□ 기술해설 □

정수론과 디지탈 서명

국방대학원 남 길 현*

목 차

1. 서 론

정수론은 정수와 관련된 이론을 연구하는 학문으로서 아주 오랜 역사를 갖고 꾸준히 발전되어 왔다. 특히 정보화 사회로 진입하는 시점에서 현대 첨단 과학의 견인차 역할을 수행하는 컴퓨터의 발전과 함께 정수론은 전자계산학, 정보론, 암호학, 통신론 등의 제분야에서 활발히 응용되고 있다. 최근에는 컴퓨터의 계산이론과 정수론의 원리에 근거를 둔 다양한 암호시스템들이 개발되고 있으며 그 중에서도 암호시스템을 응용한 디지탈 서명은 종이에 찍힌 인감 도장을 대신할 수 있는 전자적 서명 방식으로서 정보화 사회를 앞당길 수 있는 중요한 도구로 인식되고 있다.

정보화 사회에서는 많은 중요 문서나 자금 결재 서류 등이 디지탈 통신망을 이용하여 교환되고 있으며 이러한 문서 교환에서의 문제점은 서로 상대방이 누구인지를 정확하게 인증하는 것과 차후에 교환된 문서에 대한 변조 또는 부인을 할 수 없도록 하는 것이다. 디지탈 서명은 이와 같은 인증이나 부인봉쇄를 효과적으로 해결할 수 있는 매우 좋은 방식으로 인정되고 있다.

현재 급속도로 진행되고 있는 각종 전산망의 확장과 더불어 중요 문서를 전송하는 메세지 처리 시스템(MHS), 금융망에서 많이 취급되고 있는 전자 자금결재 시스템 또는 무역망을 통한 계약이나 자금 결재를 위해서는 디지탈 서명이 거의 필수적인 사항이라 인식되고 있다.

본고에서는 디지탈 서명을 이해하는데 기본이 되는 정수론과 관련된 기초 이론을 간단히 알아보고 디지탈 서명의 특성과 함께 실제 구현할 수 있는 방안을 설명하고자 한다. 아주 구체적인 깊은 이론이나 세부 사항은 가급적 피하고 암호학이나 정수론에 깊은 지식이 없는 독자들도 쉽게 개념을 파악하여 활용할 수 있도록 하는데 중점을 맞추었다.

2. 정수론과 풀기 어려운 문제들

2.1 역원(inverse)과 소수(prime)

2.1.1 정수의 연산과 역원

* 종신회원

정수(integer)는 0, 1, −1, 2, −2,… 등과 같은 소숫점이 없는 수를 뜻하며 이중에서도 자연수는 1, 2, 3,…과 같은 양의 정수만을 나타낸다. 그리고 덧셈, 곱셈과 같은 정수의 연산에서 항등원(identity)과 역원(inverse)을 정의할 수 있다.

정수의 연산 ⊙에 대한 항등원과 역원은 임의의 정수 a에 대하여 다음 조건을 만족시켜야 한다.

항등원(I) : $a \odot I = I \odot a = a$
역원(a^{-1}) : $a \odot a^{-1} = a^{-1} \odot a = I$,

정수의 연산에서 $a+0=0+a=a$이므로 0은 덧셈의 항등원이며 $a * 1=1 * a=a$이므로 1은 곱셈의 항등원이다. 또한 $a+(-a)=(-a)+a=0$이므로 $-a$는 덧셈에 관한 a의 역원이 된다. 그러나 $a*\frac{1}{a}=\frac{1}{a}*a=1$이 되지만 $\frac{1}{a}$은 a가 1 또는 −1이 아닌 경우에는 정수가 아니므로 정수의 연산에서 곱셈에 관한 a의 역원은 존재하지 않는다.

2.1.2 소수

1보다 큰 정수 p가 1 또는 p이외의 양의 정수로는 나머지 없이 나누어지지 않을 때 이러한 수 p를 소수(prime)라고 한다. 또한 1보다 크면서 소수가 아닌수를 합성수(composite)라고 한다. 소수는 무한히 많이 존재하지만 정수가 커짐에 따라 소수의 분포 밀도는 점점 희박해 지며 지금까지 소수를 만들어 낼수 있는 일반적인 공식은 아직 찾아내지 못하고 있다. 따라서 10^{100} 이상되는 큰 소수가 필요할 때는 난수를 이용하여 적당한 크기의 홀수를 임의로 선택한 후 소수 판별식을 이용하여 그 수가 소수인지 아닌지를 판별하여 소수를 만들어내는 방법을 사용하고 있으며 다양한 소수 판별식들이 사용되고 있다. 그리고 두 정수 a와 b에 대하여 (a,b)의 최대 공약수가 1일 때 a와 b를 상대소수 또는 서로소라고 한다.

2.2 합동식

임의의 정수 a와 b에 대하여 0보다 큰 정수 m이 (a-b)의 약수일 때 "a는 법(modulus) m에 관하여 b와 합동이다"라 하고 이것을

$a \equiv b \pmod{m}$

으로 표현하며 이렇게 표현된 식을 합동식이라고 한다. 즉, $a \equiv b \pmod{m} \Leftrightarrow a-b \equiv mK$ (K:정수)이다. 합동식에서도 $aa^{-1} \equiv 1 \pmod{m}$관계가 성립되면 a^{-1}은 법 m에 관한 a의 곱셈역원이 된다.

합동식은 일상 생활에서 일정한 주기를 갖고 반복되는 현상과 비슷한 특성을 갖고 있으며, 무한히 많은 정수들을 유한한 범위를 설정하여 그 안에 매핑(mapping)시킬 수도 있다.

2.3 소인수 분해 문제

양의 정수 n (n>1)이 유한 개의 소수의 곱으로 나타내질 때 이를 n의 소인수 분해라고 하며 모든 양의 정수는 반드시 유일하게 소인수 분해된다.

$n = p_1 p_2 p_3 \cdots p_r$ (p_i : 소수, r>=1)

소수가 아닌 합성수 n의 소인수 분해는 $1 < p_i \leq \sqrt{n}$까지의 모든 소수에 대하여 나눗셈을 해봄으로써 구할 수 있으나 n이 매우 큰 소수의 합성수일 경우에는 소인수 분해가 쉬운 일이 아니다.

페르마(Fermat)의 이론에 기초한 인수분해 방법을 비롯하여 수체선별법, 이차선별법, 타원곡선법 등 다양한 소인수 분해 기법들이 연구되고 있으나 지금까지의 연구 수준으로서는 약 50자리 소수의 곱으로 이루어진 $n \approx 10^{100}$ 정도의 큰 합성수를 소인수 분해할 수 있는 정도에 머무르고 있다. 최근에 새로운 인수분해 알고리즘의 연구와 병렬처리 컴퓨터의 발달과 함께 소인수 분해 가능한 합성수의 상한선은 자꾸 높아지고 있으나 10^{200} 정도의 큰 합성수에 대한 소인수 분해는 현재의 기술 수준에서는 매우 어려운 문제로 인식되고 있다.

공개키 암호시스템으로 제안된 RSA(Rivest Shamir Adleman)시스템은 소인수 분해의 어려움에 근거를 두고 합동식과 오일러(Euler)정리를

이용하여 공개키를 알려주더라도 비밀키를 찾을 수 없도록 하고 있다.

RSA시스템은 약 10^{200} 정도되는 큰 합성수 n을 사용하고 있다.

2.4 이산대수 문제

p가 소수이고, g를 법 p에 관한 원시근이라고 하면, p보다 작은 임의의 양의 정수 y에 대하여

$$y \equiv g^x \pmod{p}$$

를 만족하는 $x(0<x<p)$가 반드시 존재하며 서로 유일하게 1 대 1로 대응된다.

일반적으로 윗식에서 x,g,p가 주어졌을 때 p가 비교적 큰 정수라고 해도 y는 고속지수 계산 알고리즘을 사용하여 쉽게 구할 수 있지만 y, g, p만 주어졌을 때 x를 구하는 문제는 매우 어려운 것으로 인정되고 있으며 이를 이산대수문제(discrete logarithm problem)라고 한다.

이산대수 문제의 난이도는 대략 소인수 분해 문제의 난이도와 비슷한 것으로 판단되고 있으며 ElGamal 암호시스템은 이러한 이산대수 문제의 어려움에 근거를 두고 제안된 공개키 암호시스템으로서 약 200자리수의 크기를 갖는 소수 p를 사용하도록 제안하고 있다.

3. 디지탈 서명의 특성과 표준화 동향

3.1 디지탈 서명의 특성과 필요 조건

앞에서 잠깐 언급한 바와 같이 디지탈 서명은 종이 문서에 찍힌 인감 도장과 같은 역할을 수행할 수 있는 기법이다. 우리가 중요한 문서에 대해서 문서 내용을 확인하고 보증해 줄 수 있는 책임을 명확히 하기 위해서는 보증자의 인감 도장을 문서에 날인하고 인감 증명서를 첨부하고 있다. 이러한 경우에 차후에 문서에 관한 분쟁이 발생한 사건에 대해서 해결방법을 생각해 보자.

첫째, 문서를 작성한 보증자가 문서 내용이나 인감도장 날인 사실을 부인하는 경우이다.

둘째, 문서를 보관하고 있는 자가 문서 내용을 변조하거나 인감 도장을 위조하여 자신에게 유리하게 허위 주장을 하는 경우이다.

이와 같은 두 가지 경우에 대한 일반적인 해결은 종이 문서의 내용이 변조되거나 다른 내용을 오려 붙일 경우에 흔적이 남는다는 사실때문에 쉽게 판별이 가능하며 인감 도장은 원본이 관공서에 등록되어 있고 보관 책임은 본인에게 있으며 이를 전문 감식가도 구분할 수 없을 정도로 완벽하게 위조한다는 것은 매우 어렵다는 사실을 바탕으로 분쟁 발생에 대한 진위 판단을 내리고 있다.

이제 전산망을 통하여 중요 문서가 전송되었을 때 서로가 상대방을 어떻게 인증하고 송신자의 문서 내용이나 전송 사실에 대한 부인을 방지하며 수신자가 단독으로 문서 내용을 변조할 수 없도록 하기 위해서는 디지탈 서명이라고 하는 특별한 방식이 필요하게 된다. 왜냐하면 보통의 팩시밀리와 같은 일종의 스캐너를 이용하여 인감 도장의 모양이나 개인의 필적이 담긴 서명을 메세지와 함께 영상으로 보내는 경우에는 수신자가 서명 부분만을 따로 편집하여 마음대로 변조할 수 있으므로 송수신자 사이에 분쟁이 발생할 경우에 진위 판단이 매우 어려워지기 때문이다. 예를 들어서 다음과 같이 전송된 영수증 메세지를 생각해 보자.

영 수 증

일금 일천만원정

위 금액을 김갑동으로부터 정히 영수함

1994년 1월 30일

홍 길 동 (서명)

나중에 송신자 홍길동은 메세지를 변조하여 일백만원만 받았다고 하거나 아예 돈을 받은 일이 없다고 주장할 수 있으며, 한편 수신자 김갑동이도 보관하고 있는 메세지를 변조하여 일억원을 주었다고 주장할 수 있다. 따라서 이러한 분쟁을 해결하기 위해서 디지탈 서명은 다음의 조건을 만족시킬 수 있어야 한다.

[조건 1] 수신자는 송신자(서명자)와 문서내용을 인증할 수 있어야 한다.

[조건 2] 송신자 이외에는 수신자를 포함한 어느 누구도 송신자의 서명을 위조

할 수 없어야 한다.

[조건 3] 송수신자 사이에 분쟁 발생시에는 제 3자(판정관)가 진위여부를 판단해 줄수 있어야 한다.

이와 같은 조건들 중에서 송신자 또는 수신자가 메세지 내용을 변조할 수 없도록 하기 위해서는 [조건 2]가 가장 중요한 역할을 한다고 볼 수 있으며 문서 내용이 조금만 변경되어도 서로 상이한 디지탈 서명이 생성된다. 만약 동일한 내용을 반복 서명하는 경우에도 시간을 포함시켜 재사용을 막을 수 있다.

우리가 여기에서 주의할 사항은 지금 상용으로 많이 유통되고 있는 전자 서명 방식이나 사내 문서 결재 방식은 전송 도중에 도청자나 사고에 의한 메세지 변조를 검출하기 위한 메세지 인증 방식만을 사용하거나 메세지 내용과 서명을 분리하여 메세지 내용과는 무관한 서명을 사용함으로써 [조건 2]를 만족시키지 못하는 경우가 대부분이라는 점이다. 따라서 [조건 2]를 만족시켜주지 못하는 전자 서명 방식은 책임 소재를 명확히 해야하는 중요 문서의 전송을 위해서는 적합한 방법이 되지 못하며 다른 부가적인 조치를 마련해야 한다.

3.2 표준화 동향

디지탈 서명과 관련된 국제 표준화는 ISO/IEC JTC1의 SC27에서 주도적으로 수행하고 있다. 디지탈 서명의 표준화 과제는 메세지 회복형 디지탈 서명과 부가형 디지탈 서명으로 구분되며 메세지 회복형 디지탈 서명은 1991년에 국제 표준으로 제정되었고, 부가형 디지탈서명은 현재 초안 작성이 진행되고 있다. 그러나, 디지탈 서명의 국제 표준은 어느 특정 서명 알고리즘을 국제 표준으로 채택하지는 않고 전반적인 프레임워크(framework)만을 규정할 뿐이다.

또한 디지탈 서명을 활용하기 위해서는 해쉬함수, 키관리 메카니즘, 신뢰성있는 제 3자 등에 대한 표준화가 함께 이루어져야 하며 이들에 대한 표준화도 SC27에서 동시에 수행하고 있다.

미국은 국가 표준 디지탈 서명을 서두르고 있는 대표적인 국가로서 1991년에 DSS(Digital Signature Standard)안을 제안하여 안전성, 특허권 등과 같은 여러 문제점을 수렴하여 보완작업을 진행하고 있으며 빠른 시일내에 국가 표준으로 제정할 것이 예상된다. 일본에서도 ESIGN이라는 서명 알고리즘을 제안하고 있으며, 다른 국가들도 자국의 기술과 환경여건에 적합한 독자적인 국가 표준 서명 알고리즘을 제정하려는 움직임을 보이고 있다.

한편 우리 나라에서 디지탈 서명 표준화에 관한 기초 연구는 한국통신 정보보호학회, 개방형 통신학회를 비롯하여 한국전산원, 한국통신, 한국전자 통신연구소, 한국 산업표준원 등에서 산발적으로 수행되어 왔으나 구체적인 표준화 작업은 미진한 상태이다. 그러나 1994년도에는 ISO/IEC JTC1/SC27의 한국지부를 주축으로 하여 관련학회의 지원을 받아 국가 표준 디지탈 서명을 제정하기 위한 1단계 사업이 수행될 것으로 전망된다. 국가 표준을 제정하기 위해서는 산업체와 전산망을 운용하는 단체 및 공공기관 그리고 전문가들이 모두 합심하여 요구사항을 수렴하고 분석하여 우리 환경에 적합한 표준이 되도록 하여야 할 것이다.

4. 디지탈 서명의 구현 방안

4.1 디지탈 서명의 구현 환경

디지탈 서명을 구현하여 활용될 수 있는 여건을 마련하기 위해서는 다음과 같은 환경이 뒷받침되어야 한다.

첫째, 기술적인 환경이다.

사용자 요구사항에 맞는 서명 알고리즘을 개발하거나 기존의 알고리즘을 선택할 수 있어야 하며 부수적으로 필요한 해쉬함수, 고속 지수계산 알고리즘, 소수의 생성과 함께 키관리 메카니즘이 뒷받침되어야 하며 사용자 편의성과 성능 향상을 위해서는 IC카드를 이용하는 방안도 고려되어야 한다.

둘째, 관리적 환경이다.

기술적인 측면과 복합적으로 이루어져야 하지만 비밀키와 공개키의 생성, 분배 및 관리를 위한

키관리 센터의 기능설정 및 운영방안이 중요하며 분쟁시에 판정관 역할을 수행하고 사용자 편의성을 제공해 주는 신뢰성있는 제 3자의 운영도 필수적이라고 할 수 있다. 또한 지속적으로 축적되고 변경되는 각종 자료에 대한 관리 대책도 강구되어야 한다.

셋째, 법 제도적 환경이다.

디지탈 서명이 정착되기 위해서는 종이 문서를 사용하지 않더라도 법적인 보장을 받을 수 있고 책임 한계를 명확히 할 수 있는 제도적 장치가 필요하다. 특히 디지탈 서명은 재산상의 소유권이나 계약 분쟁의 원인이 될 가능성이 높기 때문에 명문화된 법적 뒷받침이 요구된다.

4.2 RSA와 DSS 디지탈 서명 방식

디지탈 서명 방식은 대부분 공개키 암호방식을 이용하고 있으며 개인키 암호방식을 이용하는 경우도 있으나 이때는 쌍방이 신뢰할 수 있는 공정한 제3자 또는 변조 불가능한 특수 하드웨어를 필요로 하기 때문에 더욱 어려워진다. 디지탈 서명 방식은 크게 메세지 회복형과 부가형으로 구분할 수 있으며 최근에는 부가형 서명 방식이 더욱 많이 논의되고 있다.

본고에서는 가장 대표적인 방식이라고 할 수 있는 RSA 서명 방식과 DSS 서명 방식의 특성과 기본 알고리즘을 간단히 소개하고자 한다.

4.2.1 RSA 서명 알고리즘

Rivest, Shamir, Adleman이 제안한 RSA 서명 알고리즘은 각 가입자별로 서로 다른 시스템 계수를 갖는다. RSA 서명 방식은 메세지 회복형과 부가형에 모두 사용될 수 있으나 여기에서는 부가형 방식을 설명한다.

가. 시스템 계수 선정

(1) 소수 p와 q : p와 q는 약 10^{100} 정도되는 비밀 계수

(2) 법 $n=pq$: n은 약 10^{200} 정도되는 공개 계수

(3) 해쉬함수 H : H는 임의의 메세지를 입력 받아 일정한 길이의 압축 스트림을 출력하는 보안성있는 함수

(4) 공개키 e, 비밀키 d : $ed \equiv 1 \bmod (p-1)(q-1)$

나. 서명 생성(송신자)

(1) H(M) 구함 (M은 문서 내용)

(2) $S=H(M)^d \pmod n$ 계산

(3) 서명 S를 M과 함께 수신자에게 보냄

다. 확인 과정(수신자)

(1) H(M) 구함

(2) $V=S^e \pmod n$ 계산

(3) V=H(M)을 확인하여 만족되면 적법한 서명으로 인정함

위의 시스템 계수 (4)에서 수신자는 공개키 e를 알고 있으므로 (p-1)(q-1)를 알 수 있으면 비밀키 d를 쉽게 계산할 수 있다. 즉 n을 소인수 분해할 수 있으면 d를 알 수 있으므로 RSA 서명 방식의 안전성은 소인수 분해 문제의 어려움과 일치한다. 그러나 n을 소인수 분해할 수 없으면 수신자는 서명을 확인할 수는 있지만 서명 S를 만들수는 없으며, 서명은 오직 송신자(서명자)만이 생성할 수 있게 되어 나중에 부인하거나 변조할 수가 없게 되어 앞에서의 [조건 2]를 만족시켜 준다.

4.2.2 DSS 서명 알고리즘

DSS(Digital Signature Standard)는 미국의 NIST에서 국가 표준으로 제안한 방식으로서 RSA 방식과 달리 모든 가입자들에게 공통으로 동일한 공개 계수를 갖거나 그룹별로 공유할 수 있으며 각 가입자는 자신들의 비밀키를 간직한다.

가. 시스템 계수

(1) 소수 법(prime modulus) p, $2^{511}<p<2^{512}$

(2) 소수 법 q, q |p-1이고 $2^{159}<q<2^{160}$

(3) $g=h^{(p-1)/q} \bmod p$, g>1이고 0<h<p

(4) 해쉬함수 H, 출력은 160비트

(5) 공개키 $Y=g^x \pmod p$, x는 비밀키이며, 0<x<q

나. 서명 생성(송신자)

(1) 0<k<q인 임의의 난수 k를 생성

(2) $R=(g^k \bmod p) \bmod q$ 계산

(3) H(M) 구함, M은 문서 내용

(4) $k^{-1}k \bmod q=1$인 k^{-1}계산 (k^{-1}은 k의 역원)

(5) $S=k^{-1}(H(M)+xR) \bmod q$ 계산
(6) 서명 (R,S)와 함께 문서 M을 수신자에게 보냄

다. 서명 확인(수신자)
(1) $W=S^{-1} \bmod q$ 계산
(2) H(M) 구함
(3) $A=H(M)W \bmod q$ 계산
(4) $B=RW \bmod q$ 계산
(5) $V=(g^A Y^B \bmod p) \bmod q$ 계산
(6) V=R을 확인하여 만족되면 적법한 서명으로 인정함

DSS의 안전성은 앞에서 설명한 이산대수 문제의 어려움에 근거하고 있으며 동일한 난수 k를 두번 사용하지 않도록 해야 한다. 미국의 NIST가 DSS 서명 방식을 제안할 때 고려사항은 서명의 안전성, 특허 저촉 문제, 수출 용이성, 국가적 보안, 법적 영향과 민간 부문의 활용성 등을 중요하게 평가하였다. DSS안에 대해서는 여러가지 긍정적인 면과 부정적인 면들이 검토되고 있으며 보완 작업이 진행중이다.

5. 결 론

지금까지 계산 이론과 관련하여 정수론에서 풀기 어려운 문제로 인정되고 있는 소인수 분해 문제와 이산대수 문제를 간단히 살펴보고 이들을 응용한 디지탈 서명에 대해서 기본적인 특성과 대표적인 서명 알고리즘을 소개하였다.

컴퓨터와 전산망이 선도하는 정보화 사회로 진입하기 위해서는 중요 문서 전송시에 요구되는 디지탈 서명의 필요성이 더욱 증대되고 있으며 현재 연구되고 있는 대부분의 디지탈 서명 알고리즘은 계산 이론에서 알고리즘의 난이도에 근거를 두고 있다.

디지탈 서명에 대한 국가 표준화와 활용성을 제고하기 위해서는 안전성 분석과 함께 부수적인 환경 여건이 충족되어야 할 것이다.

마지막으로 계산 이론을 연구하는 독자들이 이론 자체의 연구에 그치지 않고 실생활에 활용될 수 있는 응용 분야와도 연계시키도록 노력하는 분위기가 조성되길 기대한다.

참고문헌

[1] 남길현외, 전산망시큐리티 기술표준연구, 한국전산원, 1992.
[2] 박승안, 김응태, 정수론, 경문사, 1991.
[3] 원동호 외, 공중통신망에 적합한 한국형 디지탈 서명 메카니즘의 실용화 기술개발 및 표준화에 관한 연구, 한국통신 연구개발단, 1993.
[4] ISO/IEC JTC1/SC27, Information Technology-Security Techniques-Digital Signature Scheme with Appendix, 1992.
[5] NIST,Digital Signature Standard(proposal) ,1992.
[6] M.R.Schroeder, Number Theory in Science and Communication, Springer-Verlag, Berlin, 1984.
[7] J.Seberry and J.Pieprzyk, Cryptography, Prentice Hall, 1989.

남 길 현

1969 육군사관학교 졸업
1973 서울대학교 공과대학 토목과 졸업
1979 미 해군대학원(전산학 석사)
1983 위스콘신(메디슨) 주립대(전산학 석사)
1985 루이지아나 주립대(전산학 박사)
1985 ~현재 국방대학원 전산학과 부교수
관심 분야 : 컴퓨터 보안, 암호학, 데이타베이스, 알고리즘 분석