전자상거래에서의 RSA 알고리듬의 분석과 구현

우원택
경산대학교 정보과학과

1. 개요

- 역사:
1976 Diffe 와 Hellman: 공개키 암호시스템
Merkle-Hellman:
knapsack 암호시스템
1977 Rivest, Shamir, Adleman: RSA 암호시스템
1978 RSA 암호시스템공개
- 용도: 암호화, 전자서명
- 방법: 소인수분해
- 특징: 복호화보다 암호화가 빠르다.
서명보다 검증을 더 빠르게 수행
대칭키(DES)암호시스템과 함께 사용
DES 보다 100배(S/W 구현),
1000-10,000배(H/W 구현)느리다
현재 함호화는 DES 암호화에 사용된 세션키 암호화는 RSA로 HYBRID
암호시스템
- 안전도: 증명, 반증명 존재 무
- 소수의 수 :
n 보다 작거나 같은 소수의 수: n/log n
길이가 약 512비트의 소수의 수: 10^{150} 개 정도

- 소수 판정법
확률론적 소수 판정법
실제 소수가 아닐 확율: 2^{-100} 정도

2. RSA 알고리듬

가. 키생성

각실체는 RSA 공개키와 그에 대응하는 비밀키를 생성한다.
① 두 개의 (서로 다른) 큰 소수 p 와 q를 임의로 생성한다.
② n = pq 와 $\phi=(p-1)(q-1)$ 를 계산한다.
③ gcd(e, ϕ) = 1 인 정수 e(1<e< ϕ)를 임의로 선택한다.
④ 확장된 유크리드 알고리듬을 사용하여 ed ≡ 1(mod ϕ)인 유일한 정수
d (1<d< ϕ)를 계산한다.
⑤ A의 공개키: (n, e)
A의 비밀키: d
단, n 모듈러스 e 암호화 지수 d 복호화 지수라 함.

나. RSA

B는 메시지 m을 암호화 하여 A에게 보내고, A는 복호화 한다.
(1) 암호화 (B가 수행)
① A의 인증된 공개키 (n, e)를 얻는다.
② 메시지 m을 [0, n - 1]사이의 정수로 표현한다.
③ c ≡ m^e mod n를 계산한다.
④ 암호문 c를 A에게 보낸다.

(2) 복호화
① 비밀키 d를 이용하여 m ≡ C^d mod n를 계산한다.
예>(1) 키생성
① A는 소수 p = 2357, q = 2551를 선택하고, n = pq = 6012707와
ϕ = (p - 1)(q - 1) = 6007800을 계산한다.
② A는 e = 3674911을 선택하고, 확장된 유클리드 알고리듬을 이용하여,
ed ≡ 1(mod ϕ)인 d = 422191을 찾는다.
③ A의 공개키는 (07, e = 3674911)이고, 비밀키는 d = 422191 이다.
(2) 암호화
암호화할 메시지가 m = 5234673이라 하자.
B는 c = m^e (mod n) = $5234673^{3674911}$(mod 6012707) ≡ 3650502를
계산하여 A에게 보낸다.
(3) 복호화
A는 c^d (mod n) = 3650502^{422191}(mod 6012707) ≡ 5234673을 계산한다.

본사례>

평문 $M = M_1, M_2, ...M_{k-1}, M_k \rightarrow P_1P_2, ...P_k$

암호문 $C = C_1C_2 .....C_k \quad C_i = P_i^e \% n$

복호화 $P_i = C_i^d \% n = (P_i^e)^d \% n = P_i^{e.d} \% n$

공개키 (n = 2773, 2 = 17) 비밀키 d = 157

n(2773) = P(47) * P(59)

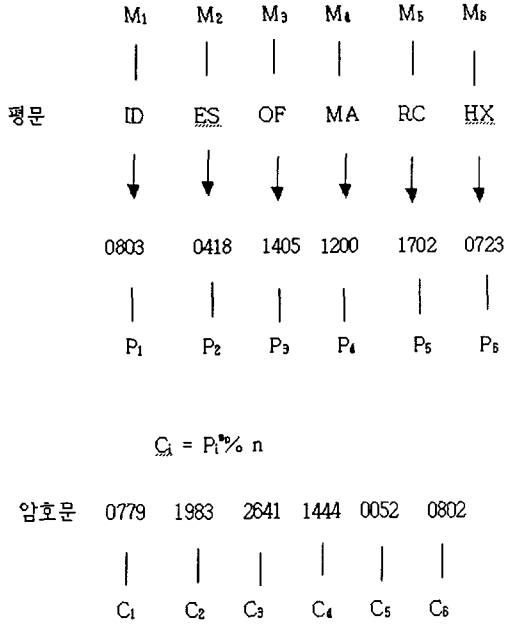
e의 선택: e.d % [(p - 1).(q - 1)] ≡ 1 이 되게

복호화 $P_i = C_i^d \% n$

3. RSA의 안전도

가. 소인수분해

공개키 (n, e)로부터 비밀키 d를 계산하는 문제와 n을 소인수분해하는 문제는 계산적으로 동등하다. 따라서 RSA에서는 n이 소인수분해 된다면, ϕ와 d를 계산하기 쉽다. 즉 복호화를 수행하여 암호문 c로부터 메시지 m을 얻을 수 있다. 다른한편 공격자가 d를 계산할 수 있다면, 다음과 같이 n을 쉽게 소인수 분해할 수 있다.



나, 작은암호화지수 e

작은 암호화지수 e = 3 은 작은 메시지 m에서 문제가 발생할 수 있다.

다. Forward 조사공격

메시지크기가 작거나 예측가능하면 암호문 C를 복호화 할 수 있으므로Salting(평문메시지에 적어도 64비트이상의 의사난수적으로 생성한 비트 스트링을 첨부하는것)에 의해 공격을 피할 수 있다.

라. 작은 복호화 지수 d

gcd(p-1, q-1)가 작고 그리고 d가 모듈러스 n 비트의 약 1/4 bit라면, 공개키 (n, e)로부터 d를 계산하는 효율적 알고리듬이 존재하며 이 공격을 피하기 위해 복호화 지수 d는 n의 크기와 비슷해야 한다.

마. 곱셈특성

RSA의 homomorphic성질($(m_1 m_2)^e \equiv m_1^e m_2^e = C_1C_2 \pmod n$)이 성립하므로 RSA암호화에 대한 adaptive선택-암호문공격의 빌미를 제공하며 이 공격은 평문메시지에 어떤 구조적 강제기능을 부과하여 이를 피할수 있다.

바. 공통모듈러스공격

RSA모듈러스 n을 각자 선택않고 공통선택한다면 (e_1, d_i)와 같이 공개적으로 활용가능한 정보만을 사용하여 높은 확률로 메시지를 복원할 수 있다.

사. Cycling공격

Cycling공격은 $f = \gcd(C^{en} - c, n) > 1$ 인 가장 작은 양의 정수 u를 찾는 것으로 Cycling공격은 n을 소인수분해 하는 데에 사용될 수 있다. 소수 p와 q를 임의로 선택하면 이 공격을 피할 수 있다.

아. 메시지감추기

$m^e \equiv m \pmod n$에 의해 항상 감추어지지 않는 메시지가 존재한다.(예, m - 0,m - 1, 그리고 m - n - 1) 그러나 p, q가 임의의 소수이고 e 가 임의로 선택된다면 (만일 e가 e = 3 또는 $e = 2^{16} + 1 = 65537$과 같은 작은수라면) RSA암호문에 의해 감추어지지 않은 메시지의 비율은 무시할 만큼 적다.

자. Wiener 공격

e, n을 사용한 Continued Fraction Approximation을 사용하여 d를 복구가능

하며 이 공격법은 RSA모듈러스에 비해 d가 상대적으로 작을 때 $d < n^{1/4}$일 때

실용적이므로 d를 선택할 때 너무 작지 않게 선택하여야 한다.

차. 확율적소수사용

모듈러스계산에 사용된 소수중의 하나가 실제 소수가 아닌 경우 즉 비-소수의 출력가능성은 아주 작으며 설사 나타나드라도 모두 제거할 수 있다.

4. 구현

가. H/W

<표1> 현존하는 RSA CHIP

회사	Clock 속도(MHz)	512비트 당처리 속도율(K)	512비트 암호당Clock Cycles(M)	기술(micron)	Chip당 비트	트랜지스터 개수
Alpha Techn.	25	13	.98	2	1024	180,000
AT&T	15	19	.4	1.5	298	100,000
British Telecom	10	5.1	1	2.5	256	-
Business Sim Ltd.	5	3.8	.67	Gate Array	32	-
Calmos Syst. Inc.	20	28	.36	2	593	95,000
CNET	25	5.3	2.3	1	1024	100,000
Cryptech	14	17	.4	Gate Array	120	33,000
Cylink	30	6.8	1.2	1.5	1024	150,000
GEC Marconi	25	10.2	.67	1.4	512	160,000
Pijnenburg	25	50	.256	1	1024	400,000
Sandia	8	10	.4	2	272	86,000
Siemens	5	8.5	.03	1	512	60,000

자료: 한국정보보호센터 기술본부/기술연구팀, RSA 공개키 암호시스템 현황, 1998년 5월

나. 속도

	512비트(sec)	768비트(sec)	1024비트(sec)
암호화	0.03	0.05	0.08
복호화	0.16	0.48	0.93
서명	0.16	0.52	0.97
검증	0.02	0.07	0.08

<표 2> 8비트 공개키를 가진 다른 모듈러스 길이에서 속도

RSA는 H/W로 구현되었을 때, DES보다 1000배 정도 느리고, S/W로 구현되었을 때, DES 보다 100배 정도 느리다.

(SPARC II에서)

자료: 한국보호센터 기술본부/기술연구팀, RSA 공개키 암호시스템 현황, 1998년 5월

5.결연

본연구에서는 전자상거래에서의 RSA 알고리듬의 응용분야와 RSA 알고리듬의 구조적 분석을 함으로써 공개키 암호화 기법에 대한 개념을 파악하고 실제 Visual C++로 RSA 알고리듬을 프로그래밍하여 이를 실행해 봄으로써 RSA 알고리듬의 실제적 구현을 통한 비밀키 암호기법에 대한 이해를 높혔다고 할 수 있겠다. 그리고 RSA 암호화 기법의 안전성에 대해서도 문헌고찰을 통하여 검토해 보았다. 본 연구에서의 RSA 알고리듬은 비교적 단순한 것으로 실제적으로 사용되는 RSA 알고리듬은 더욱 확장되어 사용되어 사용되고 있을 것이다. 미국정부는 암호장비들을 무기로 분류하고 그 수출을 제한하고 있다. 하지만 RSA 알고리듬은 전문지들을 통해 세계적으로 유포된 상태이므로 원하는 사람이면 누구나 이 알고리듬을 손에 넣을 수 있다. 현재 상업용에는 RSA암호가 널리 이용되고 있으나 최근 타원곡선암호가 국내외의 몇몇 기업체에서 구현/실용화하고 있다. 그리고 국제표준화기구인 ISO/SC27 나 IEEEp1363에서 타원곡선을 이용하는 방식의 표준화가 추진되고 있으며 금후에는 RSA와 함께 이용될 것으로 생각된다. 이때 복수암호방식의 병용으로 인한 상호 운용성의 문제가 생기는데 이점에 대해서는 송수신 간에 이용 가능한 암호 방식을 선택하고 네고하는 프로토콜에[1] 의하여 해결돼 갈 것으로 생각된다. 그리고 최근 종전의 공개키암호와는 다른 수학적 문제에 안전성의 근거를 두는 새로운 공개키 암호가 제안됐다. 이것은 <유클리드(Euclid)>공간의 격자에 관한 수학적으로 어려운 문제에 안전성의 근거를 두는 방식이며 이론적으로는 흥미가 많으나 1bit 마다 암호화하기 때문에 효율이 대단히 나쁘고 현시점에서는 실용화할 단계에 이르지 못하고 있다. 전술한 RSA 방법은 완벽하지는 않다. 공용 키들을 공용화할 수 있지만, 이 공용 키들의 신뢰도는 어떤 사람이 실제로 광고하는 공용 키가 그들만의 것임을 보증하는 믿을 만

1) 컴퓨터 상호간의 대화에 필요한 통신규약을 말한다.

한 방법이 있을 때만 그 효과를 믿을 수 있다. 그러나 RSA 공용 키 테크닉은 더 쉬운 여러 가지 방법보다 강력하고 안전하다[2]. 그러나 큰 수들을 분쇄하는 새로운 테크닉들이 고안되면서, RSA는 그 효과를 잃고 있다. 또, RSA가 처음 도입되었을 때보다 컴퓨터 처리 능력들이 상당히 향상되었기 때문에 사이즈가 작은 키들에 대한 무차별 공격 시도들이 가능해졌다. 1994년 한 집단에서 129자리의 RSA 모듈들을 분쇄했다[3]. 이 집단이 150자리의 공용키를 분쇄하려 했다면 약 200년이 걸렸을 것이다. 더 빠른 처리능력을 갖춘 더 저렴한 워크스테이션들이 오래지 않아 만들어 지면 공용키의 사이즈는 훨씬 더 길어져야 보안을 유지할 수 있을 것이다. 우리나라의 경우 이미 전자거래기본법과 전자서명법이 발효되고 현재는 중단상태이지만 암호이용촉진법 제정을 추진하고 있으며, 표준암호 알고리듬 제정에도 나서고 있다. 국가적 차원에서의 정보보안에 대한 종합대책을 시급히 마련하고 정보보호 업무를 종합적.체계적으로 추진하기 위하여 한국정보보호센터가 설립되어 활발한 활동을 수행하고 있다. 또, 전자서명 기술을 활용한 전자서명을 안전하고 신뢰성있게 이용할 수 있는 환경을 조성하고 공인인증기관을 효율적으로 관리하기 위하여 전자서명인증관리센터가 설립되어 본격적인 전자상거래 시대에 적극적인 대처를 하고 있다. 학계와 관련기관에서도 선도적인 암호관련 연구개발을 수행하고 있으며 업계쪽에서도 암호전문 업체들이 자체 기술력으로 상용암호화 기술을 이미 확보하여 활발히 제품을 공급해오고 있다. 정보통신부는 한국정보인증(주)과 한국증권전산(주)을 전자서명공인인증기관으로 지정했으며 이 기관들은 앞으로 인증서 발급을 비롯, 내용증명, 전자공증, 신용증명, 전자거래인증, 휴대전화를 비롯한 단말기 인증 업무를 수행한다.[4] 오늘날의 정보시스템은 개방화와 접속성이 급격히 증대되고 있으므로 필연적으로 조직 외부로부터의 보안 위협을 높여주게 된다. 따라서, 전자상거래 시스템과 같이 이러한 특성이 극대화되는 정보시스템에 대한 적절한 보안대책의 강구는 필수적이라 하겠다.[5] 최근 커머스넷이 전세계를 대상으로 한 설문조사 자료에 의하면 99년 전자상거래 걸림돌 1위는 보안 및 암호화 문제였다. 98년의 경우에는 보안 및 암호화 문제의 순위는 하위에 머물러 있었는데, 보안 및 암호화 문제의 비중이 이같이 증가한 원인은 전자상거래를 도입하는 기업이 증가함에 따라 보안상의 위험도에 대한 인식이 확산되었기 때문이다. 즉, 전자상거래 도입 초기만 해도 비즈니스 모델링이나 전자상거래 애플레이션간, 그리고 레거시 시스템과의 상호운용성이 주요 관심사였다. 실제 시스템 구현과 서비스 확대로 시장이 성숙되면서 핵심적인 문제가 비로소 드러나게 된 것이다. 이같은 전자상거래 시장과 정보보호산업과의 밀접성으로 전자상거래 시장의 급속한 성장과 함께 정보보호산업 시장의 규모 및 점유비 또한 급속한 성장이 예측되고 있다. 암호기술 분야가 갖는 안보적인 측면이나 경제적인 측면의 특성과 중요성은 미국의 암호정책 추이를 보면 알 수 있는바 미국은 테러국가나 집단의 오용에 대한 우려를 이유로 40비트 이상의 암호기술에 대해서는 수출을 금지해 오다가 지난해 7월부터 제한된 국가에 한하여 56비트 이하의 암호기술 수출을 허용하였다. 한편, 지난해 12월 오스트리아 비엔나에서 바세나르협약국인 33개국은 64비트 이상의 암호기술의 수출을 제한하는 새로운 협약을 체결하였는데 사실상 미국의 주도로 이루어진 이 협약은 미국을 제외한 128비트 암호기술을 확보한 국가들의 수출을 제한하려는 목적에서 이루어진 측면이 강하다. 미국은 앞으로 암호관련 기술력 장악을 통해 2000년까지 600억 달러 이상의 수출효과를 기대하고 있다.

2) Pete Loshin저. 새라새것역, 전자상거래의 모든 것, 성안당, 1997년, p.46

3) 약 8개월 동안 수백대의 워크스테이션을 이용했다.

4) 조선일보, 해킹잡는 보안업체 햇빛, 2000년 2월 11일, p.13

5) 김종기, 정보시스템보안의 효과성 모형에 관한 실증적연구, 정보시스템연구제7권제2호정보시스템학회, 1998년 12월, p. 105

참고문헌

김권식편저, 노턴유틸리티 6.01 완성, 삼양출판사, 1993, pp.176-182

김영건, 정보시스템 Security 의식실태에 관한 비교연구-한일정보처리정보요원중심으로, 정보시스템연구제5권, 한국정보시스템학회, 1996년 12월, pp.43-70

김종기, 정보시스템보안의 효과성 모형에 관한 실증적연구, 정보시스템연구제7권제2호정보시스템학회, 1998년 12월, pp.91-108

김철, 암호학의 이해, (주) 영풍문고, 1996

네트워크컴퓨팅솔루션팀 한국아이비엠, SET을 이용한 IBM전자상거래솔루션, e-business 솔루션포럼, 한국아이비엠(주), 1997년 5월 30일, pp.1-46
박봉주, 다중계층키 관리(Multilevel Security), 이화여자대학교수리과학연구소, 1998년 10월, pp. 121-133
박영호.이창순, 3세대 이동통신 시스템에서의 보호, 한국산업정보학회/한국정보기술응용학회/한국정보전략학회 추계공동학술대회논문집, 1999년, pp.579-589
심상규, Primes in Cryptography, 이화여자대학교수리과학연구소, 1998년 10월, pp.100-106
신장균. 황재준, 전자 지불 시스템의 보안 평가 기준, CALS/EC KOREA'99, Proceedings of International Conference vol. 2, 한국전자거래학회, 1999년 7월, pp. 491-500
시큐리티정보, 21세기 정보사회와 암호학, 월간정보보호21C,pp. 59-62
안중호.박철우, 인터넷과 전자상거래, 홍문사, 1999
안창준, 전자상거래시스템의 핵심기술 '정보보호', 월간정보보호21C, pp.22-25
임국인, 공개키 암호법과 수학의 역할, 이화여자대학교수리과학연구소, 1998년 10월, pp.87-92
임규건, 이재규, 전자지갑의 구조 현황과 차세대 구조 설계, Proceedings of CALS/EC Korea'98 International Conference vol.2, 한국 CALS/EC 학회, 1998년, 10월, p.391
임춘성.김법조옮김, 전자상거래, 북플러스, 1998
이경석, 제5회정보보안기술표준화워크샵 Seminar지상중계, 월간정보보호21C, pp.108-114
이병철, 전자지불서비스, EC-CALS저널, 1999년6월 No.2, pp.34-37
이재규, 최형림, 김현수, 이경전 편저, 전자상거래 원론, 법영사, 1999년, p. 258
이창순, 디지털도서관과 지식인프라 구축, 제2회 디지털도서관 컨퍼런스 논문집, 한국데이타베이스진흥센터, pp.139-147
이창순, 디지털 테이터의 정보보호와 저작권보호, 제2회 디지털도서관 컨퍼런스 논문집, 한국데이타베이스진흥센터, 1999년, p.140-141
이창순, 스마트카드를 이용한 전자지불시스템, 한국산업정보학회논문지 제4권 제1호, 1999년 3월, pp. 97-101
이형원편저, 정보시스템안전대책, 영진출판사, 1993
전자상거래실증추진협의회, 암호이용기술핸드북, 1998년 2월, 전자상거래실증추진협의회공동시큐리티관련기술검토WG
전자상거래실증추진협의회, 비즈니스프로세스 검토 가이드라인, 1998년 3월, 전자상거래 실증추진협의회전자공증검토 WG, 비즈니스프로세스검토 WG
전자상거래실증추진협의회, 인증에 관한 외국의 법제도 조사보고서, 전자상거래 실증추진협의회인증국검토 WG, 1998년3월
전자상거래실증추진협의회, 해외EC관련기업.조직등의 동향조사, 전자상거래실증추진협의회 국제제휴 WG, 1998년 3월
전자상거래실증추진협의회, 인증국운용가이드라인, 전자상거래실증추진협의회인증국검토 WG, 1998년 3월
전자상거래실증추진협의회, 상호인증가이드라인, 전자상거래실증추진협의회 인증국검토 WG, 1998년 3월
정광호, Visual C++5.0 비주얼하게 배우기, 북스힐, 1998
조선일보, 해킹잡는 보안업체 햇빛, 2000년 2월 11일, p.14
한국정보보호센터 기술본부/기술연구팀, RSA 공개키 암호시스템 현황, 1998년 5월
황대준.엄영익공저, C++프로그래밍, Scitech, 1999
홍기융, 안전한 전자상거래환경구축, 월간정보보호21C, pp.32-36

Ahuja, Vijay, Network & Internet Security, AP Professional, 1996, p.159
Cary A. Jardin, Java Electronic Commerce, Wiley Computer Publishing, 1997
Gurpreet Dhillon, Managing Information System Security, Macmillan, 1997
Louise Yngstrom and Jan Carlsen, Information Security in Research and Business, Chapman & Hall, 1997
Kate Maddox and Dana Blankenhorn, Web Commerce -Building a Digital Business, John Wiley & Sons, Inc. 1998
Pete Loshin저, 새라새것역, 전자상거래의 모든 것, 성안당, 1997
Nyhoff, Larry, C++ An Introduction to Data Structures, Prentice Hall, 1999
POSTECH, Security+ for Unix, POSTECH Laboratory for UNIX Security, fourth edition, 1987

http://digital.verisign.com/index.html
http://digital.verisign.com/client/help/ms_managing.htm
http://digital.verisign.com/client/help/ms_sign.htm
http://digital.verisign.com/client/help/ms_sign.htm
http://digital.verisign.com/client/help/ms_encrypt.htm
http://grouper.ieee.org/groups/1363
http://my.netian.com/~dubs37/cyber_law.htm
http://myhome.netsgo.com/lyra97/security2.htm
http://myhome.netsgo.com/lyra97/security4.htm
http://myhome.netsgo.com/lyra97/security6.htm
http://www.microsoft.com/windows/ie-int/ko/features/certpage.htm
http://www.rootca.or.kr/index.htm
http://www.rsa.com/rsalabs
http://www.securityinformation.com
http://www.verisign.com/client/help/index.html
http://www.verisign.com/client/index.html
http://www.verisign.com/secureemail/guide
http://www.verisign.com/smine/networkinternet open
http://www.verisign.com/securemail/guide