특 집

암호기술 동향

김 승 주, 이 홍 섭
한국정보보호센터

Ⅰ. 서 론

일반적으로 암호 기술의 기본 기능은 비밀성 기능("암호화 기술"이라고도 함)과 인증 기능("기본적인 암호 프로토콜 기술"이라고도 함)으로 나눌 수 있다. 비밀성 기능이란 정보통신망에서 전송되는 중요 데이터의 불법적인 노출을 방지하는 기능으로, 메시지를 제3자가 해독 불가능한 형태로 변형하거나 또는 암호화된 통신문을 해독 가능한 형태로 변환하기 위한 원리, 수단, 방법 등을 취급하는 기술 또는 과학을 말한다. 암호의 비밀성 기능과 관련된 중요한 용어 몇 가지를 설명하면 다음과 같다. 송신자가 수신자에게 보내고 싶은 보통의 메시지를 평문(plaintext)이라 하며, 평문을 제3자가 그냥 보아서는 이해할 수 없는 암호문(ciphertext)으로 변환시키는 조작을 암호화(encryption)라고 한다. 역으로 암호문을 본래의 평문으로 바꾸는 조작을 복호화(decryption)라 한다. 복호화는 정당한 수신자가 정당한 절차를 통해 평문을 복원하는 경우를 말하며, 부당한 제3자(도청자)가 다른 수단을 통해 평문을 알아내는 것을 암호 해독(cryptanalysis)이라 한다. 또한 암호화/복호화 방식을 암호/복호 알고리즘이라 하며, 암호/복호 알고리즘에 의한 평문/암호문의 변환을 제어하는 파라메터를 암호화/복호화 키(encryption/decryption key)라 한다. 또한, 암호/복호 알고리즘은 대칭키 암호알고리즘과 공개키(비대칭키) 암호알고리즘으로 나누어지며, 미국 표준인 56비트 DES(Data Encryption Standard) 및 한국 표준인 128비트 SEED는 대표적인 대칭키 암호알고리즘이며, RSA는 대표적인 공개키 암호알고리즘이다.

암호의 인증 기능이란 비밀성 기능과는 달리 현대 사회의 업무가 고도 지식정보사회로 변형되는 과정에서 새로이 야기되는 정보보호문제—통신하는 사람간의 신분확인 문제, 전송되는 전자문서의 위 변조 방지 문제, 사이버공간상에서 발생하는 전자적 행위에 대한 사후 부인을 방지하는 문제, 계약시간을 확인해주는 시점확인(time-stamp) 문제 등—를 해결하는 기능으로, 정보화 사회가 활성화 될 수록 매우 중요한 역할을 담당하게 된다. 인증 기능을 지원하기 위한 기술로서는 전자서명 알고리즘, 해쉬 알고리즘, 부인방지 프로토콜, 개인식별 프로토콜 등이 있으며 미국 표준인 DSA(Digital Signature Algorithm)와 한국 표준인 KCDSA(Korea Certificate-based Digital Signature Algorithm) 등은 대표적인 전자서명 알고리즘이다.

Ⅱ. 대칭키 암호알고리즘

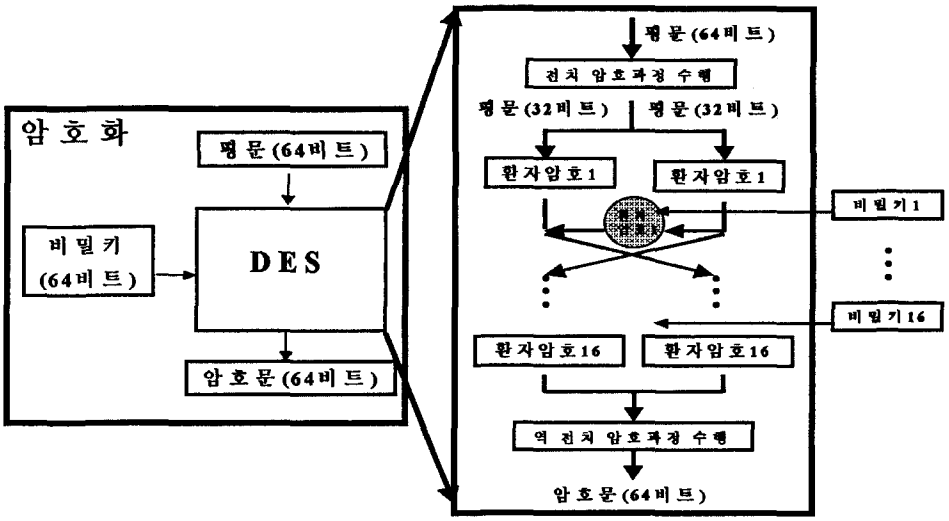
현대 암호방식은 키 관리 측면에 따라 크게 대칭키 암호 알고리즘(symmetric-key encryption algorithm)과 공개키 암호 알고리즘(public key encryption algorithm)으로 분류할 수 있다. 대칭키 암호 알고리즘은 송·수신자가 동일한 키에 의하여 암호화 및 복호화 과정을 수행하는 방식을 일컫는다 (즉, 암호화 키=

〈표 1〉 세계 각국의 표준 대칭키 암호알고리즘의 개발 현황

국 가	명 칭	현 황
러시아	GOST	구 소련의 국가표준
미국	DES	· 1977년 표준으로 제정되어 1997년까지 전세계적으로 널리 사용됨. · DES 알고리즘은 미국 연방 정부의 데이터 보호용으로 출발하여 ANSI의 표준 암호알고리즘, ABA에서 미국 내 금융정보의 보호 표준으로 사용하기에 이르러 사용 범위가 확산되었고, UNIX의 crypt() 명령, SET, SSL/TLS 등의 보안 프로토콜에도 사용되는 등 실질적인 세계 표준으로 널리 활용되어 왔음.
	Rijndael	· 미국정부는 매 5년 주기로 DES의 안전성을 검증하였으며, DES가 더 이상 안전하지 않다고 판단하여 1998년 폐기하고, 이를 대체할 차세대 암호알고리즘으로 Rijndael을 공모를 통하여 개발하였음.
	RC4	· SSL/TLS 보안프로토콜 및 블루투스에서 데이터 송수신시 암호화 기능을 제공하기 위해 사용됨.
	C2	· DVD의 불법복제를 방지하기 위해 사용됨. · 콘텐츠 제공자가 디지털 콘텐츠를 C2 블록암호알고리즘으로 암호화하여 배포하면 사전에 암호키를 발급 받은 유료 사용자만이 암호화된 콘텐츠를 해독 가능한 형태로 변환하여 시청하게 됨.
유럽	IDEA	· 유럽 산업체 표준 · SSL/TLS 보안프로토콜에서 암호화 기능을 제공하기 위해 사용됨.
	SAFER	· 블루투스에서 사용자의 신분확인 기능을 제공하기 위해 사용됨.
일본	KASUMI	· 차세대 이동 통신망인 IMT-2000에 사용될 목적으로 국제 표준으로서 개발되었으며, 일본 미쯔비시전기(주)에서 개발한 MISTY를 기반으로 하여 설계됨.
한국	SEED	· DES등의 외산 암호알고리듬이 보안성에 문제가 있다고 판단하여 한국정보보호센터가 1999년에 개발한 국내 표준 대칭키 암호알고리즘으로서, 국내 전자상거래(EC)·전자우편·전자문서교환(EDI)·위성방송시스템 등의 분야에서 데이터 송수신 및 저장시 암·복호화 기능을 제공함. · SEED는 운영통신망기술, 전송기술, 선로기술, 정보보안 등 13개 분야 1260건의 정보통신 표준 중 그 활용도가 1위로 조사됨. (2001년 3월6일자 전자신문)

복호화 키). Caesar 암호로부터 DES(미국 표준 56비트 대칭키 암호알고리즘) 및 SEED(한국정보보호센터가 개발한 국내 표준 128비트 대칭키 암호알고리즘)에 이르기까지 2천여년 이상 사용하여 온 대칭키 암호 알고리즘은 송신자와 수신자가 같은 키를 공유하는 방식으로 복호화는 암호화의 단순한 역조작(예 : 덧셈은 뺄셈, 곱셈은 나눗셈)이어서 암호화할 때와 복호화할 때 사용하는 키가 동일하다. 현재 사용되고 있는 세계 각국의 표준 대칭키 암호알고리즘의 개발 현황은 다음의 〈표 1〉과 같다.

그러면 현재 우리가 쓰고 있는 표준 블록 암호알고리즘 DES, SEED 등은 어떻게 구성되어 있을까? 우리가 가장 손쉽게 암호알고리즘을 만들 수 있는 방식은 치환(substitution) 암호와 전치(permutation) 암호가 있다. 치환은 원래 본문의 문자를 어떤 규칙에 의해 다른 문자로 대치하는 것이고, 전치는 문자들의 위치를 서로 바꾸는 것이다. 예를 들어, 세 번째 문자는 첫 번째, 다섯 번째 문자는 두 번째로, 첫 번째 문자는 세 번째로 재배치하면, 재배치된 문장이 암호문이 되며, 암호문을 평문으로 복원하는 복호화 과정



〈그림 1〉 DES 표준 블록 암호알고리즘의 구조

은 암호화 과정의 반대 순서로 재배치를 하면 평문이 복원된다. C.E.Shannon 교수의 유명한 연구 결과중의 하나가 강한 암호알고리즘은 약한 (단순한) 암호알고리즘을 반복함으로써 얻어질 수 있다는 것으로, 현대의 암호알고리즘 구조는 이 이론에 근거하고 있다. 즉, 치환 암호와 전치 암호를 교대로 반복 적용함으로써 강한 암호 알고리즘을 만들 수 있다는 것다. DES나 SEED의 구조를 생각해보면, S-box라는 것이 있으며, 이것은 치환 암호의 역할을 한다. 또한 S-box를 거친 후, 좌우로 나누어서 교차시키는 부분은 전치 암호의 역할을 수행하는 부분이다. 이를 도식화 해보면 〈그림 1〉과 같다.

II. 공개키 암호알고리즘

대칭키 암호알고리즘의 최대의 난제는 암호화 과정에서 사용되는 키의 안전한 분배였다. 암호가 군사 혹은 외교 등 한정된 분야에만 사용되던 시대와는 달리 현재는 불특정다수에 의한 데이터의 교환이나 프라이버시(privacy) 보호를 위하여 민간 부분에서도 비밀 통신에 대한 수요가 급격히 증가하고 있다. 따라서 비밀 통신을 하고자 하는 양자간에 키의 안전한 전송은 일상 업무에서 아주 중요한 문제가 되었다. 1976년 W. Diffie와 M.E.Hellman이 논문 "New Directions in Cryptography"에서 최초로 제시한 공개키 암호방식은 기존 암호학의 상식을 뛰어넘는 혁신적인 발상으로 키의 일부를 공개함으로써 키 관리의 어려움을 해결하고자 하는 방식이다. 대칭키 암호방식은 송·수신자가 동일한 키에 의하여 암호화 및 복호화 과정을 수행하므로, 키를 안전하게 전송하고 보관함에 있어 어려움이 야기된다. 이에 비하여 공개키 암호방식은 암호화할 때 사용하는 키(일명 공개키(public key))와 복호화할 때 사용하는 키(일명 비밀키(private key))가 달라서 공개키는 공개하고 비밀키만 안전하게 유지하는 방식이다. 즉, A가 B와 비밀 통신을 하고자 하는 경우, A가 공개키 디렉토리(public directory, 예 : 전자 게시판 등)에 공개된 B의 공개키를 가지고 송신할 내용을 암호화하여 B에게 전송하면, B는 자신만이 가지고 있는 비밀키를 이용하여 암호문을 복호화 한다. 따라서 대칭키 암호방식에서 전제로 하였던 키의 안전한 분배는 필요없게 된다. 일반적으로 공개키 암호방식을 구성하는 방법으로는 전산학의 계

산 복잡도 이론(complexity theory)에서 어려운 문제(NP 문제)로 알려진 다음의 2문제를 가장 많이 사용한다.

[정의 1] **(소인수 분해 문제 (Factorization Problem))**

주어진 합성수 n의 소인수들을 찾는 문제로 n의 자릿수가 매우 큰 경우(10^{150} 이상)에는 n의 소인수를 효율적으로 찾는 알고리즘이 아직까지는 존재하지 않는다고 알려져 있다.

[정의 2] **(이산대수 문제 (Discrete Logarithm Problem))**

소수 p가 주어지고 $y \equiv g^x \pmod p$인 경우, 역으로 $x \equiv \log_g y \pmod p$인 x를 계산하는 문제. 여기서 x를 모듈러 p상의 y의 이산대수라 한다. p가 매우 큰(2512 이상) 소수이고, g의 위수(order)[1] k가 2^{140} 이상인 경우, x, g, p가 주어졌을 때, p가 비교적 큰 정수라 해도 y는 고속 멱승 연산 알고리즘을 사용하여 쉽게 구할 수 있지만, y, g, p가 주어졌을 때 $x \equiv \log_g y \pmod p$인 x를 구하는 문제는 어려운 것으로 인정되고 있다.

1976년 이후 공개키 개념을 실현하기 위하여 여러 알고리즘이 발표되었지만 현재 안전성을 인정받고 있는 공개키 암호알고리즘은 RSA와 Diffie-Hellman 알고리즘 등에 거의 한정되어 있다. 본 절에서는 RSA 공개키 암호알고리즘에 대하여 간략히 살펴본다. RSA는 1978년 Rivest, Shamir, Adleman이 발표한 논문인 "A Method for Obtaining Digital Signatures and Public Key Cryptosystems"에 제안된 암호방식을 말하며, 발표자의 머리 문자를 연결한 것이다. 이차 방정식의 해를 구하는 경우를 생각해 보자. 이차 방정식

$$ax^2+bx+c=0$$

이 주어졌을 때, 이 방정식의 해는 근의 공식에 따라

$$x=\frac{-b\pm\sqrt{b^2-4ac}}{2a}$$

이다. RSA 공개키 암호 알고리즘의 경우 다음과 같은 방정식과 근의 공식을 사용한다.

RSA 방정식)

$$x^e-c=0 \pmod{pq}$$

RSA 근의 공식)

① 유클리드 알고리즘을 사용하여 다음을 만족하는 정수 (d, k)를 계산한다.

$$de+k(p-1)(q-1)=1$$

② $x=c^d \pmod{pq}$

그러면 위의 RSA 방정식과 근의 공식을 이용하여 공개키 암호방식을 구현해 보자. RSA 공개키 암호알고리즘은 매우 큰 정수의 소인수 분해가 어렵다는 가정하에서 설계된 것이다. 시스템 구성은 다음과 같다. 사용자 A가 사용자 B와 비밀 통신을 하고자 하는 경우, B는 사전에 두 개의 큰 소수 p(예, 11)와 q(예, 13)를 생성하여 n=pq(예, 11×13=143)를 계산하고, (p-1)(q-1)과 서로 소가 되는 난수 e(예, 11)를 임의로 선정한다. 이제 사용자 B는 공개키 n값과 e값을 공개된 게시판(일명 공개키 디렉토리)에 공개하고, p값과 q값은 자신만이 가지고 있는 비밀키로 간직한다.

A가 B의 공개키 (n, e)를 이용하여 메시지 'K'(ASCII 코드 값이 10진수로 75)를 암호화해 보내고자 하면, A는 $75^e-c=0 \pmod n$을 만족하는 c(예, $c=75^{11} \bmod 143=108$)를 계산하여 이 값을 메시지 'K'에 대한 암호문으로 B에게 전송한다. 암호문 c를 수신한 사용자 B는 자신의 비밀키 (p, q)를 가지고 RSA 근의 공식을 이용하여 ① (d=11, k=−1) : $d\times11+k\times10\times12=1$, ② $x=108^{11} \bmod 143=75='K'$를 계산하여 암호문을 복호화 한다. RSA 공개키 암호알고리즘은 공개키 n과 e를 가지고 d를 구할 수 있으면

1) g의 위수 k는 $g^k \equiv 1 \pmod p$를 만족하는 최소의 양의 정수.

해독이 가능해진다. d를 찾아내기 위해서는 (p-1)(q-1)을 계산할 수 있으면 가능하지만, n의 소인수분해를 모르고서는 (p-1)(q-1) 값을 결정하기 어렵다. 만약, 소수 p와 q가 약 256 비트(bit)의 소수이고, n이 약 512 비트를 갖는 합성수라고 하면 현재의 기술로 n을 인수분해 하는 것은 거의 불가능하다고 알려져 있다.

RSA 공개키 암호알고리즘은 공개키 (n, e)를 전화 번호부처럼 공개하므로 누구든지 메시지를 암호화하여 상대방에게 보낼 수 있고, (n, e)에 대응하는 비밀키 (p, q)를 알고 있는 수신자만이 복호화가 가능하게 된다. 한편, RSA 방식은 512 비트의 정수에 대한 멱승을 필요로 하기 때문에 계산에 소요되는 시간이 대칭키 암호알고리즘에 비하여 오래 걸린다는 단점이 있다. 이러한 문제점을 해결하고, RSA 공개키 암호알고리즘을 이동통신 및 무선 PKI 환경에서 빠른 속도로 동작할 수 있게하기 위한 기술로는 RSA사의 "멀티 프라임(multi-prime) 기법"과 한국정보보호센터의 "RSA 공개키암호 고속화 기법" 등이 있다. 특히 한국정보보호센터가 개발한 기술을 사용할 경우 기존 RSA 암호알고리즘의 암·복호화 및 전자서명의 생성·검증 작업을 3배 이상 빠르게 수행할 수 있으며 그 속도의 차이가 모듈러스의 사이즈가 커질수록 점점 커지게 되므로, 메모리의 크기나 연산처리능력 등에 제한이 많은 스마트 카드나 이동 통신 단말기에 적용 가능하다.

Ⅳ. 전자 서명

보통의 경우 암호라 하면 비밀 통신을 연상한다. 물론 정보화 사회에서도 비밀 통신은 중요하다. 그러나 일상 업무중에서는 비밀 문서의 취급보다는 일반 문서에 대한 서명이나 인증이 훨씬 빈번하게 있을 것이다. 정보화 사회에서는 종이로 작성된 문서 대신에 컴퓨터나 네트워크 내에서 위·변조나 복사가 용이한 바이너리 파일(binary file)로 작성된 문서를 취급하게 될 것이므로 전자 서명이나 인증은 비밀 통신 이상으로 아주 중요한 기능이다. 일반적으로 서명이나 인감은 개인의 필요성에 의하여 언제든지 생성할 수 있고, 이 서명 또는 인감을 수신한 사람은 누구든지 수신된 서명이나 인감의 정당성을 쉽게 확인할 수 있으며, 서명의 생성자나 인감의 소유자 이외에는 이 서명이나 인감을 위조할 수 없어야 한다. 따라서 전자 서명에서도 ① 정당한 서명자만이 자신의 서명을 생성할 수 있는 '유일성', ② 위조가 불가능한 '위조 불가능성', ③ 누구든지 서명의 진위를 쉽게 확인할 수 있는 '진위 확인의 용이성', ④ 서명자가 서명한 후에 자신이 서명한 사실을 부인하는 것이 불가능한 '거부의 불가능성' 등의 요구 사항을 만족해야 한다. 이러한 의미에서 자신의 서명을 스캐너(scanner)로 읽어들여 전자 문서에 덧붙이는 형태의 서명방식은 덧붙여진 서명 영상을 다시 스캐너로 읽어들여 임의의 문서에 복사할 수 있으므로 '유일성', '위조 불가능성' 등을 만족하지 않는다.

공개키 암호방식을 이용한 서명 방식은 다음과 같다. 서명자 A는 전자 문서에 대하여 자신의 비밀키를 사용하여 서명값을 생성한 후, 검증자에게 전송한다. 검증자는 공개키 디렉토리에 등록된 A의 공개키를 사용하여 서명값을 검증한다. 서명 알고리즘의 효율성을 증가시키기 위하여 메시지에 대한 서명을 생성하는 대신에, 압축 알고리즘의 일종인 일방향 해쉬 함수(one-way hash function) H(·)를 이용하여 메시지를 압축한 후, 이 압축한 값에 대한 서명값을 생성할 수도 있다. 대표적인 일방향 해쉬함수로는 미국 표준인 SHA(Secure Hash Algorithm)와 한국 표준인 HAS-160(160-Bit Hash Algorithm Standard) 등이 있다. 현재 사용되고 있는 세계 각국의 표준 전자서명 알고리즘의 개발 현황은 다음의 〈표 2〉와 같다.

여기에서는 RSA 서명방식에 대하여 간략히 살펴본다. RSA 서명방식의 시스템 구성은 RSA 암호방식과 같다. 사용자 A가 디지털 서명을 하고자 하는 경우, 사전에 A는 두 개의 큰 소수 p (예, 7)와 q(예, 11)를 생성하여 n=pq(예, 7×

〈표 2〉 세계 각국의 표준 전자서명 알고리즘의 개발 현황

국가	명칭	현황
미국	DSA	· 1991년 미국의 NIST가 개발하여, 1994년 미국 연방표준으로 제정됨.
	RSA	· Rivest. Shamir, Adleman 세 사람이 1978년 개발한 세계 최초의 전자서명 알고리즘으로서 현재 실질적인 세계 표준으로 널리 활용되고 있으며, 2000년 미국 연방표준으로 제정됨.
일본	ESIGN	· 1985년 일본의 NTT사가 개발.
한국	KCDSA	· 전자문서의 불법적인 위·변조를 방지하기 위하여 한국정보보호센터가 1997년에 개발한 국내 표준 전자서명 알고리즘으로서, 1999년 2월 5일 제정된 전자서명법(법률 제5792호)에 의해 DSA 및 RSA와 더불어 기존의 서명이나 인감과 동일한 법적 효력을 가짐.

11=77)를 계산하고, (p−1)(q−1)과 서로 소가 되는 난수 e(예, 13)를 임의로 선정한 후, 공개키 n값과 e값을 공개키 디렉토리에 공개하고, p값과 q값은 자신만이 가지고 있는 비밀키로 간직한다. 서명자 A는 "RSA 근의 공식"을 이용하여 비밀값 p와 q로부터 $de+k(p-1)(q-1)=1$을 만족하는 d(예, 37)와 k를 계산한 후, 메시지 m(예, ASCII 코드 값이 10진수로 18인 문자)에 대한 서명값 $x=m^d \pmod n$을 계산하여 메시지 m과 서명값 x(예, $x=1837 \bmod 77=39$)를 검증자 B에게 전송한다. 메시지 m과 서명값 x를 수신한 B는 "RSA 방정식"과 A의 공개키 (n, e)를 이용하여

$x^e-m\stackrel{?}{=}0 \bmod n$ (예, $39^{13}-18\stackrel{?}{=}0 \bmod 77$)

이 만족하는지를 검사한다.

V. 암호기술의 응용분야

인터넷을 기반으로 하는 고도의 지식정보사회에서는 현재 우리가 하고 있는 모든 업무가 사이버업무로 변환된다. 현대사회는 정보기술활용이 점차 극대화되고 암호기술이 일상생활에서 널리 사용되는 등 빠르게 암호사회로 진입하고 있다. 예를 들어, 상용 위성방송시스템의 경우 방송사가 방송 전파를 암호화하여 전송하면 사전에 암호키를 발급 받은 유료 사용자만이 암호화된 방송 전파를 해독 가능한 형태로 변환하여 시청하게 되어 있으며, 또한 인터넷상에서 안전한 신용카드 결제를 실현하기 위하여 비자사와 마스터카드사가 공동으로 개발한 SET 프로토콜의 경우, 이를 사용하면 고객의 신용 카드 번호가 암호화되어 전송되며, 이밖에도 통신 상대방의 인증, 주문 의뢰가 도중에 위·변조되지 않았음을 확인하기 위하여 전자서명을 사용할 수도 있도록 되어 있다. 이외에도 암호이용 동향을 살펴보면 휴대전화를 이용한 요금 부과 등 암호기술을 이용, 단말기를 인증하는 서비스 분야도 창출되고 있으며 인터넷 상의 암호화 통신 및 인증을 위하여 암호기능이 지원되는 VPN 산업도 계속하여 성장하고 있다. 이처럼 암호기술은 이미 정보통신의 다양한 분야에 이용되고 있다. 현대사회에서 이러한 암호기술이 실생활에 활용되고 있는 분야 및 활용될 수 있는 분야에 대해 간략히 살펴보면 다음 〈표 3〉, 〈표 4〉와 같다. (〈표〉에서 "기밀성"이란 인터넷을 통해 전송되는 중요정보의 불법노출을 방지하는 기술이며, "인증"이란 전송된 정보의 송신자와 수신자를 확실하게 보장하는 기술이며, "무결성"이란 정보의 위·변조 여부를 판단하는 기술이다. 이외에도 전자계약에서의 동시성 문제, 계약시간을 확인해주는 "시점확인(time-stamp)", 전자상거래에서의 거래 당사자들간에 형평성을 보장하는 "공정성(fairness)" 등이 있다.)

〈표 3〉 암호기술의 활용분야

분야	활용분야	암호기술 적용 부분	암호 서비스
전자 정부	전자선거	◦ 일인 일투표	부인봉쇄 공정성
		◦ 정당한 자격을 갖는 사람만이 선거에 참여	인증
		◦ 투표내용에 대한 기밀유지	기밀성
		◦ 투표자로부터 투표내용을 추적할 수 없음	익명성
		◦ 공정한 투표 집계 보장	공정성
		◦ 적법한 선거 기간내에 투표되었음을 보장	무결성
		◦ 투표이후, 내용변경 불가	무결성
	전자결재	◦ 결재문서의 위·변조 방지	무결성
		◦ 결재자의 결재 사실 부인방지	부인봉쇄
		◦ 전자문서 송·수신 부인방지	부인봉쇄
	온라인 민원 서비스	◦ 신청자 신원확인	인증
		◦ 공인기관이 적법하게 발급한 문서임을 증명	인증
		◦ 발급된 민원 서류의 위·변조 방지	부인방지
	전자조달	◦ 조달문서 위·변조 방지	무결성
	전자조세	◦ 개인의 재산 및 납세 내용에 대한 기밀보호	기밀성
		◦ 납세고지서 위·변조 방지	무결성
		◦ 납세고지서 송·수신 부인방지	부인봉쇄
전자 상거래	전자입찰	◦ 입찰문서의 위·변조 방지	무결성
		◦ 유효기간내에 입찰 참가 여부 확인	인증
		◦ 제출한 문서가 공정한 절차에 의해 처리됨을 보장	공정성
		◦ 입찰기한까지 접수된 입찰내용 누출방지	기밀성
	홈쇼핑	◦ 구매정보 및 지불정보	무결성
		◦ 상점인증	인증
		◦ 구매사실 부인방지	부인방지

〈표 4〉 암호기술의 활용분야

분야	활용분야	암호기술 적용 부분	암호 서비스
전자 상거래	전자공증	◦ 공증문서의 위·변조 방지	무결성
		◦ 공증 시점의 변조방지	인증
		◦ 공증한 사실에 대한 부인방지	부인방지
	전자계약	◦ 계약 당사자간 동시에 서명이 이루어졌음을 보장	동시성
		◦ 계약 사실의 부인방지	부인방지
		◦ 계약 문서의 위·변조 방지	무결성
		◦ 계약문서의 기밀유지	기밀성
	전자지불	◦ 지불 정보의 비밀유지	기밀성
	홈뱅킹	◦ 계좌 소지자의 신분확인	인증
		◦ 거래하는 은행 인증	인증
		◦ 거래 정보 변조방지	무결성
	전자화폐	◦ 계좌 소지자의 신분확인	공정성
		◦ 거래하는 은행 인증	익명성
		◦ 거래정보 변조 방지	공정성
사이버 교육	원격교육	◦ 인가된 사람만이 교육을 받을 수 있음	인증
의료 사업	원격진료	◦ 인가된 사람만이 진료기록에 접근	인증
		◦ 환자의 진료정보 기밀 유지 및 위·변조 방지	기밀성 무결성
		◦ 통신 상대방 확인	인증
		◦ 처방 문서에 대한 부인방지	부인방지
온라인 통신	전자메일	◦ 전송되는 메일 내용 노출	기밀성
		◦ 전송되는 메일내용 위·변조 방지	무결성
		◦ 메일 송·수신 부인방지	부인방지

V. 결 론

모든 첨단과학 기술이 전쟁에 이용되면서 발전돼 왔듯이 암호기술 역시 전쟁을 통해 발전을 거듭해 왔다. 컴퓨터가 생긴 뒤에는 더욱 정교하고 풀기 어려운 새로운 암호기술이 만들어져 사용되

고 있다. 특히 경제, 군사, 산업, 교육활동 등 모든 정보교환이 컴퓨터를 통해 이루어지고 있는 현대에 있어 국가든 단체든 개인이든간에 자신에 관한 모든 것을 원치않은 제3자가 손바닥 보듯이 보고 있다고 가정하면 암호화 기술이야말로 생존의 수단이 될지 모른다.

앞서 살펴보았듯이, 디지털 사회로의 이행기에서 현재 암호기술의 사회 경제적인 위치는 『특정 분야에서 이용되는 특수한 기술』에서 『차세대 사회 경제의 기반 기술』로 크게 변화하여 그 중요성은 점차로 높아지고 있는 실정이며, 또한 공공안전의 확보를 위한 핵심 요소기술로서 침입차단시스템(Firewall), 침입탐지시스템(IDS), PKI, 가상사설망(VPN) 등의 요소기술로서 활용되고 있다. (일본의 경우 1998년의 암호산업의 시장규모는 약 ¥900억이었으며, 미국의 경우 2006년 암호산업의 시장규모를 $90억로 예상하고 있음.)

그러나 암호와 해독은 창과 방패와 같아서 컴퓨터의 처리능력 향상이나 암호 해독 기술의 새로운 발견에 따라 그 강도가 약해지거나 한순간에 무력하게 될 수 있다. 따라서 단일 암호 기술에 지나치게 의존하는 것은 피해야 하며 차세대 암호 기술의 개발을 위해 지속적으로 투자하는 것이 요구된다.

참 고 문 헌

〔1〕 1. Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, "Handbook of Applied Cryptography", CRC Press.

〔2〕 Bruce Schneier, "Applied Cryptography", John Wiley & Sons, Inc.

〔3〕 William Stallings, "Network and Internetwork Security, Principles and Practice", IEEE Press.

〔4〕 Douglas R. Stinson, "Cryptography: Theory and Practice", CRC Press.

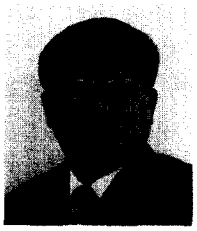
〔5〕 Man Young Rhee, "Cryptography and Secure Communications", McGraw-Hill.

〔6〕 원동호 역, "정보와 부호이론", Ohm사.

저 자 소 개

金 昇 柱

1971년 9월 22일생, 1990년 3월~1994년 2월 : 성균관대학교 정보공학과 졸업 (공학사), 1994년 3월~1996년 2월 : 성균관대학교 정보공학과 대학원 졸업 (공학석사, 암호학 전공), 1996년 3월~1999년 2월 : 성균관대학교 정보공학과 대학원 졸업 (공학박사, 암호학 전공), 1999년 12월~현재 : 한국정보보호센터 기술부 암호기술팀장, 2000년 6월~현재 : 한국정보통신기술협회, 정보보호 기술위원회, 암호기술연구반 의장, 2001년 1월~현재 : 한국통신정보보호학회 논문지 편집위원, 〈주관심 분야 : 암호학, 정보이론, 암호키 복구기술, 소프트웨어 역분석 방지 기술〉



李 弘 燮

1953년 6월 24일생, 1979년 : 한양대학교 전자공학과 졸업 (공학사), 1985년 : 한양대학교 전자공학과 대학원 졸업 (공학석사), 1999년 : 대전대학교 컴퓨터공학과 대학원 졸업 (공학박사), 1980년~1996년 : 한국전자통신연구원, 연구원~책임연구원, 실장, 1996년~현재 : 한국정보보호센터 연구개발부장, 기술본부장, 인증관리센터구축준비반장, 현 기술부장, 1996년~현재 : 한국통신정보보호학회 상임이사, 1997년~현재 : 정보통신기술협회 정보보호기술위원회 의장, 2000년~현재 : 전자거래/금융/개인정보 분쟁조정위원회 조정위원, 2000년~현재 : 인터넷보안기술포럼 의장, 2001년~현재 : 사이버/컴퓨터수사 자문위원회 위원, 2001년~현재 : 대한전자공학회 회지편집위원회 위원, 〈주관심 분야 : 정보보호 관리, 정보보호기술 표준화, PKI, 시스템 및 네트워크 보안 등〉