정보보호에서의 기술적 보안(암호화 기법)

2005. 10. 25(火)
의료관리학교실
곽미숙

1. 서론

다양한 분야의 정보화가 급속도로 진전되면서 국내외적으로 개인정보보호에 대한 관심이 높아지고 있는 가운데, 해킹, 바이러스 침해, 개인정보 유출 등 정보화 역기능의 가능성이 커지면서 각종 정보의 불법적인 유출, 변조, 파기 등을 방지하기 위한 정보보호는 고성능 컴퓨터와 초고속 통신망에 기초한 정보 시스템을 운영하는 조직들에게 필수적인 사항으로 인식되고 있다.

의료분야도 마찬가지로 정보화가 가속화되면서 대부분의 환자 의료 정보들이 디지털화된 형태로 저장, 관리되고 있을 뿐만 아니라, 의료기관의 일상적인 진료 업무 외 경영관리, 보험청구 등 모든 영역의 업무를 수행하기 위해 컴퓨터를 활용하여 각종 정보를 수집하고 관리·이용하고 있어 환자의 개인정보와 의료 정보보호 문제들이 주요 이슈로 부각되고 있는 실정이다. 또, 최근 의료기관간 의료 협력 정보망의 발달, 전자의무기록 시스템 도입의 확산과 EHR(Electronic Health Record)로의 발전, 인터넷을 통한 고객관계관리 (CRM: Customer Relationship Management)의 확산 등으로 인해 인터넷을 통한 의료정보의 전송이 빈번해지고 있으며 향후에도 인터넷을 통한 정보 교환은 더욱 증가할 것으로 예상됨으로써, 정보화에 따른 개인정보보호에 많은 관심을 가지게 되었다.

따라서, 여기에서는 정보보호의 일반적인 내용에 대해 살펴보고, *정보보안의 3가지 측면(기술적 보안, 관리적 보안, 물리적 보안) 중 기술적 보안으로써 가장 널리 알려지고 쓰여지고 있는 정보통제 방법인 암호화 기법*에 대해 살펴볼 것이다.

2. 정보보호의 개요

가. 정보보호의 정의

(1) 정의

정보보호는 국가별로 여러 가지 형태로 정의되고 있는데, 우리나라의 경우에는 정보화촉진기본법 제 2조에 '정보의 수집, 가공, 저장, 검색, 송신, 수신 중에 정보의 훼손 변조 유출 등을 방지하기 위한 관리적 기술적 수단을 강구하는 것'으로 정의하고 있고, 정보보호진흥원(KISA)의 전문용어집에서는 '정보의 수집·가공·저장·검색·송신·수

신 도중에 정보의 훼손·변조·유출 등을 방지하기 위한 관리적·기술적 수단 또는 그러한 수단으로 이루어지는 행위. 내·외부의 위협요인들로부터 네트워크, 시스템 등의 H/W와 S/W, 데이터베이스, 통신 및 전산시설 등 정보자산을 안전하게 보호·운영하기 위한 일련의 행위'라고 정의하고 있다.

(2) 정보보안 vs 정보보호의 개념

'information security'는 정보보호 또는 정보보안을 의미하는데, 정보보안은 사람에 의하여 고의적으로 발생하는 정보의 유출, 파괴, 변조에 대한 대응을 강조하며, 정보보호는 고의적인 침해뿐만 아니라 우연히 발생하는 자연재해나 사람의 실수에 의한 침해에 대한 대응도 포괄하는 포괄적인 용어이다(김세헌, 정보보호 관리 및 정책, 생능출판사, 2002). 국내 관련 학계에서는 security라는 용어가 information과 결합될 때는 정보보안이라는 용어보다는 정보보호라는 용어를 주로 사용하며, 정보보호기술 표준용어로는 정보보호가 사용되고 있다(http://www.kisa.or.kr/standard/word_search).

(3) 보안이란?

보안은 크게 *기술적 보안과 물리적 보안, 관리적 보안*으로 나누어서 설명할 수 있다. 기술적 보안은 개인정보의 보호와 접근 제어에 사용되는 기술, 정책, 절차 등의 기술적 정보보호를 의미하고, 물리적 보안은 대상기관의 정보시스템 및 관련 건물, 장비들을 자연 재해나 환경적 위험요인, 불법적인 침입으로부터 보호하기 위한 물리적인 수단, 정책, 절차를 의미한다. 관리적 보안은 개인정보를 보호하기 위해 필요한 보안 수단의 선택, 개발, 실행(implementation), 유지보수에 관한 사항과 대상 기관 인력의 정보보호와 관련한 행위를 관리하기 위한 관리적인 행동, 정책, 절차를 말한다.

나. 정보보호의 3가지 요소

다양한 위협으로부터 정보를 보호하기 위해서는 *정보보호의 기밀성, 무결성, 가용성의 3가지를 유지하고 보장*하여야 한다. 기밀성(confidentiality)이란 접근이 인가된 사람만 정보에 접근할 수 있도록 보장하는 것이고, 무결성(integrity)이란 정보와 정보처리 방식의 정확성과 완전성을 보장하는 것으로써, 데이터나 소프트웨어가 마지막으로 인가된 상태 그대로 유지되어 있는 것을 말한다. 기밀성과 무결성은 서로 밀접한 관계를 가지는데, 기밀성은 데이터나 소프트웨어에 대한 불법적인 접근(access)에 관한 문제이며, 무결성은 이들에 대한 불법적인 쓰기(writing)에 관한 문제이다. 가용성(availability)은 인가된 사용자가 필요할 때에는 정보 및 이에 관련된 자산에 접근 할 수 있는 것이 보장되는 것으로써, 정보보호에만 국한된 개념은 아니며, 모든 물리적인 자산들의 분야에서도 사용하고 있는 개념이다.

다. 정보보호의 대상

한 조직의 자산은 그 조직에게 가치가 있으며, 따라서 조직이 보호하여야 하는 모든 것들을 의미한다. 자산의 적절한 관리와 관리 책임 규명은 조직의 자산에 대한 적절한 보호를 유지하기 위하여 필수적인 사항이다. 정보보호에서 고려하여야 할 자산으로는 데

이터베이스, 데이터 파일, 시스템 문서, 사용 안내서, 교육훈련 자료 등의 *정보자산*과 응용 소프트웨어, 시스템 소프트웨어, 개발 툴 및 유틸리티 등의 *소프트웨어 자산*, 컴퓨터 기기, 통신 장비, 저장장치, 기타 기술적 장비들을 포함하는 *물리적 자산*, 전산처리 및 통신 서비스 등의 *서비스* 등이 있다.

라. 정보보호의 위험요소

정보보호의 위험요소로는 손실이나 해를 초래하기 위해 활용할 수 있는 보안 시스템의 *취약점(vulnerability)*, 예를 들어 물리적 통제의 결여, 패스워드의 잘못된 선택 및 사용, 외부 네트워크와의 보호되지 않은 연결, 문서의 보호되지 않는 저장(암호화 되지 않은 저장), 충분하지 못한 정보보호 교육훈련 등을 들 수 있다. 또 손실이나 해를 초래할 수 있는 잠재력을 지닌 *위협(threat)*이나 취약점을 이용하여 침투를 시도하는 능동적 또는 수동적 *공격(attack)*등이 여기에 속한다. 위협을 일으키는 주체로는 해커, 산업 스파이 등의 *외부인*과 내부직원, 외부 용역회사 직원, 외부 컨설턴트 등의 *내부인*으로 나눌 수 있는데, 실제로 정보시스템에 주된 위협을 주는 사람은 내부인에 의한 것이 많다.

마. 보안통제방안

정보보호의 통제방안에는 접근통제, 암호화, 내부자에 의한 통제, 인터넷 정보보호 등이 있는데, 가장 중요한 통제방안은 정보에 대해 인가된 사람만 접근을 허용하고 인가하지 않은 사람에게는 접근을 허용하지 않는 접근통제(access control)이다. 접근 통제는 정보시스템에 대한 신체적인 접근을 통제하는 물리적인 접근통제 방식과 정보시스템에 대한 접속을 통제하는 접근통제 방식이 있다. 컴퓨터가 네트워크로 연결되기 전에는 물리적 통제방식이 매우 효과적이었으나, 현재와 같은 사이버 세상에서는 ID/password, smart card, PKI, 지문인식, 홍채 인식 등의 정보시스템에 대한 접속을 통제하는 접근통제가 중요한 이슈가 되고 있다. *접근통제와 더불어 또 하나의 중요한 통제 방안은 암호법이다. 조직이 가지고 있는 접근 통제 기능이 뚫렸을 경우에도 정보를 보호할 수 있는 기술로서 불법적으로 정보를 습득한 사람이 해독하지 못하도록 하는 것이다. 이것은 3장에서 자세하게 다루어진다.* 내부자에 의한 통제로는 접근 통제와 더불어 정보보호 수칙 준수에 대한 모니터링과 불법적인 행동을 하지 못하도록 하는 적절한 교육과 훈련 등이 있다. 인터넷 정보보호는 방화벽이나, 침입차단시스템, 침입방지시스템 등이 있다.

3. 암호화 기법

가. 역사와 기본 용어

(1) 역사

암호법은 인류 역사상 수 천년 전부터 사용되어져 왔다. 고전적인 암호방식은 줄리어스 시저의 시저 암호(Ceaser cipher), 제 2차 세계 대전 시에 사용된 독일의 ENIGMA, 미국의 M-209등으로 주로 알파벳의 위치를 바꾸거나(transposition) 또는

다른 부호로 대치하는(substitution) 방법을 사용하였다. 이후 컴퓨터의 발전으로 인하여 모든 정보가 0과 1의 나열로 이루어진 이진파일(binary file)의 형태로 저장되고 전송됨으로써 이진파일을 암호화하는 방식이 사용되게 되었다. 그러던 중 1976년에 기존의 암호법과는 전혀 다른 공개키 암호법(public key ciphers)이라는 새로운 암호법이 등장하면서부터 암호학(cryptography)은 정보를 암호화하는 데에만 사용되는 것이 아니고, 매우 중요한 새로운 여러 응용 분야에 사용될 수 있게 되었고, 공개키 암호법의 다양한 응용 분야 중에서 가장 중요한 전자서명(digital signature)을 가능하게 하였다.

(2) 기본 용어

(가) 평문(plaintext, cleartext): 암호화 되지 않아, 읽을 수 있는 문장

(나) 암호문(ciphertext): 암호화되어 읽을 수 없는 문장

(다) 암호화(encryption, encipherment): 평문을 암호문으로 바꾸는 과정

(라) 복호화(decryprion, decipherment): 암호문을 평문으로 바꾸는 과정

(마) 암호기술(crytography): 메시지를 안전하게 유지하는 기술과 학문

(3) 암호화 알고리즘

암호법마다 사용하는 알고리즘이 다르고 사용하는 키도 다르다. 과거에 컴퓨터가 등장하기 이전의 암호법은 알고리즘과 키를 모두 비밀로 유지함으로써 암호문의 비밀을 유지하는 방법을 사용하였는데, 이것을 비밀키 또는 대칭키, 관용 암호 알고리즘이라고 한다.

컴퓨터가 사용되는 현대의 암호법에서는 키의 비밀성만을 통하여 암호문의 비밀성을 유지하며 알고리즘의 비밀성은 보유하지 않는다. 현대 암호법에서는 알고리즘은 아예 공개하며 이 알고리즘에 사용된 키의 비밀성만을 송/수신자 간에 유지함으로써 암호문이 비밀성을 보장하도록 하는데, 이것을 공개키 혹은 비대칭키 암호 알고리즘이라고 한다. 따라서, 공격자가 알고리즘을 알고 있어도 키를 모르면 암호문을 복호화할 수 없는 기능을 가진 암호 알고리즘을 사용한다는 것이다.

나. 대칭키 암호법(비밀키, 단일키 암호법)

(1) 암호화 방식

그림 1은 대칭키 암호법(symmetric cryptosystem)의 암호화 방식을 보여주고 있다. 이 암호법은 비밀키 암호법(secret-key cryptosystem) 혹은 단일키 암호법(single-key cryptosystem, one-key cryptosystem)으로 불리며, 암호문은 공개된 채널에서 전달하고, 비밀키는 안전한 채널로 공유하는 방법으로 다음과 같은 암호 알고리즘을 거친다.

공개 시스템(open system)인 인터넷은 암호법을 사용하지 않는 한 비밀성이 보장되지 않기 때문에, 송/수신자는 사용할 알고리즘과 키를 미리 결정하여야 한다. 이때 이들은 사용할 알고리즘은 공개적으로 결정할 수 있지만, 사용할 키는 두 사람 이외에는 알 수 없도록 보장된 비밀 통신 채널을 이용하여 결정하여야 한다. 이렇게 키를

교환한 후에 송신자는 평문 M과 비밀키 K를 암호화 알고리즘 E에 입력하여 암호문 C를 만들고, 이 암호문 C는 안전하지 않은 통신 시스템(공개된 채널)을 통하여 수신자에게 전달된다. 수신자는 암호문 C와 비밀키 K를 복호화 알고리즘 D에 적용하여 평문 M을 만들어 메시지를 확인할 수 있다.

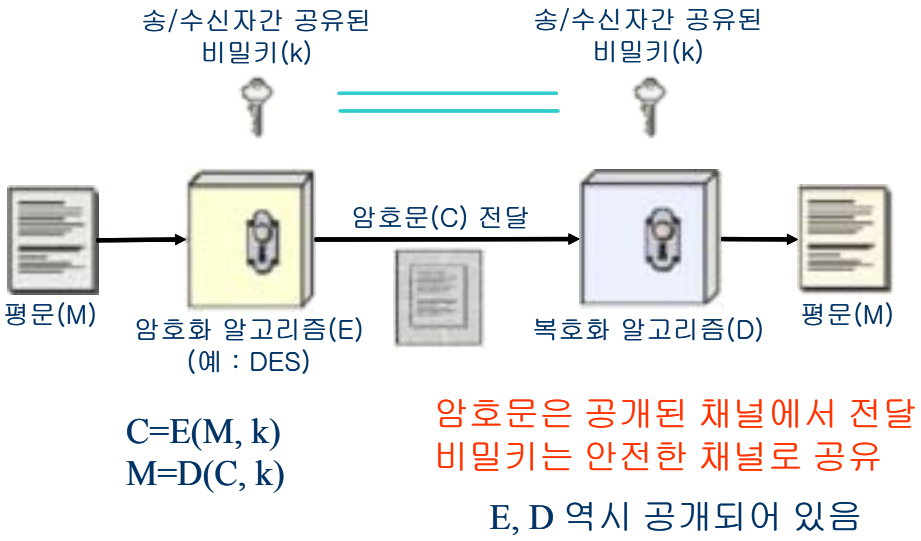

그림 1. 대칭키(비밀키, 단일키) 암호법

(2) 특성

대칭키 암호법의 경우, 기밀성(Confidentiality)과 무결성(Integrity)을 보장한다. 전송 내용의 비밀성을 보장할 뿐만 아니라, 키를 모르는 사람은 평문으로 복구될 수 있는 암호문을 만들 수 없으므로 중간에 다른 사람에 의해 변조되지 않은 것이라는 사실이 확인 가능하다. 그러나, 키를 공유하는 송/수신자가 어떤 계약을 위해서 계약서를 암호문으로 작성한 경우, 추후 분쟁이 생겼을 때 이 암호화된 계약서를 누가 만들었는지 입증할 수 없다. 즉 전자서명의 기능이 없다는 것이다.

다. 공개키 암호법(비대칭키 암호법)

(1) 암호화 방식

그림 2와 3은 공개키 암호법의 암호화 방식을 보여주고 있다. 이 암호법은 비대칭키 암호법(dissymmetric cryptosystem)으로도 불리며, 대칭키 암호법과 달리 평문을 암호화하는 데에 사용하는 키와 암호문을 평문으로 복호화하는 데에 사용하는 키가 서로 다르다. *각 개인은 개인키(private key)와 공개키(public key)를 가지고, 개인키로 암호화 하면 공개키로 복화화하고, 공개키로 암호화하면 개인키로 복호화하여 메시지를 확인할 수 있다.* 따라서, 복호화 키를 모르는 사람이 암호문에서 평문을 구해낼 수 없고, 두 개의 키는 서로 다르며 둘 중 하나를 알고 있을 때 나머지 하나를 알아내는 것이 현실적으로 불가능하다.

(가) 기밀성을 보장하는 암호기술

그림 2는 공개키 암호법을 이용한 비밀 통신을 보여주고 있다. 그림에서 Bob과 Alice는 각각 공개키와 개인키를 가지고 있다. 공개키 암호법에서 모든 사람들은 자신의 암호화 키(공개키)는 공개하고, 복호화 키(비밀키, 개인키)는 비밀로 한다. 공개키는 통신망의 모든 사람들에게 공개된다.

만일 그림 2에서와 같이 Bob이 Alice에게 평문을 비밀로 보내고자 한다면, Bob은 공개된 Alice의 공개키를 찾아서, Alice의 공개키를 암호화 알고리즘에 입력하여 메시지를 암호화 한다. 이렇게 암호화된 메시지는 비밀이 보장되지 않은 통신망(공개된 채널)을 통하여 Alice에게 전달되고, Alice는 암호를 자신만이 알고 있는 개인키를 복호화 알고리즘에 입력하여 평문을 얻어서 메시지를 확인하게 된다. *이 암호법의 경우, 전송 도중에 제 3자가 암호문을 도청하였다 하더라도, 그는 복호화 키(Alice만이 알고 있는 Alice의 개인키)를 모르기 때문에 평문을 알아내지 못한다. 즉, 전송 내용의 비밀성을 보장할 수 있다.*

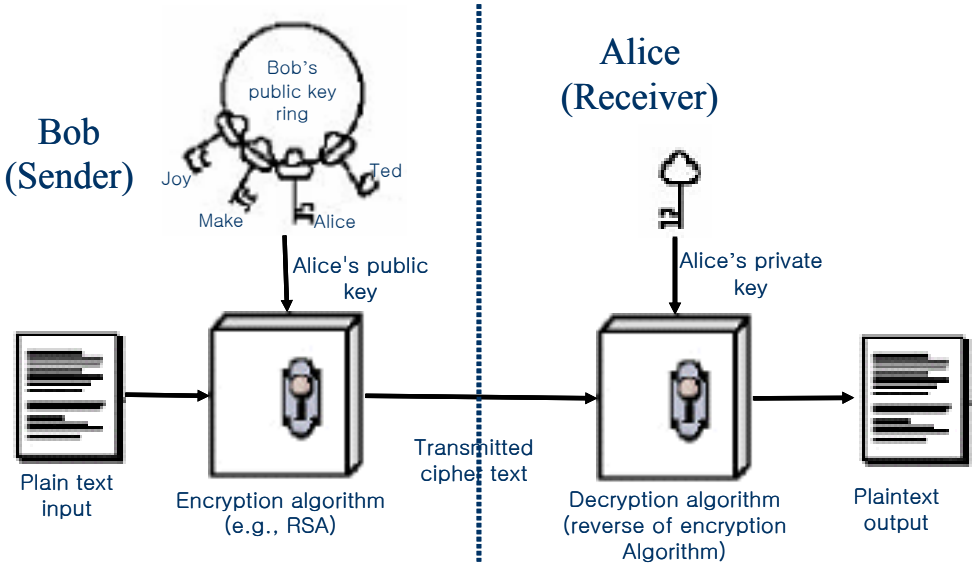

그림 2. 공개키 암호법의 기밀성 보장

(나) 인증(Authentication)을 가능하게 하는 암호기술

그림 2에서 설명하고 있는 암호법은 내용에 대한 인증을 전혀 보장하지 못한다. Alice의 공개키는 누구나 알 수 있는 것이기 때문에, Bob이 보낸 평문이라는 것을 입증해 주지 못하고, 수신된 메시지가 전송 도중에 다른 사람에 의해 변조된 것이 아니라는 무결성을 보장해 주지 못한다.

그러나, 그림 3에서와 같이 Bob이 Alice에게 평문을 보낼 때, Bob이 자신의 비밀키(개인키)를 암호화 알고리즘에 입력하여 메시지를 암호화하여 공개된 채널로 암호문을 전달하고, 이를 수신한 Alice가 Bob의 공개키를 복호화 알고리즘에 입력하여 평문을 얻어낸다고 한다면, *메시지에 대한 인증과 무결성을 보장할 수 있다. 그러나, 이*

암호법에서는 기밀성은 보장되지 않는다. Bob의 공개키는 모든 사람에게 공개되어 있기 때문에, 누구나 메시지를 복호화하여 읽을 수 있다.

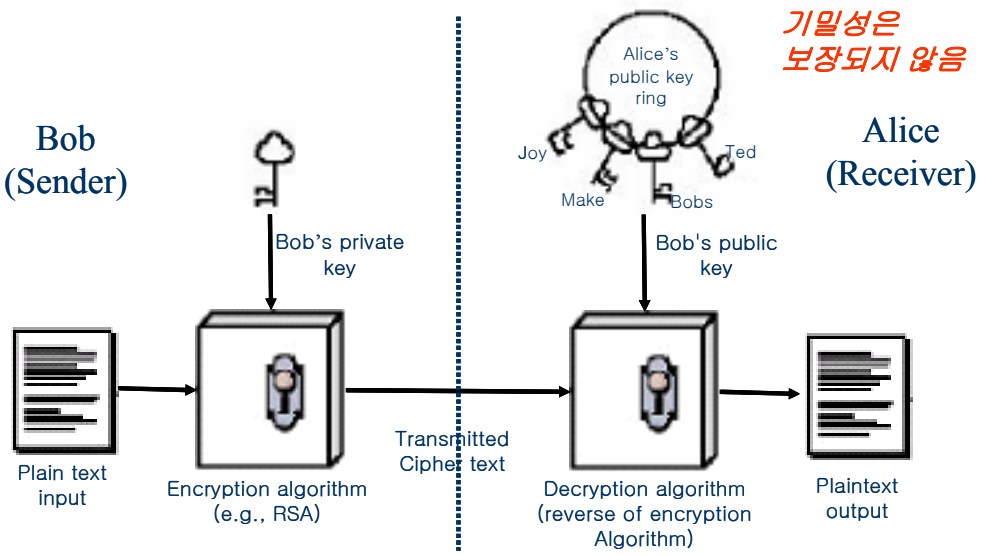

그림 3. 공개키 암호법을 이용한 메시지 인증

(다) 이중 암호화

그림 4에서 설명하고 있는 공개키 암호법은 그림 2와 3에서 설명한 공개키 암호법의 단점을 모두 보완한 방법으로 메시지의 기밀성과 메시지 내용의 인증, 무결성을 모두 보장해주는 이중 암호화 법이다. 먼저 송신자 A는 평문을 자신의 비밀키(개인키)로 암호화하고, 다시 B의 공개키를 이용하여 암호화 한 암호문을 작성하여 전송한다. 이 암호문을 받은 B는 자신의 비밀키(개인키)로 복호화 하고, 다시 A의 공개키로 복호화 과정을 적용하여 평문을 읽는다. 즉, 이용자 A의 공개키로 복호화가 가능한 경우에 분명히 A로부터 온 정보라는 것을 확인할 수 있고, 이용자 B의 공개키로 암호화하였으므로 B만이 복호화가 가능하여 기밀성이 보장된다.

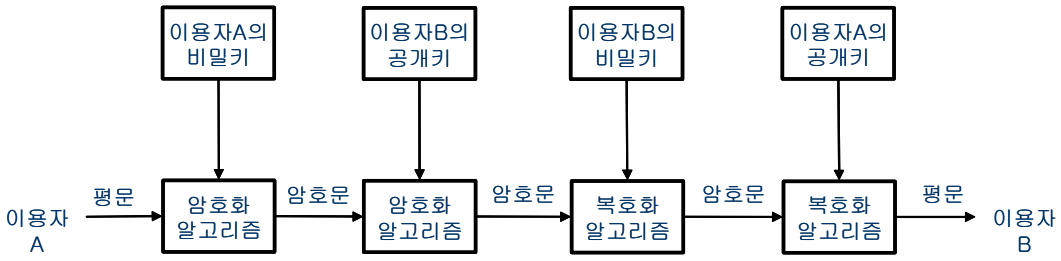

그림 4. 공개키 암호법을 이용한 비밀성 보장 및 메시지 인증

(2) 대칭키 암호법과 공개키 암호법의 비교

공개키 암호법을 이용하면 대칭키 암호법이 가지고 있는 키 관리의 문제를 해결할 수 있다. 대칭키 암호법은 통신망에 있는 각 쌍 당 하나의 키가 필요한 것과 달리 공개키 암호법은 각 개인 당 두 개의 키를 필요로 한다. 만일 N명의 사람들이 있는 통신망에서 모든 쌍 끼리 비밀 통신을 가능하게 하려면 대칭키 암호시스템에서는 N(N-1)/2 개의 키를 비밀키로 관리해야 하지만, 공개키 암호시스템에서는 N개(자신의 개인키)의 키만을 비밀로 유지하면 된다. 더욱이 대칭키 암호시스템에서는 하나의 키를 두 사람에게 비밀리에 전달해야 하는 문제를 가지고 있는 반면에 공개키 암호시스템은 각 개인의 공개키는 공시하고, 비밀키만을 비밀로 가지면 된다. 주로 대칭키 암호시스템은 메시지를 암호화 할 때 사용하고, 공개키 암호시스템은 전자서명에 많이 사용한다.

표 1. 대칭키 암호시스템과 공개키 암호시스템의 비교

구분	대칭키	공개키
작업을 위한 요구사항	수신자와 송신자는 알고리즘과 키를 공유해야 함	공개키는 모두에게 공유하고, 자신만의 비밀키는 사용자만이 보관
필요한 키의 개수 (비밀로 유지해야 하는 키)	N(N-1)/2	N
키 분배 방법	비밀스럽게	공개적으로
전자서명	구현 불가능	구현 가능
사용분야	메시지의 암호화	전자서명

라. 전자서명

(1) 전자서명이란?

공개키 암호법은 전자적인 문서에 대한 서명의 기능으로 사용할 수 있다. 해쉬함수와 공개키 암호기술을 이용하여, 전자서명 생성키(개인키)와 전자서명 검증키(공개키)의 쌍으로 이루어진다.

(2) 암호기술(해쉬함수)

암호학적 해쉬 알고리즘(secure hash algorithm)은 임의의 유한 길이의 입력값을 고정된 크기의 출력값으로 바꾸는 함수로써, 이때의 출력값을 해쉬값(hash value) 혹은 메시지 다이제스트(message digest)라고 한다. 메시지의 인증(authentication) 혹은 무결성(integrity)을 만족시키기 위해 사용된다.

(3) 전자서명의 원리

그림 5에서 설명하고 있는 전자서명의 원리는 다음과 같다. Alice가 전달하고자 하는 원본문서를 해쉬함수를 이용하여 메시지를 축약/해쉬값을 얻은 후, 해쉬값을 나(Alice)의 개인키로 암호화한 후, 암호화한 서명값(전자서명)을 원본문서에 추가하여 전달한다.

문서를 수신한 Bob은 원본문서와 서명값을 분리하여, 서명값을 Alice의 공개키로 복호화하고, 원본문서를 해쉬함수를 통해 해쉬값을 얻어, 얻어진 해쉬값과 복호화된 값을 비교한다. 만일, 두개의 값이 같다면, 임의로 위변조 되지 않았다는 것을 말합니

다.

이로써, Alice의 공개키로 복호화하였기 때문에 Alice가 보낸 메시지라는 것을 인증할 수 있고, 비교된 해쉬값이 같다면, 문서의 무결성도 보장될 수 있는 것이다.

의료에서의 전자서명의 활용분야는 전자 건강보험증, 전자 차트, 처방전 등이 있을 수 있겠다. (참고 site: 전자서명인증관리센터 http://www.rootca.or.kr/)

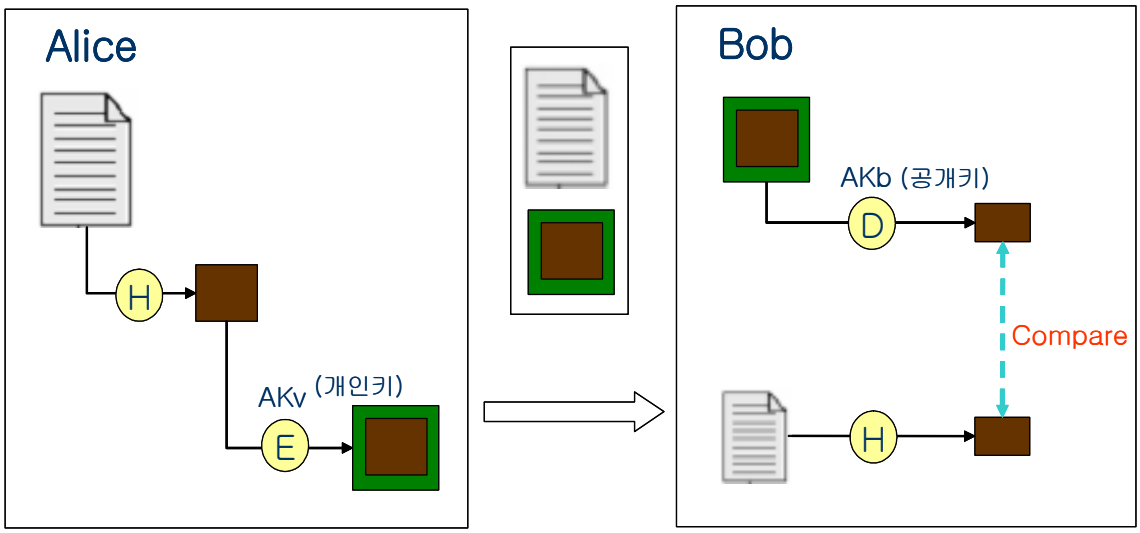

그림 5. 전자서명의 원리

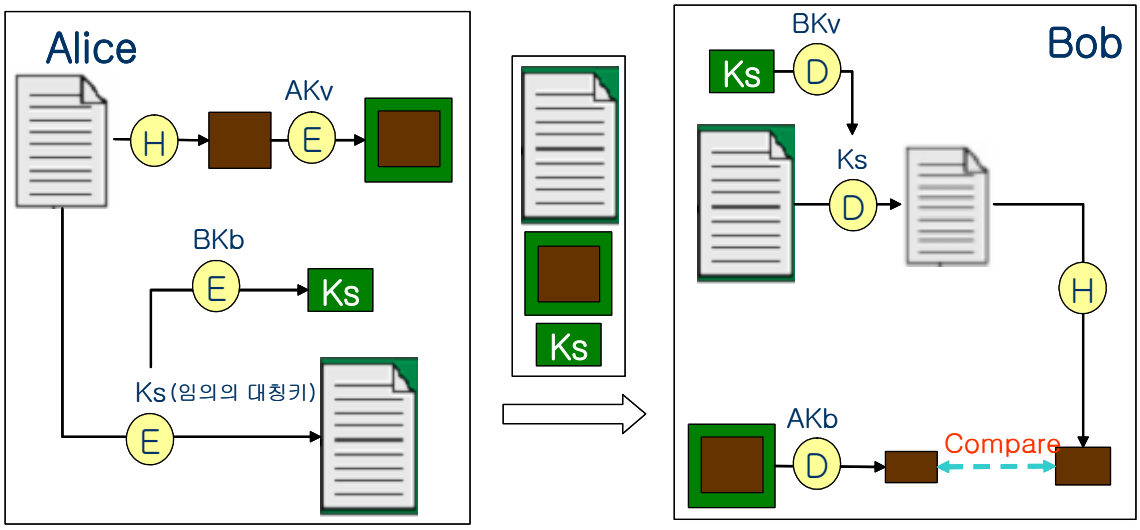

그림 6. 기밀성이 보장되는 전자서명 방식

(4) 공개키 기반구조(PKI: Public Key Infrastructure)

공개키를 안전하게 사용할 수 있는 기반을 구축하는 것을 의미하며, 인증기관과 등록기관들로 이루어진 인증서 발급 및 유효성 검증체계를 공개키 기반구조라고 한다. (ex. 공인인증서)

4. 결론

이제까지 기술적인 정보보안의 정보통제에 있어서 가장 중요한 요인으로 꼽히고 있고, 그 중에서도 가장 널리 쓰이고 중요하게 인식되고 있는 암호화 기법에 대해 살펴보았다.

만일 완벽한 접근통제가 이루어질 수 있다면 정보통제(대표적 예: 암호통제) 만으로도 적정한 정보보호를 이룰 수 있을 것이다. 그러나 어떠한 정보시스템도 완벽한 접근통제는 불가능하다. 기존의 접근통제 기술을 능가하는 해킹 기술이 개발될 수 있으며, 또한 시스템에 관련된 사람들의 부주의나 고의적인 행동에 의하여 불법적인 접근이 이루어질 가능성은 항상 존재하기 마련이다. *이렇게 파일이 노출되는 상황에서도 파일이 가지고 있는 정보를 노출시키지 않을 수 있는 마지막 정보보호 수단으로 사용되는 것이 이제까지 살펴 본 암호법(cryptography)이라고 할 수 있다. 특히 통신의 경우에는 옥외를 통하는 유무선 통신망을 통하여 파일이 전송되기 때문에 통신망에 대한 도청(wiretapping)이 언제든지 일어 날 수 있다. 이러한 상황에서 전송되는 정보를 비밀로 유지할 수 있는 유일한 방법은 정보를 암호화하여 전송하는 것이다.*

그러나, 앞에서 언급한 바와 같이 기술적인 방법만으로 성취할 수 있는 정보보호는 제한적이며, 기술적인 방법은 적절한 관리와 지침으로 지원되어야 한다. 이러한 정보보호 관리체계는 종합적이며 체계적으로 구축하여야 보안에 취약한 점들을 가능한 한 줄일 수 있다. 이러한 정보보호 관리체계를 구축하기 위해서는 여러 가지 다양한 관점에서 관리적, 물리적 정보보호 통제 과정이 도입되어 기술적인 통제 방안들과 상호 보완적으로 운영 체계가 구축되어야 할 것이다.

5. 토론 가능한 주제

1. EHR에서의 정보보호의 방향, 기술적 필요 구성요소에 대한 검토
2. EHR 구축 시 정보보호의 기술적 정보통제(암호화 기법)의 적용분야 및 적용방안

6. 참고문헌

1. 김세헌. 정보보호 관리 및 정책. 생능출판사. 2002
2. 김동수. 암호화 및 공개키 기반 구조(PKI). 2005
3. 김동수. 전자상거래의 신뢰성, 전자상거래 보안 기술. 2005
4. 변대호. e-비즈니스 전자상거래. 2004
5. 김연수. 개인정보보호. 사이버출판사. 2001.
6. British Standards Institution. Information security management Part 1: Code of practice for information security management. BS-7799, 1999
7. British Standards Institution. Information security management Part 2: Specification for for information security management systems. BS-7799, 1999
8. e-Health 발전전략 수립을 위한 주요 검토 과제. 보건복지부. 2005
9. 김동수. XML 정보보호 기술을 적용한 ebXML 보안 시스템의 설계. 2002 정보과학회

추계학술발표회 논문집. 2002년 10월 25-26일. 수원대학교
10. 한국정보보호진흥원 http://www.kisa.or.kr/
11. 전자서명인증관리센터 http://www.rootca.or.kr/