워크 보호는 다중 호스트 및 네트워크상에서 인가되지 않은 노출, 변경, 파괴로부터 네트워크, 네트워크 서비스 및 네트워크상의 정보를 보호하기 위한 기술로 계층별 인터넷 통신 프로토콜, 웹 보호, 회선 보안, 전송 보안 등이 포함된다.

3. 암호 기술

암호는 고대 국가에서부터 오늘날에 이르기까지 인류와 함께 해 왔다. 특히 전쟁과 관련하여 중요한 정보를 적으로부터 보호하고 기밀을 유지시키는 보다 효과적인 작전 수행 방법으로써 많은 역할을 해 왔다. 암호화란 원래 내용을 숨긴 원본과 달라진 전달문 혹은 비밀문을 만드는 과정으로 한 문자를 다른 문자로 대체하는 일련의 규칙들의 집합이다. 이들의 규칙들은 XOR나 어떤 수학적인 기법을 통해 만들어진다. 넓은 의미에서의 암호학은 평문을 보호하기 위한 암호화 알고리즘을 연구하는 암호학과 평문을 해독하기 위하여 암호화 과정과 암호문을 연구하는 암호 해독학으로 구분된다. 암호화되지 않은 상태의 평문을 암호문으로 만드는 암호화 과정, 역으로 암호문을 평문으로 변화시키는 복호화 과정, 암호화와 복호화 과정에서 사용되는 암호화 키와 키 관리 등 정보 보호를 위한 일련의 프로세스를 암호시스템이라고 한다.

3.1 암호시스템 구분

암호시스템은 전통적으로 세 가지 독립된 영역으로 구분된다.

① 평문을 암호문으로 변환하기 위한 연산자의 유형

모든 알고리즘은 두 가지의 일반적인 원리에 기초를 둔다. 치환을 통해 평문의 각 원소(비트, 문자, 비트군, 또는 문자군)를 다른 원소에 사상시키고, 전치를 통해 평문의 원소들을 재배열시켜 근본적인 요구조건은 정보 손실을 없애는 것이다.

② 사용된 키의 수

송·수신자 양측이 같은 키를 사용하는 시스템을 대칭, 단일키, 비밀키, 또는 관용 암호방식이라고 하며, 송·수신자가 각각 다른 키를 사용하는 시스템을 비대칭, 이중키, 또는 공개키 암호방식이라고 한다.

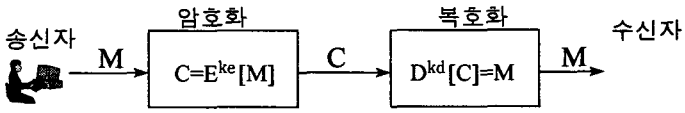
③ 평문 처리 방법

블록 암호화는 입력을 한 번에 하나의 원소 블록씩 처리하여 각 입력 블록을 생성한다. 스트림 암호화는 입력을 연속적으로 처리하여 입력이 주어지는 대로 출력을 생성한다.

3.2 암호시스템 표현

키를 사용하는 암호시스템은 〈그림 2〉와 같이 표현할 수 있다. 평문을 M, 암호문을 C, 암호화 과정은 함수 E로 간주하여 E(M)=C로 표시한다. 또한 복호화 과정은 함수 D(C)=M으로 표시한다. 암호화 키는 일반적으로 K로 표시하며, 키의 가능한 값의 범위를 키 공간이라고 한다. 여기서 Ke는 암호화에 필요한 키이며, Kd는 복호화에 필요한 키이다. 키를 고려하는 암호화 및 복호화 과정은 각각 다음의 함수로 표현할 수 있다[16].

$$Ke(M) = C,\ Kd(C) = M$$



- M : 평문
- E : 암호화알고리즘
- Ke : 암호화 키
- C : 암호문
- D : 복호화 알고리즘
- Kd : 복호화 키

〈그림 2〉 암호화와 복호화 과정

Ⅲ. 인증관련 알고리즘 방식

컴퓨터와 정보통신의 발달은 생활에 혁신적인 편리함을 제공하지만 여러 가지 부작용도 가지고 있다. 그동안의 상거래는 대면으로 이루어졌지만 이제는 전자상거래가 점차적으로 늘어나고 있다. 전자서명으로 대치되는 변화는 대면에 의한 확인을 점차 어렵게 하고 있다. 거래에서 요구되는 계약 당사자들 간의 신분 확인, 교환되는 정보의 신뢰성 등에 관한 확인이 필수적인 요소가 되었다. 이러한 문제를 해결하는 기능이 인증시스템을 통하여 이루어지고 있다.

1. 암호 알고리즘

정보교환을 위해서는 당사자 간의 합의가 필요로 하는데 이것은 정보 교환 당사자간이나 도청자의 기만을 배제하기 위한 일련의 규칙이 있어야 한다.

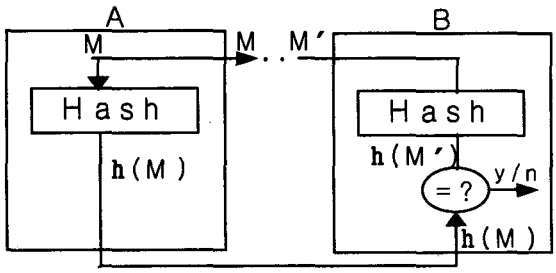
1.1 메시지 무결성(Message Integrity)

메시지 무결성은 정보가 정확하게 전달될 수 있도록 정보가 조작되는 것을 방지하는 것으로 저장 또는 송신된 메시지가 변조되었는지의 여부를 검사하는 방법과 도청자에 의해서 도청되었는지 여부를 검사하는 방법 등을 포함한다.

메시지 무결성을 신속하게 확인하는 방법으로 일방향 함수가 사용된다. 메시지 또는 메시지의 일부분은 일방향 함수의 입력이 된다. 계산된 결과는 무결성의 확인

에 사용되고 이 값은 누구나 계산할 수 있기 때문에 계산된 결과 값은 수신자에게 나누어 송신된다. 일방향 함수는 입력 값에서 출력 값을 쉽게 계산해 내지만 출력 값에서 입력 값을 추출하기는 사실상 불가능하다.

A가 B에게 메시지 M을 보낼 때 A는 메시지 M의 무결성을 확인하기 위해 h(M)을 계산한다. B는 수신된 메시지의 Hash 값을 계산하고 분리되어 수신된 h(M)과 비교하여 메시지의 무결성을 확인한다. 메시지가 도청되었다면 B는 메시지 M과는 다른 메시지 M′을 수신하게 되고 메시지 M′의 Hash 값 h(M′)은 h(M)과 다르게 계산 될 것이다[16].



〈그림 3〉 Hash 함수를 이용한 메시지

Hash 함수는 Hash 코드 h(M′)이 주어진 메시지 M의 Hash 코드 h(M)과 일치하는 메시지 M′을 생성하는 것이 실제적으로 불가능해야 한다.

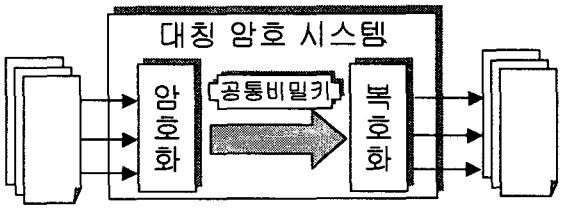
1.2 사용자 인증(Entity Authentication)

사람이나 시스템 등이 정말로 원하는 사람과 시스템이 동일한지를 검증하는 것을 의미한다. 여기서 주의할 것은 메시지 송신자와 수신자의 신분 확인이 필요하다. 메시지의 출처를 결정할 때는 사용자 인증은 대칭과 비대칭 알고리즘이 사용된다.

1.2.1 대칭 알고리즘 방식

대칭 알고리즘은 사용자 인증을 위하여 인증을 원하는 사람은 자신이 보낸. 예측할 수 없는 자료에 대하여 비밀키를 포함하는 일련의 암호 연산을 수행할 것을 상대방에게 요구하여 얻어진 결과와 자신이 수행한 동일한 암호 연산의 결과를 비교하여 정당한 사용자인지 아닌지를 결정한다. 대칭 암호 알고리즘은 메시지 처리 형

식에 따라 스트림 암호 알고리즘과 블록 암호 알고리즘으로 나누어 볼 수 있다.



〈그림 4〉 대칭 알고리즘

대칭 암호는 다시 스트림 암호와 블록 암호로 구별된다. 보호하고자 하는 데이터의 길이와 같은 길이의 키로 비트별 XOR는 방식이 스트림 암호인데, 이는 정보이론 관점에서 안전하다는 One Time Pad를 실용적인 관점으로 구현한 것이다. 스트림 암호는 키를 이용하여 매우 긴 주기를 갖는 난수열을 발생하여 평문과 비트별 XOR하는 방식이다.

① 스트림 암호 알고리즘

스트림 암호 알고리즘이란 통상 이진화된 평문과 키(이진수열)의 배타적 논리합으로 암호문을 생성하는 알고리즘을 말한다. 스트림 암호는 꼭 이진 수열 발생기만 사용되는 것은 아니고 적당한 범위의 문자열을 발생시키는 난수 발생기만 있으면 언제든지 구성될 수 있다[16].

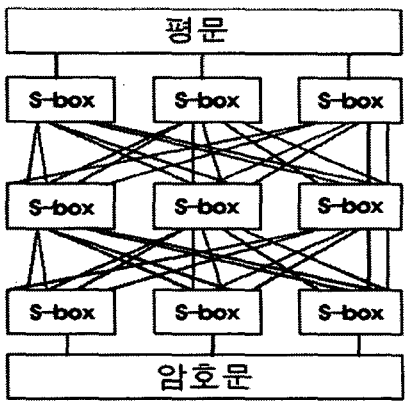
현재 스트림 암호 알고리즘은 군사 및 외교용으로 많이 사용되고 있으며, 이동통신환경에서 구현이 용이하고, 안전성을 수학적으로 검증할 수 있다는 장점으로 인하여 무선통신 데이터 보호 등에 활용된다. 스트림 암호 알고리즘은 블록 암호 알고리즘과는 달리 비교적 수학적 분석이 가능하여 여러 가지 중요한 수치(주기, 선형 복잡도 등)에 대하여 이론적인 값을 계산할 수 있다는 장점이 있다. 또한 데이터에 대한 에러 전파현상이 발생하지 않으며 하드웨어로 알고리즘을 구현하는 것이 비교적 용이하다.

② 블록 암호 알고리즘

블록 암호는 대치와 치환을 번갈아 사용하면 안전한 암호를 설계할 수 있다는

Shannon의 이론에 근거하여 설계된 것으로 암호학적으로 약한 라운드 함수를 반복적으로 사용함으로써 강한 암호를 설계한다. 블록 암호는 여러 가지 방식으로 사용할 수 있다. 블록 암호 알고리즘은 고정된 크기의 입력 블록을 고정된 크기의 출력 블록으로 변형하는 암호 알고리즘에 의해 암호화 및 복호화 과정을 수행한다. 출력 블록의 각 비트는 입력 블록과 키의 모든 비트에 영향을 받아 결정되며, 키의 크기는 암호 시스템의 빈도에 의하여 결정된다[23].

이에 대한 개념은 아래 〈그림 5〉와 같은데 대치-치환 Network라 한다.



〈그림 5〉 블록 암호 알고리즘

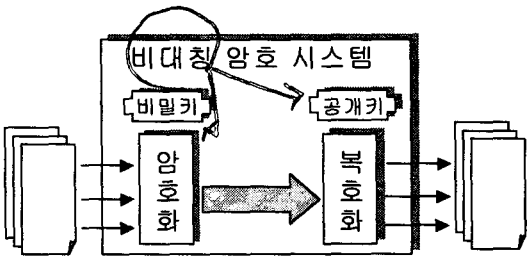
1.2.2 비대칭 알고리즘 방식

비대칭 암호는 암호화할 때 사용하는 키(비밀키)와 복호화할 때 사용하는 키(공개키)가 달라 공개키는 공개하고 비밀키만을 간직함으로써 동일한 키로 암호화와 복호화를 수행하는 대칭키 암호에서 발생하는 키 관리 문제를 효과적으로 해결하는 것이다. 또한, 암호 목적 이외에 정보화 사회의 기본 기술인 전자서명을 가능하게 하는 수단을 제공한다.

비대칭 암호가 사용되는 경우는 비밀성보다는 무결성 등에 많이 사용되고 있으며, 키 공유 또는 분배를 위한 제한적인 목적으로 암호화를 수행할 때 사용된다.

비대칭 암호 알고리즘은 〈그림 6〉과 같이 암호화할 때 사용되는 키(공개키)와 복호화할 때 사용하는 키(비밀키)를 다르게 작성하여 공개키는 공개하고 비밀키만 안전하게 유지하는 방식이다. 비대칭 암호 알고리즘이 성립하기 위해서는 암호화 과정과 복호화 과정이 역함수 관계에 있어야 하며, 암호화 과정은 비밀키를 이용하

면 누구나 계산할 수 없으며, 비밀키를 갖고 있지 않은 상태에서 공개된 정보만을 가지고 복호화 하는 것은 불가능해야 하는 조건이 있어야만 한다.



〈그림 6〉 비대칭 암호 알고리즘

비대칭 암호의 등장은 암호 응용 기술로 알려진 무결성 서비스, 부인 봉쇄 서비스, 인증 서비스 등이 가능해졌다. 또한, 대칭 암호에서는 통신쌍방 간에 비밀 통신을 하기 위해서는 별도의 채널을 통하여 키를 공유하고 관리해야 하는 번거로움이 있었으나, 비대칭 암호는 자신의 비밀키만 관리하고 상대방의 공개키는 항상 획득하여 비밀 통신을 할 수 있는 형태이므로 대칭 암호보다 키 관리에 대한 어려움이 많이 해소되었다.

2. 암호 프로토콜

정보화 사회에서는 종이 문서에 기반을 둔 기존의 모든 업무가 고도로 발달된 통신 및 정보처리기술에 의하여 전자문서에 기반을 둔 새로운 형태의 업무로 전환된다. 특별한 정보보호 목적을 얻기 위하여 두 개 또는 그 이상의 실체에 요구되는 행위를 정확하게 규정하는 일련의 단계별로 정의되는 분산된 알고리즘이다. 그러나 현재의 업무가 정보화 사회에 알맞은 전자적인 방법을 이용한 업무로 변환되기 위해서는 해결해야 할 몇 가지 문제들도 있다. 정보화 사회에서는 전자계약에서 계약당사자 간의 상대방의 신분을 확인하는 것이 개인 식별 문제, 계약문서의 내용을 확인하는 것이 인증문제, 인감도장을 전자적으로 실현하는 것이 전자서명 문제이다. 특히, 통신망을 통하여 전자적으로 동시성 문제를 해결하는 것은 매우 어려운 문제들로써 현실적으로 불가능해 보이기도 한다. 이와 같이 안전성에 관련된 많은 문제들을 해결해 주는 분야가 암호 프로토콜이다.

암호 프로토콜은 기존의 통신 프로토콜에 정보보호이론을 부가하여 고도의 정보처리 및 통신을 하는 프로토콜을 의미한다. 따라서, 암호 프로토콜은 단순히 암호알고리즘과는 달리 서로 모르는 송·수신자라도 통신망을 이용하여 서로의 목적을 이룰 수 있도록 하는 상호 통신 알고리즘을 의미한다.

3. 키분배 방식

암호기술은 특정한 암호변환(cryptographic transform)을 결정하는 파라메타들의 집합인 키로 정보를 보호하는 것을 말한다. 따라서 암호에서 효율적으로 정보를 보호하기 위해서는 키를 안전하게 관리하여야 한다. 키 관리는 키의 생성, 보관, 폐기, 그리고 분배로 나누어 생각할 수 있는데 이 중 가장 문제가 되는 것이 키를 분배하는 것이다. 키분배 방식은 크게 중앙집중형 키분배(centralized key distribution) 방식과 공개키 분배(public key distribution) 방식으로 나눌 수 있다.

중앙집중형 키분배 방식은 키분배 센터가 가입자의 요구에 의해 비밀 통신로를 통하여 암호화에 사용될 세션키(session key)를 가입자에게 분배하는 방식으로 암호화 키와 복호화 키가 동일한 대칭 암호시스템(symmetric cryptosystem)에 주로 사용한다. 키분배를 위해 각 사용자는 키분배 센터와의 통신을 위한 암호키가 유일하게 설정되어 있는 상태에서 적절한 암호 프로토콜을 통해 세션키를 확립한다. 중앙집중형 키분배 방식에서는 세션키 분배를 위한 비밀키를 사용자가 보관하고 있어야 하며 키분배 센터를 충분히 신뢰할 수 있게 키가 관리되어야 하고 키분배 센터가 마비될 경우 암호통신이 불가능하다는 단점이 있다.

공개키 분배 방식은 이산대수문제를 이용하여 고안된 공개키 개념을 도입한 것으로 공개 통신로를 통해 얻어지는 상대 가입자의 공개키(public key)와 자신의 비밀키(secret key)로 세션키의 생성이 가능하다. 공개키 분배에서는 암호키가 공개키와 비밀키로 분리되므로 비대칭 암호시스템(asymmetric cryptosystem)에 적용된다. 이 방식은 공개된 모든 가입자의 키의 저장 장소인 키 디렉토리에서 가입자 공개키의 등록, 보관, 갱신, 분배 등을 관리하며 암호 통신을 원하는 상대 가입자의 공개키를 공개된 채널을 통하여 전송할 수 있으므로, 중앙집중형 분배에서와 같은 비밀 통신로를 통한 키 전송 문제는 해결되나 분배된 공개키를 인증해야 하는 문제점이 발생한다. 하지만 모든 가입자는 키 디렉토리의 공개키를 분배받는 과정에서

적절한 암호 프로토콜을 사용하여 상대방과 상대방의 공개키를 인증할 수 있으며, 분배된 공개키와 자신의 비밀키로 암호 통신에 사용될 세션키를 공유할 수 있다.

암호 통신을 하기 위해 세션키를 얻는 과정은 중앙집중형 키분배나 공개키 분배는 비슷한 통신 복잡도(complexty)를 가지며 인증 문제를 해결하기 위한 기능이 있어야 한다. 이러한 문제점을 해결할 수 있는 방법이 개인 정보에 의한 키분배 방식이다.

Ⅳ. 인증 알고리즘 구현 사례

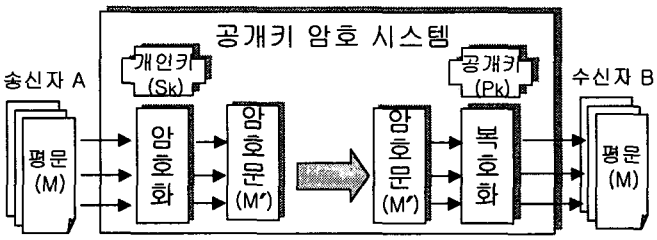
비대칭 암호 알고리즘은 대칭 암호 알고리즘의 단점인 키 관리 문제를 효과적으로 해결하였음에도 불구하고 비대칭 암호 알고리즘 단독으로 비밀성을 구현하는데는 문제점이 있다. 비밀 통신을 하고자 할 때, 통신 쌍방 간에는 난수를 발생하고 비대칭 암호 알고리즘을 이용하여 이를 안전하게 공유함으로써 키 분배에 대한 문제를 해결하고, 공유된 정보를 대칭 암호 알고리즘의 키로 사용함으로써 비밀성을 이룬다.

1. 전자서명에 의한 방식

전자서명(digital signature)은 컴퓨터의 디지털정보를 완전하게 동일한 다른 내용으로 복제가 가능하기 때문에 위조, 복제, 부인(否認) 등이 용이하다. 이런 것들을 방지하기 위해(authentication) 암호화 기법과 더불어 전자서명(digital signature) 등과 같은 추가적인 기술들이 있다. 전자서명은 일반적으로 펜과 패드가 달린 컴퓨터에서 전자펜으로 패드 위에 글씨를 써서 서명을 하면 그 이미지가 컴퓨터에 저장되는 것을 상상하는 사람들이 많다. 그러나 그 이미지 역시 디지털파일로 저장하기 때문에 마음만 먹으면 얼마든지 복사해서 동일한 이미지를 복제할 수 있는 것이다. 그러므로 이런 방식을 전자서명이라고 부를 수는 없다.

전자서명을 구현하기 위해서는 공개키 암호화 방식을 이용하는데, 공개키 암호화 방식은 암호화 키와 복호화 키가 동일하여 교환되는 정보에 대한 인증을 제공하지 못하는 대칭형 암호화 기술과 달리 암호화에 사용되는 키와 복호화에 사용되는 키

가 서로 다르다. 일반적으로 복호화 키는 공개를 하기 때문에 공개키로 정의되어지며, 암호화하는데 사용되는 키는 비밀로 간직하기 때문에 비밀키로 정의되어진다. 공개키 암호화 방식은 암호화 알고리즘 특성상 개인키로 암호화된 정보는 개인키에 대응되는 공개키를 반드시 사용하여 복호화할 수 있다[5]. 공개키 암호화 방식의 절차는 〈그림 7〉과 같다.



〈그림 7〉 공개키 암호화 방식의 절차

〈그림 7〉에서 보는 바와 같이 송신자 A는 개인키(Sk)를 가지고 평문 M에 대한 암호문을 구성하고, 수신자 B는 A의 개인키로 암호화된 M′을 받고 암호화된 M′을 복호화하기 위해서 A의 공개키(Pk)를 이용한다. 〈그림 7〉과 같은 공개키 암호화 절차과정은 결과적으로는 송신자 A가 암호화하기 위한 평문 M에 자신의 개인키를 사용하여 전자서명한 효과이다. 이와 같은 공개키 암호화의 특성 때문에 정보 인증을 위해서는 공개키 암호화 방식을 근간으로 하는 전자서명을 사용한다.

2. 전자지불 서비스

전자지불시스템은 아직 공인된 표준이나 산업계 표준이 존재하지 않은 상태에서 여러 종류의 전자지불시스템이 발표되고 있다. 대다수가 아직 스펙이나 계획만 발표하고 있을 뿐 서비스는 시작하지 않고 있는 상태이다[19].

인터넷상에서 구현되어 있는 전자지불시스템은 크게 네 가지 부류로 나누어 볼 수 있다. 먼저 이상적인 사이버스페이스 상에서의 지불 방식으로 생각되고 있는 전자 현금시스템, 신용카드 거래를 인터넷상에서 구현한 인터넷 신용카드 지불시스템, 장표결제수단 중의 하나인 수표를 인터넷상에서 구현한 전자수표시스템, 마지막으로 순전히 전자지불을 위한 시스템은 아니지만 인터넷상의 가상은행(cyberbank)을 이

용한 전자자금이체가 있다.

2.1 전자현금시스템

전자현금시스템은 수표나 신용카드 등의 다른 형태의 전자지불시스템이 실세계의 지불방식을 그대로 인터넷에 옮겨 놓은 것처럼 인터넷이라는 가상공간에서 통용되는 새로운 화폐의 발행을 목표로 만들어지고 있는 시스템이다.

2.2 인터넷 신용카드 지불시스템

신용카드 기반의 지불시스템은 두 가지로 분류할 수 있는데, First Virtual이나 CyberCash와 같이 자체 기술력을 바탕으로 하는 신용카드를 통해 전자지불을 지원하는 방법과 비자나 마스터 카드와 같이 신용카드 회사에서 직접 전자지불을 지원하는 방식이 그것이다. 신용카드 역시 실세계의 신용카드 지불 절차와 동일하게 이뤄지는데, 따라서 소액 거래보다는 신용카드 한도액을 넘지 않는 범위내에서 transaction 비용을 상회하는 상당한 정도의 금액 거래시 적당하다.

2.3 전자수표시스템 전자수표

현실세계에서 사용되고 있는 종이로 된 수표를 그대로 인터넷상에 구현하고 있다. 전자수표의 사용자는 은행에 신용계좌를 갖고 있는 사용자로서 제한된다. 이 시스템은 발행자와 인수자의 신원에 대한 인증을 반드시 해야 하는 문제를 갖고 있다. 여기에 여러 가지 보안 기법들이 사용되고 있는데 이 때문에 transaction비용이 많이 들 수밖에 없다. 그러나 전자수표는 상당히 큰 액수의 거래, 기업간의 상거래의 지불 수단으로서 적합하며, 종이로 된 실세계의 수표보다는 처리비용이 적기 때문에 종이수표를 쓰는 것보다는 적은 액수의 지불에서도 사용이 가능하게 될 것이다.

2.4 전자자금이체

인터넷상의 가상은행은 최근 웹기반으로 생겨나고 있다. 가상은행은 물리적인 지점, 본점을 운영하지 않고 모든 것을 웹상에서 사용자와 인터페이스 함으로써 운영되는 은행을 말한다. 전자자금이체를 이용한 지불방식은 현재도 홈뱅킹이나 ATM으로도 가능하다. 가상은행이 홈뱅킹이나 ATM보다 편리한 점은 좀더 넓은 서비스

를 시간, 공간의 제약 없이 받을 수 있다는 데 있다. 또 인터넷을 이용한 프로세스 처리가 무척 값싸기 때문에 수수료가 훨씬 적거나 없다는 점이 우수하다.

V. 결 론

정보화 사회에서 기존의 상행위 개념을 뒤바꿔버린 전자상거래(Electronic Commerce)의 열풍은 엄청난 상업적 기대를 보장받고 있으며 이는 세계에서 가장 큰 서점이 인터넷상에 존재한다는 현 시점의 실례를 들지 않더라도 조만간 기업 활동 그 자체의 변혁을 가져올 것이 확실한 것이다.

전자상거래가 활성화될수록 인터넷의 생활화가 필연시 되어 안정된 정착화 및 활성화에 필요한 보안문제 등 기술적 대책 및 발전이 시급하다는 것이다. 전자상거래 전반에 걸쳐 정보보호가 필요하지 않은 곳이 없다고 해도 지나치지 않을 정도로 핵심적인 요소이고 적절한 정보보호 장치가 없다면 전자상거래 자체가 존재하기 어렵다. 이러한 전자상거래를 충족시키기 위해서 메시지 및 사용자에 대한 강력한 인증이 필요하다.

본 논문에서는 메시지 및 사용자에 대한 인증기능을 제시한 인증 알고리즘에 대한 이해를 증가시키고, 전자상거래의 거래 정보나 거래 내용들의 안전성과 신뢰성을 도모하기 위한 것이다. 또한, 암호기술을 이용하여 무방비로 노출되었던 통신시스템의 보안 및 정보보호의 신뢰성을 주었다. 또한, 전자상거래의 성공은 인터넷 사용자의 개인정보나 결재정보 등을 보호하여 인터넷 판매에 대한 신뢰를 얻을 수 있도록 하는 인증 알고리즘 구축의 필요성을 인식했다. 향후, 전자상거래의 보안이 수준 높은 암호 인증 알고리즘을 개발하여 효율적이고 향상된 기법 제시의 연구가 이루어져야 할 것이다.

참 고 문 헌

1. Ford Warwick & Baum, M.S., *Secure Electronic Commerce*, Prentice-Hall, 1997.
2. A. Froomkin, *The Essential Role of Trusted Third Parties in Electronic Commerce*, Ver. 1.02 Oct, 1996.
3. Cameron Debra, *Electronic Commerce*, Computer Technology Research Corp., 1997.
4. Cameron Debra, *Security Issues for the Internet and the World Wide Web*, Computer Technology Research Corp., 1997.
5. William Stallings, *Network And Internetwork Security Principle And Practice*, Prentice-Hall, Inc., 1995.
6. T. Elgamal, "A Public Key Crytosystem and a Signature Schema based on Discreate Logarithm," *IEEE trans. on Information Theory IT-31*, pp. 467~472, 1995.
7. Mark Greene, *Role of Cretificate Authority in Internet Commerce*, 1997. 5
8. Albrecht Beutelspachar, *Cryptology, Mathematical Association of America*, 1994.
9. Peter Wayner, *Disappaearing Cryptography*, 1996.
10. 한국전산원, 전자상거래를 위한 보안기술 체계 및 요소기술에 대한 이해에 관한 보고서, 1999.
11. 홍학표, "전자상거래에서의 보안 기법에 관한 연구," 성균관대학교 석사학위논문, 1999. 6.
12. 안용광, "암호화 방법에 관한 연구," 대전대학교 석사학위논문, 1999. 4.
13. 강영구 · 류성열, "전자상거래 보안을 위한 YK2 암호 알고리즘의 설계," 한국정보처리학회 논문지 제7권 10호, pp.3138~3147, 2000.
14. 조인준 · 정회경 · 김동규, "인터넷 보안 메커니즘에 관한 연구," 통신정보보호학회, Vol. 8, No. 2, pp.19~35. 1998. 6.
15. 김홍근 · 최영철, "전자상거래 정보보호기술 현황 및 대응방안," 정보처리학회지

Vol. 6, No. 1, pp.22~34. 1999. 1.
16. 육군사관학교 수학과, 암호학 개론, 경문사, 2000.
17. 한국전자통신연구원, 암호학의 기초, 경문사, 2000.
18. 서광석 · 양희선 · 김대열 · 권승탁 · 박증수, 암호와 대수곡선, 북스힐, 2000.
19. 이만영 · 김지홍 · 류재철 · 송유진 · 염흥열 · 이임영, 전자상거래 보안 기술, 생능출판사, 1999.
20. URL: http://wwwcs.dongguk.ac.kr/~dh999/Security/
21. URL: http://www.software.or.kr/javalab/
22. URL: http://www.kisa.or.kr/K_trend/KisaNews/
23. URL: http://www.kisa.or.kr/sysevaluation/menu1/
24. URL: http://cjhae.posville.co.kr/main.html/
25. URL: http://www.koraa.or.kr/junggi/contents92/
26. URL: http://www.kisa.or.kr/K_trend/KisaNews/

Abstract

A Study of Authentication Algorithm in Electronic Commerce

Kim, Young-sun

Partial transactions which use computer networks are formed in the cyberspace due to rapid progress of communication and computer technology. Electronic business transactions have security problems according to the special quality of opening networks, while it can be approached easily by anyone without being tied to time and places through Internets. To revitalize the electronic business transactions, security technology which can establish its security and trust is the prior task and both safe information communication and better information security service offer are essential factors.

The method to exchange information through Internets must be made after confirming one another's exact connection in the mutual identity certification to prevent a lot of threat which can occur in the use of password techniques. To satisfy these electronic business transactions, we intend to increase understanding of authentication algorithm provided with authentication function of messages and users as well to plan safety and trust of business information and contents in the electronic business transactions.