기밀성과 인증성을 보장하는 암호 기술
Recent Cryptographic Techniques preserving Confidentiality and Authentication

김 광조
Kwangjo Kim

한국정보통신대학원대학교
Information and Communication University

(요약문)

지식 정보사회로의 발전에 따라 부수적으로 발생하는 정보의 불법도청, 악용, 개조 등 역기능에 대비하기 위한 암호기술의 필요성이 증대하고 있다. 본고에서는 암호 기법에서 가장 널리 이용되는 기밀성 확보를 위한 비밀키 암호로 DES를 비롯한 AES의 추진 현황을 소개하고, 인증성을 확보하는 공개키 암호의 대표적인 알고리즘인 DH, RSA 등을 소개하고 새로운 공개키 암호 방식에 대하여 기술한다. 미국의 AES 추진 계획에 자극을 받은 유럽 및 일본은 자국의 암호 산업 보호 및 전자 정부 구축을 위한 암호 방식의 공모 계획을 최근 수립하였는 데 그 내용을 소개하고 암호 기술의 향후 발전 전망을 제시하였다.

I. 서론

급속한 정보통신망의 발전을 통하여 우리는 언제, 어디에서 누구와도 정보 교류가 가능한 새로운 새 천년을 맞고 있으며, 새로운 통신 서비스로서 기업과 기업간 (B2B) 또는 기업과 소비자간 (B2C)의 전자 상거래, 전자 화폐, 전자 증권, 전자 입찰, 전자 은행, 멀티미디어 콘텐트 등 다양한 사이버 서비스가 전개되고 있으며, 향후 기업과 정부간 (B2G)의 전자상거래도 예측되고 있는 지식 정보화 사회를 맞이하고 있다.

이러한 서비스는 사용자가 세계 어디에 있든지 이용할 수 있는 공개된 사이버 공간을 이용하므로 접근성과 편리성을 용이하게 제공하는 반면, 역으로 누구든지 접근 가능하다는 공개적인 통신로 상의 정보를 도청이나 감청하는 제 3 자의 불법 행위와 합법적인 통신 상대방간에도 비대면이라는 네트워크 상의 특징을 이용하여 불법 접근을 시도한다거나 교신 사실을 부인하는 행위가 발생한다. 따라서 안전하게 사이버 서비스를 이용하기 위해서는 보안 기술이 필수 불가결하게 요구된다.

실제로 현행 인터넷의 보안 구조상의 문제점으로 인하여 네트워크 상의 정보를 불법적으로 감청하여 정당한 통신자의 패스워드 훔쳐보기 (password sniffing)를 손쉽게 할 수 있을 뿐만 아니라, IP spoofing 공격, TCP/IP 세션 가로채기, SYN 정보를 반복적으로 특정 호스트에 주입하여 호스트의 장애를 유발시키는 서비스 부인 (denial of service) 행위 등이 가능하다. 또한 현행 인터넷은 90년대 초에 보급되기 시작하여 현재는 컴퓨터의 보급과 함께 폭발적인 증가세를 보여 고유 주소에 해당하는 IP 주소의 고갈 등의 문제점을 드러내고 있다. 현재 이런 문제점등을 고려한 새로운 인터넷과 이 새로운 인터넷의 보안 구조가 제시되고 있다. 이러한 추세를 보면 보안 기술은 모든 분야에서 선택 기술이 아니라 필수 기술로서 부각되고 있으며 특히 전자 상거래 시스템의 보급과 함께 중요성이 더욱 인식되고 있다.

암호 기술은 전통적으로 군용, 외교, 군사 목적으로 필요성이 인식되어 오래전부터 비공개로 이용되어 왔으나 미국은 연방정부 데이터 보호 목적으로 DES (Data Encryption Standard)[1]를 표준으로 77년 제정하면서 공개적인 학술 연구가 시작되었다고 할 수 있다. 그러나 비밀키 암호는 암호 사용자가 증가하면 관리하여할 키가 증가하여 관리 상의 문제점이 있다. 이러한 문제점을 해결하기 위하여 기존의 비밀키 개념에서 달리한 공개키 암호 알고리즘으로 DH(Diffie-Hellman) 공개키 암호 방식이 발표되었다. 그후 암호 알고리즘은 각국의 독자 알고리즘의 개발을 거쳐 발전하여 왔다.

새로운 천년인 21세기를 맞이하여 암호 기술은 컴퓨터 기술의 발전과 더불어 안전성의 기준이 발표 당시와 달리 적용하여야 하는 점과 해독 기법의 발전으로 종래에 안전하다고 주장한 암호 알고리즘이 쓸모 없게 되는 최근 사례도 생기었다. 예를 들면, 99년도 노르웨이 15세 소녀가 제안한 새로운 공개키 암호 방식은 1년 후 해독 방식이 발표되기도 하였다.

본 논문의 구성은 다음과 같다. 제 2 장에서는 발생 가능한 보안 취약점으로 정보의 위협 방식과 그 대책을 기술한다. 제 3 장에서는 이러한 위협으로부터 기밀성을 제공하기 위하여 64비트 이상의 정보를 처리하는 비밀키 암호 방식으로 블록 암호인 DES를 소개하고 해독 방식이 발표됨에 따는 후속 조치로 미국의 AES 암호의 추진 현황을 ,소개한다. 제 4장에는 정보의 인증성을 보장하기 위하여 주로 사용되는 공개키 암호 방식으로 키 관리 용 DH 공개키 암호, RSA 공개키 암호를 기술하고 최근에 새롭게 제안한 XTR, 따임이론을 이용한 공개키 암호를 소개한다. 제 5 장에서는 미국의 AES 계획에 자극을 받은 유럽과 일본은 자국의 암호 산업의 육성과 전자정부 구축을 위한 프로젝트를 소개하고 제 6 장에서는 향후 암호 기술의 발전 전망을 포함하여 결론을 맺는다.

II. 정보의 보안 위협과 대책

2.1 보안 위협

중요한 정보를 가공, 전달, 저장 중에 발생되는 위협으로는 불법적인 제 3 자와 합법적인 통신 상대방에 의한 행위로 구별되며 제 3 자에 의한 보안 위협으로는

(1) 기밀성의 상실 : 정보가 부당하게 노출됨.

(2) 무결성의 상실 : 정보가 불법 개조, 변조됨.

(3) 가용성의 상실 : 보존된 정보나 자산이 제3자의 컴퓨터에 부당하게 사용됨.

등의 3 가지로 나눌 수 있다.

한국정보보호센터 내의 침해사고 대응팀의 최근 보고서[2]에 의하면 이와 같은 보안 위협으로 인해 불법적인 해커들이 ID와 패스워드를 도용한다던가, 특정 해킹 프로그램 등을 이용한 정보통신망의 해킹 행위가 점차 증가하고 있다고 한다. 이러한 행위를 하는 사람들은 (a) 크랙커 (b) 외국의 스파이 (c) 테러리스트 (d) 산업 스파이 등이라고 추정되며 이러한 공격은 직접적 공격과 간접적 공격으로도 구별할 수 있다.

(1) 직접적 공격: 악의의 제 3 자가 자신의 컴퓨터를 직접 조작하여 통신로를 경유를 이용하여 네트워크에 연결된 컴퓨터로 침입하여 파일 등에 피해를 준다. 또한, 보안 허점 (security hole)을 교묘히 찾아서 대상이 되는 컴퓨터에 침입하는 행위로 부정 접근이라고도 한다.

(2) 간접적 공격: 악의의 제 3자가 부정한 소프트웨어를 목표 컴퓨터에 삽입시켜 이 소프트웨어를 이용하여 컴퓨터 내부의 파일을 공격한다. 이런 공격의 예로는 컴퓨터 바이러스에 의한 공격이 해당된다. 1999년에 국내에 최초로 엄청난 피해를 CIH 바이러스의 내부 구조와 대책은 참고문헌[3]에 자세히 기술되어 있다.

또한, 합법적인 통신 상대방에 의한 부정으로는 인증성의 상실을 들 수 있다. 즉, 통신 상대방이 계약문서 상의 일부 내용을 변조한다던가 거래 내용을 부인하는 행위가 발생할 수 있다. 예를 들어, 100,000원을 송금하였다 하였는데 10,000원을 수신하였다고 하는 부정한 행위에 대한 증거를 제시할 수 있는 수단이 제공되어야 한다. 이러한 송수신 사실을 부인을 방지하는 기법으로 공개키 암호 기법을 활용한 전자 서명 방식을 이용하면 효과적으로 대처할 수 있다.

2.2 보안 대책

가. 제 3 자의 위협으로부터 보안 대책

<표1> 에서 보듯이 직접적인 대책과 간접적 대책이 분류하며 간접적 대책으로는 보안 감시, 보안 감사, 보안 평가 등이 있으며 보안 대책을 확고히 하기 위하여는 반드시 행하여야 한다.

직접적인 대책은 접근 관리 기술과 공격 대상이 되는 통신로나 파일내의 정보를 부정 접근을 방지하는 기술을 의미한다. 접근 관리가 제대로 되면 공격에 필요한 정보를 추가하는 것이 불가능하며 기밀성, 무결성, 가용성의 상실 대책 효과가 있다. 이러한 접근 관리 기술은 다음의 2가지 기술로 분류된다.

<표 1> 보안 위협과 대책

보안 위협		보안 대책			
		직접 대책	효과	간접 대책	효과
제 3 자에 의한 위협	(1) 기밀성의 상실	접근 제어 암호화	방지	바이러스 예방 프로그램, 감시, 감사 등	검출 예방
	(2) 무결성의 상실	접근 제어 암호화	방지	바이러스 예방 프로그램, 감시, 감사 등	검출 예방
	(3) 가용성의 상실	접근 제어	방지	바이러스 예방 프로그램, 감시, 감사 등	검출 예방
통신 상대방의 위협	(4) 증거성의 상실	디지털 서명	방지 검출		
	(5) 불법 복제			Watermarking	검출 예방

(1) 사용자 인증 기술

사용자가 본인임을 증명하는 기술로 본인 확인 기술이라고 하며 현재는 패스워드 만을 이용한 것이 일반적이나 일방향 함수를 이용한 암호 시스템이나 해쉬 함수를 이용한 도전-응답 프로토콜에 의한 인증 방식 및 영지식 상호 대화형 증명 방식 등 강력한 암호 기술을 이용한 방식도 실용화되고 있다. 또한, 개인별 생체 정보의 유일성을 이용한 지문, 성문, 얼굴모양, DNA 정보 등을 겸용하여 인식하는 기법도 가능하다.

(2) 접근 제어 기술

이것은 사용자가 허가된 권한 이상으로 접근을 방지하는 기술로 네트워크의 연결점에 부정한 접근을 방지하기 위한 방화벽 (Firewall) 시스템을 이용하여 제어할 수 있다. 이런 접근 통제 기법은 MAC(Mandatory Access Control)과 DAC(Discretional Access Control) 기법이 있으며 최근 실체가 수행할 수 있는 역할에 기반한 RBAC(Role Based Access Control) 기법의 연구가 진행 중이다.

위에서 열거한 접근 관리 대책을 세웠다 하여도 제 3 자가 합법적인 타인으로 위장한다던가 보안 허점을 이용하여 침입할 가능성도 있다. 암호 기술은 접근 통제가 실패하여 제 3 자가 정보를 입수하였다고 하더라도 그 문자나 데이터를 변형하여 이해할 수 없게 하는 보호 기술이다.

나. 통신 상대방의 위협으로부터의 보안 대책

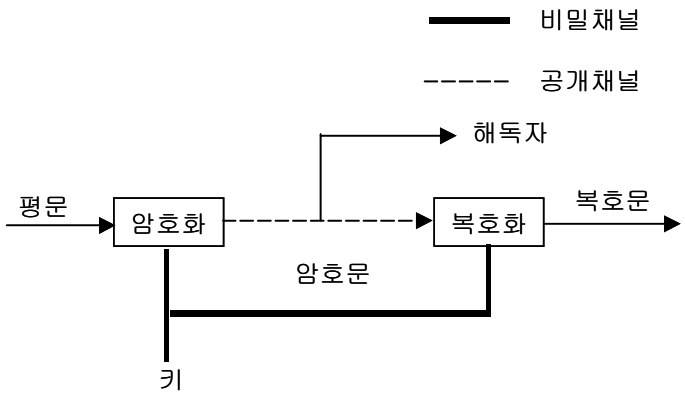
네트워크를 이용한 거래 사실을 부인하는 등의 문제를 방지하기 위하여는 통신 쌍방이 정보 내용에 대하여 행위를 한 사실을 증명할 수 있는 수단이 필요하다. 이러한 수단으로 종래에 계약서 등에 날인하는 기술이 이용되었듯이 네트워크 상에서 디지털 컨텐트에 전자적으로 서명하는 전자 인증 기법이 있다. 또한 이 전자 인증 기법을 이용하여 디지털 컨텐트의 불법 복제를 방지할 수 있으며 디지털 복제가 되었다고 하더라도 지적 소유권을 주장하게 할 수 있는 Watermarking[4] 기법도 이용된다. 한편, 컴퓨터에 저장 중이거나, 통신망을 통하여 전송 중인 정보의 보호를 위해 많은 방법들이 이용된다. 정보에 물리적인 접근을 통제하는 것으로부터, 패스워드의 다단계 이용, 컴퓨터 운영 체계의 강화 등 많은 수단이 있을 수 있다.

III. 비밀키 암호 시스템

3.1 개 요

암호의 시작은 로마 시대로부터 필요성이 인식되었다. 시저는 보호하려고 하는 평문인 영문 알파벳을 단순 천이하여(암호화) 원래의 정보(평문)를 변환한 정보(암호문)를 전달하였다고 하며 합법적인 수신 상대방은 역 천이 변환(복호화)하여 복호문을 복원하는 방법을 사용하였다고 한다. 이때 평문을 암호문으로 천이한 수를 키라고 할 수 있으며 합법적인 통신 쌍방간에는 비밀로 유지하여야 한다. 이 후 1, 2차 세계 대전 중에는 기계적인 방법을 이용한 Rotor Machine등을 이용한 암호 시스템이 이용되었으나 해독이 수월하여 현재는 사용하지 아니하다.

비밀키 암호 시스템은 (그림 1)과 같이 구성된다. 평문과 키를 이용한 암호화 변환과 공개되고 누구든지 접근이 가능한 채널을 통하여 정보를 전달하고 비밀로 가지고 있는 수신자는 암호화 변환의 역 변환인 복호화 변환을 하여 원래의 평문을 복원한다.

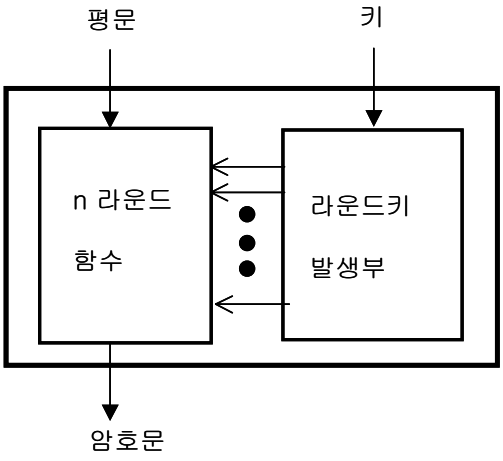


(그림 1) 비밀키 암호 시스템의 구성

한편 해독자는 접근 가능한 공개 채널을 통한 입수한 암호문으로부터 모르는 키나 평문을 추출하려고 하는 해독행위를 한다. 해독자에게 가용한 정보의 종류와 해독 행위의 상황에 따라 암호문 단독 공격(Ciphertext Only Attack), 기지 평문 공격 (Known Plaintext Attack), 선택 평문 공격 (Chosen Plaintext Attack) 등으로 구별된다. COA는 수동 공격이라고 하며 KPA, CPA는 능동 공격이라고도 분류한다. 비밀키 암호는 재래식 (Conventional) 암호 시스템, 또는 키가 동일하므로 단일키(one-key) 또는 대칭형 (Symmetric) 암호 시스템이라고 부르기도 한다.

현대 암호 시스템은 1949년대에 와서 정보이론의 대가인 Shannon[5]은 확산(Diffusion)과 혼동(Confusion)을 교대로 사용하는 변환(Mixing Transformation)을 이용한 암호 시스템의 구성을 제안을 시작점이라고 할 수 있다. 안전한 암호 시스템은 평문의 정보를 암호문의 전체에 고루 분산시켜야 한다. 평문의 각 사용 문자에 대한 정보가 암호문 전체에 분산되는 특성을 확산이라고 한다. 이 확산의 정도가 커질수록 암호 해독자는 더 많은 양의 암호문을 필요로 하게 된다. 또한 안전한 암호 시스템은 암호 해독자가 평문의 문자와 암호문의 문자 사이의 대응 관계를 알 수 없도록 하여야 하는데 이러한 특성을 혼동이라 한다. 혼돈과 확산 함수 자체는 암호학적으로 약한 함수이나 여러 회 반복 사용하면 암호학적으로 강한 함수를 구성 할 수 있다는 점을 가지고 있다.

일반적으로 비밀키 암호는 64비트 이상의 정보를 동시에 처리하기 때문에 (그림 2)에서 보듯이 블록 암호라고도 부르고 있다. (반면 1 비트 단위로 암호화 처리하는 방식은 스트림 암호라 하고 본고에서는 기술을 생략한다.) 또한, 복호화를 위하여 동일 함수를 2회 동작시키면 원래의 정보를 복원하는 Involution 함수를 라운드 함수로서 사용이 되고 있으며 이 라운드 함수에는 라운드 키를 생성하는 라운드 키 발생부와 함께 동작하게 되어 있고 동일한 반복 연산을 16회 이상을 반복 처리하여 최종 암호문을 생성하도록 되어 있다. 이런 반복 효과를 최단 반복 회수에 목표를 달성하기 위하여 입력 블록을 2개로 이등분하여 처리하는 구조를 Feistel 형태라고 한다.



(그림 2) 블록 암호의 구성

이런 블록 암호는 실시간으로 암호화가 요구되는 음성, 데이터를 비롯한 150Mb/s에서 2 Gb/s의

고속 디지털 다중 정보 보호에 사용되고 있으며 정보의 기밀성에 필수적으로 소요되며 사용 시에는 동작 모드로는 ECB(Electronic Code Book), n-bit CFB (Cipher Feed Back), CBC(Cipher Block Chaining), n-bit OFB (Output FeedBack) 모드가 있으며 응용 목적에 맞도록 선택하여 사용하며, 실제 운용을 위하여는 키 관리 방법, 암호화가 행하는 구간 선정, 암호 시스템을 소프트웨어 또는 하드웨어로 구현 할 것인지 등 여러 가지를 결정하여야 한다.

3.2 DES

가. 구성

70년도에 미국 연방정부의 데이터 보호를 위한 표준 알고리즘으로서 56비트 키를 가진 대칭키 암호 알고리즘인 DES를 채택한 바가 있다. 이후 DES는 전세계적으로 파급되어 정보 통신을 비롯한 금융 등 각 방면에 실질적으로 세계에서 가장 많이 사용된 암호 알고리즘이 되었다.

DES는 64비트의 평문을 64비트의 암호문으로 만드는 블럭 암호 시스템으로 64비트의 키를 사용한다. 이 64비트의 키 (외부 키) 중 56비트는 실제 키(내부 키)가 되고 1 바이트 당 한 비트는 패리티 비트로 사용된다. DES는 16라운드의 반복적인 암호화 과정을 가지고 있으며, 각 라운드마다 56비트의 내부 키에서 나온 48비트의 키가 섞여서 암호문을 만든다. 복호화는 암호화 과정과 동일하나 라운드 키만 역순으로 작용시키면 된다.

평문을 2등분하여 32비트 단위 블럭을 처리하도록 되어 있는 데, 왼쪽 32비트 블럭과 오른쪽 32비트 블럭을 자리바꿈(Swapping)해 가면서 처리하고, 오른쪽 32비트 블럭은 라운드 키와 f 함수라는 비선형 동작을 하는 연산을 통과하게 된다.

나. 해독

DES는 공포된 이래 많은 논란과 비판의 대상이 되어 왔다. 주요 논란의 대상이 된 두 가지는 56비트 키를 사용한 암호문은 컴퓨터 기술의 급속한 발전에 따라 키의 전수 탐색(Key Exhaustive Search)이나 Time-Memory Trade-Off 방법에 의해 공격될 수 있다는 점이고, 다른 하나는 DES의 중요한 비도를 결정하는 S-box에 대한 설계 기준이 공개되지 않아 어떤 비밀 방안(Trap Door)이 숨겨져 있지 않나 하는 점이였다.

그러나, 1990년대에 들어와서 DES를 해독하기 위한 구체적인 방법으로 차분 해독법(Differential Cryptanalysis)[6],[7]과 선형 해독법(Linear Cryptanalysis, LC)[8]이 발표되었다. 90년 이스라엘 암호 학자인 Biham과 Shamir가 발표한 DC는 DES를 키 전수 검색 복잡도인 2^{56} 보다 훨씬 적은 2^{47} 의 복잡도로 해독이 가능하다고 하였다. DC는 DES 뿐만 아니라 대부분의 블럭 암호 시스템을 공격할 수 있는 새로운 공격 방법으로 실용적 가치에 주목받고 있다.

92년 Matsui에 의해 제안한 LC는 DES에서 유일한 비선형 구조인 S-box를 적당히 선형화 시켜 분석하는 KPA로 CPA인 DC와 유사한 방법이다. 이 방법으로 DES를 해독하는 데는 2^{43}의 복잡도로 가능하여 DC 보다 더욱 효과적인 방법으로 선형 분석을 위해서는 확률이 최적인 선형근사가 필요하다. 좋은 선형근사 (선형근사의 확률이 0 또는 1에 가까운 값을 가지는 선형근사)를 구하면 선형 암호분석은 쉽지만, 반대로 좋은 선형근사를 구할 수 없으면 선형 분석은 어렵다. 이 방법을 이용하여 1994년 1월 12대의 워크스테이션을 사용하여 50일 만에 16라운드의 DES를 해독한 실증적인 결과가 발표되는 등 DES는 이제 암호 알고리즘으로서의 가치를 상실하고 있다. 이러한 DC나 LC는 키의 전수 탐색 방법보다 효율적이나 김 광조 등의 결과[9]에 의하면 DC 및 LC 방법이 키 전수 탐색 방법보다 더 효율적이지 못한 S-Box의 설계 조건을 제시하고 S-box의 구체적인 예를 제시하였고, DC 및 LC에 대한 DES의 안전성을 획기적으로 개선시키는 방법[10]도 제안되었다.

그러나, 이러한 해독법과 별도로 컴퓨터 기술의 발전으로 키 전수 검색 방식[11]이 가능하게 되어 56비트 키 크기를 갖는 DES는 3일만에 해독될 수 있는 기계를 발표하는 등 현재의 키 크기로는 안전성을 보장할 수 가 없어 미국은 DES를 3중 암호화하는 112비트 키 크기를 가지는 3DES를 표준으로 제정하고 있다.

DES의 구조와 유사한 암호로는 일본의 FEAL[12], 호주의 LOKI[13], 스위스의 IDEA(International Data Encryption Algorithm)[14], 러시아의 GOST(GOvernment STandard)[15], SAFER K-64[16] 등이 수 십종이 있으며 이들은 라운드 수가 다르거나 내부의 f 함수가 DES의 f 함수와 다른 구조를 가지고 있다.

3.3 AES

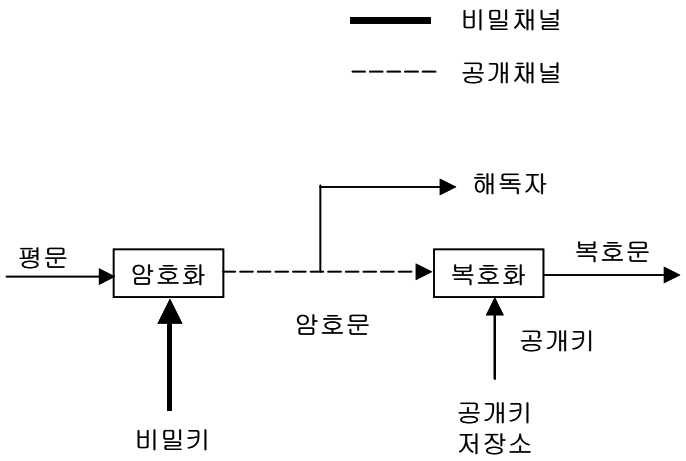
미국 표준국인 NIST는 3DES 방식은 영구적인 해결책이 되지 아니한다고 판단하고, 128비트 블록 크기를 가지고 키 전수 검색 공격에서부터 안전한 키 크기를 가지는 128비트, 192비트, 256비트의 키를 가지는 새로운 블럭 암호의 표준으로 AES(Advanced Encryption Standard) [17]를 전세계적으로 97년도 2월에 시작하여 97년 9월에 공모하기에 이르렀다. 이에 제안된 20여종 이상의 알고리즘이 세계적인 응모가 있었으며, 98년 8월에 선정 기준을 통과한 알고리즘으로 1차적으로 15개 알고리즘을 선정하여, 99년 3월에 이 중 최종 후보로 MARS, RC6, Rijndael, Serpent, Twofish인 5개의 후보 알고리즘을 선정하였다. 이 5개의 암호는 이미 알려진 여러 가지 해독방식에 의한 안전성 검토와 소프트웨어 또는 하드웨어, 스마트 카드 등 각종 구현 방식에 따른 효율성 검토가 이미 진행되었으며, NIST는 기타 여러 가지 요인을 고려하여 2000년 9월이면 AES로 최종 알고리즘을 결정 발표하게 되어 있다.

각 알고리즘은 각각 독특한 내부 구조를 가지고 있으며 RC6, Twofish는 Feistel 형태, Mars는 확장 Feistel 형태, Serpent는 SP network 형태, Square 형태가 Rijndael로 분류된다.

IV. 공개키 암호 시스템

4.1 개요

비밀키 암호 시스템에서는 암호 키와 복호 키가 동일하여, 키를 반드시 비밀로 유지하여야 암호 시스템의 안전성이 보장된다. 따라서, 송수신이 이루어지기 전에 송수신자간에 비밀키를 공유할 수 있도록 키 분배 (distribution) 방법을 약속하여야 하며. n명이 가입된 통신망에서 서로 비밀 통신을 할 경우 n(n-1)/2개의 키를 각자가 안전하게 관리하며, 이때 n이 커질수록 상당량의 정보가 된다. 이러한 키 관리 문제를 해결할 수 있는 암호 시스템이 바로 공개키 암호 시스템으로 공개키를 이름과 전화번호가 나열되어 있는 전화번호부처럼 공개하여 누구든지 통신 상대방의 공개키를 사용할 수 있도록 되어 있게 하는 것이다. 따라서 송신자와 수신자가 사전에 키의 분배를 할 필요가 없어 디렉토리 화일 등에 공개 키를 알려주고 자신의 비밀키만을 철저히 관리하면 된다.



(그림 3) 공개키 암호 시스템의 구성

대부분의 암호 시스템은 입력이 주어지면 출력을 쉽게 계산할 수 있는 일방향 함수로 구성되어 있으며 출력에서 키 정보를 모르고는 입력을 구하는 것은 불가능하게 되어 있다. 그러나, 공개키 암호 시스템을 구성하기 위하여는 일방향 함수의 역을 쉽게 구할 수 있는 방법을 강구하여야 하는 데, 어떤 정보를 알고 있는 사람은 역함수를 쉽게 구할 수 있는 일방향 Trapdoor 함수를 이용한다. 또한, 공개 키와 비밀 키 사이에는 수학적인 관계가 있고 공개 키 등의 공개 정보로부터 비밀 키를 찾아낼 수 없도록 하여야 해독자는 언제든지 공개키 정보를 가지고 있다는 점을 유의하여야 한다. .

공개키 암호는 2개 키의 역할이 달라 비대칭 (Asymmetric) 암호, 2키 (Two-key) 암호 라고도 부르며, 대표적인 공개키 암호 시스템인 DH 공개키 암호 시스템[18]와 RSA 공개키 암호 시스템[19]에 대하여 기술한다.

4.2 DH 공개키 암호 시스템

DH 공개키 암호 시스템을 이해하기 위한 수학적인 개념을 우선 소개한다. 소수 p를 법으로 하면 법에 관한 덧셈 등의 그 연산의 결과는 0,1,2,...p-1 사이의 p개의 정수들이 된다. 이 p개의 정수 중에는 원시근(primitive element)이라 불리는 정수 α가 있다. 이 원시근이란 그것의 멱승 $\alpha^0, \alpha^1, \alpha^2$,....들을 법 p에 관하여 간단히 하면 1,2,...p-1의 정수들로 되는 정수이다. 예를 들면 법이 7인 경우 3이 원시근이다.

$$3^0 \equiv 1,\ 3^1 \equiv 3,\ 3^2 \equiv 2,\ 3^3 \equiv 6,\ 3^4 \equiv 4,\ 3^5 \equiv 5 \pmod 7$$

이제 임의의 통신 상대방 A, B 사이의 비밀키 공유 과정을 살펴보자.

단계 1 : A와 B는 1,2,....p-1의 정수 중 임의로 각각 X_A와 X_B를 선택하고 이를 비밀로 한다.

단계 2 : A는 $\alpha^{XA} \pmod p$를 계산한 결과 Y_A를 B에게 (또는 공개키 저장소에)보내고, B도 역시 $\alpha^{XB} \pmod p$를 계산한 결과 Y_B 를 A에게 (또는 공개키 저장소에) 보낸다.

단계 3 : A는 받은 Y_B를 사용하여 B와 공유할 수 있는 비밀키 K1을 다음과 같이 만든다.

$$K1 = Y_B^{XA} \pmod p$$

B도 같은 방법으로

$$K2 = Y_A^{XB} \pmod p$$

를 만든다. 이때 Y_B^{XA}나 Y_A^{XB}는 모두 α^{XAXB} 이어서 서로 같은 키를 갖게 되어 이 키 K1 (또는 K2) 를 사용하여 암호문을 만들고 해독할 수 있다.

이 DH 공개키 암호 시스템의 안전성은 이산대수(Discrete Logarithm) 문제에 근거하고 있다. 이산대수 문제란 X를 알고 있을 때 $Y = \alpha^X$ 을 계산하여 Y를 알기는 쉬워도, Y를 알고 있을 때 $X = \log Y$ 를 계산하여 X를 계산하기는 아주 어렵다는 것이다.

위의 단계 2에서 Y_A 또는 Y_B 가 공개되어도 X_A 또는 X_B 를 구하는데 걸리는 계산 시간이 커지게 되어 이에 근거하는 암호 시스템은 안전하다는 논리가 되는 것이다. 소수 p의 길이가 1,000비트일 때 X_A 로부터 Y_A 를 계산하거나 Y_B 와 X_A 를 이용하여 K1을 계산하는데 1,000비트 길이의 수를 약 2,000번 곱하는 연산이 필요하지만, 역으로 log계산을 하기 위해서는 2^{100} (약 10^{30})번 이상의 연산이 필요하다. 이산대수 문제는 현재도 활발히 연구되고 있으며, 이산대수 문제의 해를 구하기 위해 소요되는 시간을 단축하려는 여러 알고리즘이 발표되고 있으며 DH 암호 시스템은 공개키 개념을 최초로 도입한 키 공유 방식이라는 점에서 가치가 있다.

4.3 RSA 공개키 암호 시스템

1978년 MIT의 Rivest, Shamir, Adleman에 의하여 제안된 RSA 공개키 암호 시스템은 합성수의 소인수 분해의 어려움에 그 안전성을 근거하고 있다. 이 RSA 공개키 암호 시스템에서는 Euler(1707-1783)의 정리가 쓰이는데 먼저 이를 살펴보자.

양의 정수의 집합 {1, 2, ..., n-1}의 원소들 중에서 n과 서로 소의 관계에 있는 원소들의 개수를 $\varphi(n)$으로 나타내고, 이를 Euler의 φ-함수라 한다. 특별히 소수인 p에 대하여 $\varphi(p) = p-1$이다. 큰 정수 n에 대하여 $\varphi(n)$값을 구하기 위하여는 n의 소인수 분해가 필수적이다. 즉, n이 두 소수 p와 q의 곱일 때 $\varphi(n) = (p-1)(q-1)$이다. 따라서, 소인수 분해 없이 $\varphi(n)$을 구하기는 매우 어렵다. Euler의 정리란 서로 소인 두 양의 정수 a와 n에 대하여

$$a^{\varphi(n)} \equiv 1 \pmod n$$

이 성립한다는 것이다.

이제 RSA 공개키 암호 시스템의 알고리즘과 간단한 보기를 살펴보자.

단계 1 : 두 개의 큰 소수 p와 q를 선정하여 자신의 비밀키로 한다.

단계 2 : $n = pq$인 n을 공개하고 $\varphi(n)$과 서로 소인 임의의 정수 e를 선택하여 공개키로 한다.

단계 3 : $e\,d \equiv 1 \pmod{\varphi(n)}$되는 d를 Euclid 호제법 등으로 계산하여 비밀키로 한다. 즉 p와 q, 그리고 d는 비밀키로, n과 e는 공개키로 한다.

암호화 단계 : 평문 M을 공개키 e를 사용하여 M^e한 다음 법 n으로 간단히 한다. 즉 암호문 C는 다음과 같다.

$$C \equiv M^e \pmod n$$

복호화 단계 : 암호문 C를 비밀키 d를 사용하여 C^d한 다음 법 n으로 간단히 한다. 다시 평문이 나오게 되는 관계식은 다음과 같다.

$$C^d \equiv (M^e)^d \equiv M^{t\varphi(n)+1} \equiv M^{\varphi(n)\,t} \quad M \equiv M \pmod n,$$

여기서, t는 ed ≡ 1 (mod φ(n))에서 유도되는 ed = tφ(n) + 1 을 만족하는 정수이다.

보다 안전한 RSA 공개키 암호 시스템을 위하여 p와 q를 선택하는 조건, e와 d에 대한 조건 등이 부가적으로 필요하다. RSA 공개키 암호 시스템은 공개키 n과 e를 가지고 비밀키 d를 구할 수만 있다면 무용지물이 된다. d를 찾기 위하여는 φ(n)을 계산할 수 있어야 하는데 이를 위해서는 n의 소인수 분해가 필요하다. p와 q가 100자리의 소수이고 따라서 n이 200자리의 합성수라면 현재의 알려진 소인수 분해 알고리즘과 컴퓨터로 n을 소인수 분해하는 것은 거의 불가능하다고 알려지고 있다고 있으나, 소인수 분해 기술의 향상에 대비하여 정보의 소요 비도 수준과 연산 능력을 고려하여 n을 512비트이상 2,048비트를 사용하여야 한다.

효과적인 소인수 분해 알고리즘은 Lenstra와 Pomerance 등에 의하여 현재까지도 연구되어 오고 있다. 지난 10년간 큰 소수의 소인수 분해는 괄목할 만한 성장을 하였는데 RSA가 제안된 당시에는 40자리 정도가 소인수 분해될 수 있었던 것에 비하여 최근에는 110자리 이상 소인수 분해되고 있는 실정이다. 이는 H/W 기술과 이론의 발전에 기인한다. Carson 등에 의해 1987년 제안되었고, 1989년 암호학회에서 Lenstra 등은 300 MIPS 기계를 1년간 가동하여야만 111자리를 인수분해 할 수 있다는 결과를 발표하였다. 1994년 컴퓨터가 쉬는 시간을 이용하여 1,600대의 컴퓨터를 네트워크로 연결하여 129자리의 정수를 인수분해한 결과도 발표되었으며, 특수한 컴퓨터를 만들어서 해결하려는 종래의 사고 방법과는 다른 개념이었다. 최근에는 155자리(512비트)의 정수도 인수분해가 되어 RSA 암호 알고리즘의 사용 시에 키의 크기를 장시간 안전성을 위하여는 1,024비트 이상을 사용하여야 한다.[20-24].

소인수 분해의 어려움에 근거하는 RSA 공개키 암호 시스템들과 비슷한 암호 시스템들이 많이 제안되었다. 1979년 Rabin의 암호 시스템[25], Lucas 수열을 이용한 Lucas 암호[26] 등이 있으나 RSA 암호 시스템에 비하여 그리 널리 사용되고 있지 않다.

이상과 같이 공개키 암호 시스템은 정보의 기밀성 유지뿐만 아니라 정보의 디지털 서명, 통신 정보의 인증, 수신 사실을 거부하는 통신 상대방으로 하여금 수신 사실을 거부할 수 없는 근거를 제공하는 부인 봉쇄 기능 등의 부가적인 기능을 제공한다. 이러한 새로운 정보보호 서비스의 응용에 대하여는 지면 관계 상 구체적인 내용은 생략하고 참고 문[27],[28]을 참조하시기 바랍니다.

3.4 최근의 공개키 암호 시스템

가장 널리 알려져 있는 RSA 공개키 암호 방식은 안전성을 위하여 키의 길이가 상당한 길이가 요구되어 연산력이 제한된 이동 통신 단말기에는 사용이 제한될 수 있다. 이에 95년 Koblitz[29]와 Miller[30]는 타원곡선을 이용한 공개키 암호 시스템을 구성할 수 있다고 제안하였다 .그 후 비트당 안전도가 타 공개키 시스템보다 효율적이라는 것이 알려졌고, 최근 높은 속도의 구현이 가능하게 되었다.

타원곡선 암호시스템은 유한체의 곱셈군에 근거한 시스템으로써 다음과 같은 장점을 가진다.

① 군(Group)을 제공할 수 있는 다양한 타원곡선을 활용할 수 있다. 즉, 다양한 암호시스템 설계가 용이하다.

② 초특이 타원곡선을 피하면 이 군에서의 준지수 시간 알고리즘(subexponential time algorithms)이 존재하지 않는다. 즉, 안전한 암호시스템을 설계하는 것이 용이하다.

③ 타원곡선 암호시스템은 기존의 공개키암호와 같은 안전도를 제공하는 데에 더 작은 키 길이를 가지고 가능하다(예, <표 2>와 같이 RSA 1024비트 키와 ECC 160비트 키를 갖는 암호시스템은 같은 안전도를 갖는다).

④ 타원곡선에서의 더하기 연산은 유한체에서의 연산을 포함하므로, H/W와 S/W로 구현하기가 용이하다. 더욱이 이 군에서의 이산대수 문제는 특히, 같은 크기의 유한체 K 에서의 이산대수 문제보다 훨씬 어렵다고 알려져 있다.

<표 2> RSA 공개키 암호 시스템과 타원곡선 암호 시스템의 안전성 비교

ECC 키 크기 (비트)	RSA 키 크기 (비트)	공격에 걸리는 시간 (MIPS Years)	키 크기 비율 (RSA 키/ECC 키)
106	512	10^{4}	4.65
132	768	10^{8}	5.65
160	1,024	10^{12}	6.4
211	2,048	10^{20}	9.48
320	5,120	10^{36}	16.0

* MIPS : Million Instructions Per Second

유한체위에서의 타원곡선은 DH 공개키 암호 방식, DSS(Digital Signature Standard)[31] 같은 서명 기법을 구현하는 데에 사용될 수 있고, 이러한 시스템들은 짧은 키 길이를 가지고도 다른 공개키 시스템과 동등한 안전도를 제공할 수 있다. 또한 짧은 키 길이를 갖는다는 것은 대역폭과 메모리가 작아짐을 의미하는데, 이로 인해 메모리와 처리능력이 제한된 스마트 카드, 이동 통신에서의 보안성 제공 같은 응용에서 중요한 기반 암호 기술이 될 수 있다. 타원곡선 암호의 또 다른 이점은 비록 모든 사용자가 같은 기저체 K를 사용한다 하더라도 각 사용자가 다른 곡선 E를 선택할 수 있다는 것이다. 즉, 모든 사용자는 체 연산을 수행하기 위해 같은 H/W를 사용할 수 있으며, 추가 보안을 위해 주기적으로 곡선 E를 바꿀 수 있다.

기타 공개키 암호로서 최근 Silverman등이 제안한 NTRU[32],[33],[34], 정보를 효과적으로 표현하여 Lenstra 등이 제안한 XTR 공개키 암호[35], KAIST 고 기형 교수 등이 제안한 따임 이론인 Blade group을 이용한 공개키 암호[36] 등이 있다, 이러한 새로운 공개키 암호는 안전성이 증명되지 아니하여 공개된 후 쉽게 해독되는 사례도 있으므로 향후 3년 정도 안전성 분석을 기다려 보아야 한다. 따라서 공개키 암호 방식을 이용할 때, 안전성을 엄밀히 증명한 구성 방법 연구가 필요하여 김광조 등이 제안한 방식[37]이 있다.

V. 각국의 최근 동향

미국의 AES 계획에 자극을 받아 일본과 유럽 연합은 각자 전자 정부를 구축 및 암호 산업의 육성을 위하여 독자적인 암호 기술을 확보하고자 각국의 사정에 따른 AES 계획과 유사한 별도의 계획을 수립하여 추진하고 있다.

5.1. 유럽

유럽은 정보 사회 기술 내에 NESSIE (New European Schemes for Signature, Integrity, and Encryption) 프로젝트[38]를 2000년 1월부터 추진을 시작하였고, 공개적인 모집과 평가를 통하여 강한 암호 방식을 만들려는 계획으로 블록 암호, 스트림 암호, 공개키 암호, 디지털 서명, 난수 발생기, 메시지 인증 부호, 해쉬 함수 등 암호를 위한 기본 함수들을 2000년 9월 29일 까지 공모하고 있다. 각 함수의 응모 기준은 공개 규격에 맞도록 발표하여 놓고 있으며 벨기에 암호 학자 Bart Preneel이 주도적으로 추진하고 있다.

이 계획은 3년간 선정 작업을 계획하고 있으며, 방식은 Gigabit 네트워크, 스마트 카드, 무선 통신용 으로 이용하려고 하고 있으며, 유럽의 암호 산업의 발전에 기여하고자 이스라엘, 덴마크, 프랑스, 독일, 스위스, 스웨덴, 영국, 벨기에, 노르웨이, 핀란드 기업이 참여하고 있으며, 최종 AES 후보와 협의하고 일차 선별 작업, 안전성 및 성능 평가, 3회 공개적인 워크샵을 통하여 표준 기구에 결과를 제공하려고 한다.

5.2. 일본

일본 정부는 도래하는 2003년 까지는 전자 정부를 구축하는 데 안전한 암호 기술이 필수불가결한 주요 요소임을 파악하고, 개인의 기밀성 확보와 전자 문서의 인증 제공 수단이 필요하다고 인식하였다. 이에 일본 정부는 국제적으로는 표준 기구인 ISO/IEC JTC1 활동에 노력을 기우리고 있다. 이런 것이 일본 통상성의 안전한 전자 정부의 실행 계획 중 하나로 2000년 4월에 개시하였다.

공모하는 알고리즘으로는 공개키 암호, 비밀키 암호, 해쉬함수, 난수 발생기 이며 2000년 7월 21일에 1차 공모가 완료되어 48종이 신청되었다. 이계획에는 기술 검토 결과를 제공하여 일전 수준 이상이 되는 암호 기술은 평가하여 합격되는 방식을 하고 있으며 이 계획을 위하여 일본의 정보처리 진흥 사업 협회인 IPA가 CRYPTREC (CRYPTography Research & Evaluation Commitee)[39]를 구성한 바가 있으며, 이위원회에는 동경대 Imai 교수가 위원장으로 활동하고 있으며 요꼬하마 국립대 Matsumoto 교수, 중앙대 Tsujii 교수, 동경이과대 Kaneko 교수 등이 참여하고 있으며 2000년 9월 중에는 1차 검토 결과를 제시하고, 11월까지 상세 평가 결과가 제시되고 2001년 2월에 추가작인 작업을 계획하고 있다.

VI. 결 론

정보보호 기술의 실제 도입 시에는 본고에서 살펴본 각종 보호 기술을 단독으로 사용되는 것보다는 복합적으로 시스템이 요구하는 보안 서비스에 맞도록 선별적으로 적용할 수 있다. 또한, 정보보호 기능의 구현에 따른 사용의 불편함이 생기는 문제는 사용의 편리성과 보호 기술간의 타협이 요구되며 망간의 호환성을 유지하기 위하여 표준화 작업도 병행하여 추진되어야 한다.

최근 이동 통신 기술의 발전, 방송과 통신의 통합 등 다양한 변화에 대비한 암호 기술이 더욱 요구되고 있다. 기밀성 보장을 위하여는 128비트 키 이상의 블록 암호가 필요하고 소인수 분해 기술의 발전에 따는 1,024비트 RSA 암호를 갈음할 수 있는 160비트 타원 곡선 암호는 구현의 어려움에 불

구하고 효율성이 기대되어 계산력이 제한된 이동통신 단말기에 사용이 예측이 된다. 그러나 새로운 공개키 암호의 설계 노력은 지속되어야 하며 안전성 분석 기술도 제공되어야 한다.

지적 소유권을 보호라는 Watermarking 기법 연구도 지속되리라고 보이며, 암호 기술은 설계와 해독 기술간의 상호보완적 발전이 지속될 것이 Quantum Computing 기술을 응용한 해독 기술도 가능하리라 보이며 암호 기반 기술의 발전을 위하여는 지속적인 연구 개발이 요구되며 2001년 2월에는 공개키 암호 기술의 이론 연구와 응용 기술 발전을 위하여 국제적인 학술대회 PKC2001[40]이 제주도에서 개최될 예정으로 되어 있다.

참 고 문 헌

[1] NIST, "Data Encryption Standard(DES)", Federal Information Processing Standard Publication 46, Apr. 1977.

[2] CERTCC-KR, "99 국내외 해킹 현황 분석", http://www.certcc.or.kr/statistics/hacker/99/99-hack.html

[3] 황규범, 김광조, 안철수, “CIH 바이러스 분석 및 대책”, KIISC 논문지, No 4, pp.49-60, 1999.12

[4] S. Katzenbeiser and F. A. Peticolas, "Information Hiding Techniques for Steganography and Digital Watermarking", pp. 95-145, Artech House, 2000.

[5] C.E.Shannon, "Communication Theory of Secrecy Systems", Bell Syst. Tech. J., Vol. 28, pp. 656-715 Oct. 1949.

[6] E. Biham and A. Shamir, "Differential Cryptanalysis of DES-like Cryptosystem", J. of Cryptology, vol. 4, pp. 3 - 72, 1991.

[7] E. Biham and A. Shamir, "Differential Cryptanalysis of the full 16-round DES", Advances in Cryptology-Crypto92, Springer-Verlag, pp.487-496, 1993.

[8] M. Matsui, "The First Experimental Cryptanalysis of the Data Encryption Standard", Advances in Cryptology-Crypto'94, Springer-Verlag, pp.1-11, 1994.

[9] K.Kim, S.Lee, S.Park and D.Lee, "Securing DES S-boxes against Three Robust Cryptanalysis", 1995 Workshop on Selected Areas in Cryptography, pp.145-157,Carleton Univ., Canada, May 15-16, 1995.

[10] E.Biham and A.Biryukov, "How to Strengthen DES Using Existing Hardware", Advances in Cryptology-Asiacrypt'94, Springer-Verlag, pp.398-412, 1995.

[11] http://www.eff.org/DEScracker.

[12] A.Shimizu and S. Miyaguchi "Fast Data Encipherment Algorithm FEAL", Advances in Cryptology-Eurocrypt'87, Springer-Verlag, pp.267-278, 1988.

[13] L. Brown, K. Kwan, K. Pieprzyk and J. Seberry, "Improving Resistance to Differential Cryptanalysis and Redesign of LOKI", Advances in Cryptology-Asiacrypt'91, Springer-Verlag, pp.36-50, 1992.

[14] X. Lai, "On the Design and Security of Block Ciphers", ETH Series in Information Processing, Ph. D Dissertation, Vol 1, 1992.

[15] "Cryptographic Protection for Data Processing Systems", GOST (Government Standard) of the USSR 28147-89, 1989.

[16] J.L.Massey, "SAFER K-64 : A Byte Oriented Block-Ciphering Algorithm", Cambridge Security Workshop, Cambridge, U.K., Dec. 9-11, 1993.

[17] http://www.nist.gov/aes/

[18] W. Diffie and M. E. Hellman, "New Directions in Cryptography", IEEE Trans. Inform. Th., Vol. 22, pp. 644-654, Nov. 1976.

[19] R.L. Rivest, A. Shamir and L. Adleman, "A Method for obtaining Digital Signatures and Public Key Cryptosystems", Vol. 21, No. 2, pp. 120-126 Feb. 1978,

[20] C. Pomerance, J.W. Smith and R. Tuler, "A Pipe-line Architecture for Factoring Large Integers with the Quadratic Sieve Algorithm", SIAM J. Comp. Vol. 17, pp. 387-403, 1988.

[21] D. Atkins, M.Graffs, A.K.Lenstra, and P.C.Leyland, "The Magic Word are Squeamish Ossifrage", Advances in Cryptology-Asiacrypt'94, Springer-Verlag, pp.263-277, 1995..

[22] J. Cowie et al, "A world wide number field sieve factoring record : on to 512 bits", Advances in Cryptology-Proc. of Asiacrypt96, LNCS 1163, pp. 382-394, Springer Verlag, 1996

[23] A.J. Lenstra, E.R.Verhaul, "Selecting cryptographic key sizes", Proc. of PKC2000, LNCS Vol. 1751, pp446-465, Springer Verlag, Feb., 2000

[24] S. Cavallar, B, Dodson et al, "Factorization of a 512-bit RSA modulus", Advances in Cryptology-Proc. of Eurocrypt2000, LNCS, Vol.1807, pp.1 -18, May 2000.

[25] M. O. Rabin, "Digitalized Signatures and Public - Key Functions as Intractable as Factorization," MIT Laboratory for Computer Science, MIT/LCS/TR-212, Jan. 1979.

[26] Peter Smith, "LUC Public Key Encryption", Dr. Dobb's Journal, pp. 37-42, Jan. 1993.

[27] Bruce Schneier, *Applied Cryptography*, 2nd Edition, Addison-Wesley, 1996.

[28] W. Stallings, *Network and Internetwork Security*, Prentice Hall, 1995.

[29] N. Koblitz, "Elliptic curve cryptosystems", Mathematics of Computation, Vo.48, pp.203-209, 1987

[30] V. Miller, "Uses of elliptic curves in cryptography", Advances in Cryptology-Proc. of Crypto85. LNCS, Vol.218, pp.417-426, Springer Verlag, 1985.

[31] NIST Pub, 186, "Digital Signature Standard", U.S. Department of Commerce, May, 1994.

[32] Jeffery Hoffstein, Jill Pipher, Joseph H. Silverman, "NTRU : A ring based public key cryptosystem", ANTS'3, Vol.1423, LNCS, pp.267-288, Springer Verlag, 1998

[33] Jeffery Hoffstein, Joseph H. Silverman, "Reaction attacks against the NTRU public key cryptosystem", Technical Report 15, NTRU Cryptosystems, Aug, 1999

[34] Eliane Jaulmes, Antoine Joux, "A Chosen-ciphertext attack against NTRU", Advances in Cryptology-Proc. of Crypto2000,, pp.21-35, Vol. 1880, Springer Verlag, Aug. 2000.

[35] Arjen L. Lenstra, Eric R. Verhaul, " The XTR public key system", Advances in Cryptology-Proc. of Crypto2000,, pp.1-20, Vol. 1880, Springer Verlag, Aug. 2000.

[36] Ki Hyoung Ko et al. " New public key cryptosystem using braid groups", Advances in Cryptology-Proc. of Crypto2000,, pp.166-183, Vol. 1880, Springer Verlag, Aug. 2000.

[37] Joonsang Baek, Byoungcheon Lee, Kwangjo Kim,"Secure length-saving ElGamal Encryption under the Computational Diffie-Hellman Assumption", Proc. of ACISP2000, LNCS, Vol.1841, pp.49-58, Springer-Verlag, July, 2000

[38] http://www.cryptonessie.org

[39] http://www.ipa.go.jp/security/enc/CRYPTREC/index-e.html

[40] http://caislab.icu.ac.kr/pkc01