□ 기술해설 □

정보보호 기술의 최근 동향과 발전 전망

한국전자통신연구소 김광조*

● 목 차 ●

1. 서 론
2. 용어의 정의
3. 비밀키 암호 시스템
 3.1 DES
 3.2 DES의 해독
 3.3 기타 비밀키 암호 시스템
4. 공개키 암호 시스템
 4.1 DH 공개키 암호 시스템
 4.2 RSA 공개키 암호 시스템
 4.3 기타 공개키 암호 시스템
5. 국제 학술 활동
6. 미국과 일본의 정책 동향
 6.1 미국의 정책
 6.2 일본의 정책
7. 발전 전망

1. 서 론

인간이 사회 생활을 시작하면서 상대방과 대화를 통하여 의사 소통을 하기 시작한 이래, 통신 수단을 이용하여 자신의 의사를 원거리에 전달하고자 하였고 정보를 전달하는 통신로 상에는 정보의 탈취, 변조 등의 위협으로부터 전달 정보를 보호하고자 로마 시대 시저는 영문 알파벳을 단순 천이하여(암호화) 원래의 정보(평문)를 변환한 정보(암호문)를 전달하였다고 하며 합법적인 수신 상대방은 역 천이 변환(복호화)하여 복원하는 방법을 사용하였다고 한다. 이때 평문을 암호문으로 천이한 수를 키라고 할 수 있다. 이후 1, 2차 세계 대전 중에는 군용 정보라든가 외교 정보를 보호하기 위하여 암호학이 발전되어 왔다. 전 세계의 어느 곳곳에서나 거의 동시에 통신이 가능한 정보화 사회에 접어든 현재는 통신로를 통한 불법적인 해킹 행위나 정보의 불법 감청, 개인의 프라이버시의 노출 등 통신 상대방도 모르는 사이에 개인의 비밀이 노출될 가능성이 있으며 컴퓨터에 접근하기 위하여 사용하는 패스워드는 화면상에는 보이지 않으나 통신로상에는 입력한 패스워드 정보가 그대로 전달됨으로 불법 감청에 의하여 자신의 패스워드가 노출될 가능성이 크다.

한편, 컴퓨터에 저장 중이거나, 통신망을 통하여 전송 중인 정보의 보호를 위해 많은 방법들이 이용된다. 정보에 물리적인 접근을 통제하는 것으로부터, 패스워드의 다단계 이용, 컴퓨터 운영체제의 강화 등 많은 수단이 있을 수 있다. 그러나 무엇보다도 on-line 통신망의 정보에 대한 직접적인 보호가 가장 효과적인 방책이 된다.

이 직접적인 보호 방법은 평이한 정보(Plain Data)를 암호화된 정보(Cryptographic Data)로 만드는 정보보호 이론, 즉 암호학에서 연구되고 있다. 이 암호학은 암호 알고리즘을 연구하는 암호학(Cryptography)과 암호 알고리즘의 안전성을 평가하는 암호 분석학(Cryptanalysis)으로 대별할 수 있다[1]. 이들 분야의 이론적인 배경은 정수론 (Number Theory), 추상 대수론(Abstract Algebra), 통계 및 확률론 등 수학의 많은 분야에 기초하고 있다. 이들 이론을 응용하여 정보 자체의 암호화에 의한

*비 회 원

보호와 나아가 정보 사회의 필수 요소인 문서 인증(Message Authentication), 위조할 수 없는 디지탈 서명(Digital Signature), DB(Database)의 보호 등에 활용되고 있다. 특히, 디지탈 서명은 EDI(Electronic Data Interchange) 또는 CALS(Continuous Acquision and Lifecycle Support 또는 Commerce At Light Speed) 구축에 필수적인 요소가 되며, 이밖에도 앞으로 광범위하게 이용될 스마트 카드 등에 정보보호 이론은 핵심 기술로 활용되고 있다.

본 고에서는 우선, 독자의 이해도를 증대하고자 정보보호 이론에서 널리 사용되는 용어를 정의하고 대표적인 비밀 키 암호 시스템과 공개 키 암호 시스템의 동작 원리 및 해독 결과를 간단히 기술하고, 정보보호 기술의 가장 최근의 결과를 발표하는 국제적인 학술 활동에 대하여 조사하고, 미국과 일본의 정보보호 관련 최근 정책에 대하여 서술하고 끝으로 정보보호 기술의 발전 전망을 예측하여 본다.

2. 용어의 정의

우선 본고에서 사용하는 용어를 정의한다.

(1) 정보보호(Information 또는 Data Security) : 시스템 내의 각종 형태의 정보를 불법적인 제 3자의 침탈로부터 보호하는 것으로 합법적인 상대에게만 정보의 소유를 허락하는 기밀성(Privacy)과 정보의 불법적인 변경을 방지함으로써 보낸 이의 합법성을 보장해 주는 인증(Authenticity, Integrity)에 정보보호의 목적을 두고 있다.

(2) 암호화(Encipherment, Encryption) : 평문(Plaintext)을 수학적 일정 규칙(암호알고리즘)에 키를 동작시켜 암호문(Ciphertext)을 얻는 과정을 말한다. 이의 역과정을 복호화(Decipherment, Decryption)라고 한다. 따라서 위에서 언급된 암호학은 좁은 의미에서는 이 암호화 과정을 연구하는 것이고, 넓은 의미로는 암호 알고리즘의 안정성을 분석하는 암호분석학(Cryptanalysis)을 포함하는 것을 말한다.

(3) 암호 시스템(Cryptosystem) : 적절한 암호화 기법을 채용하는 암호화, 복호화 과정으로 구성된 시스템으로, 암호화 및 복호화를 위한 키에 관한 부분과 이 키를 사용하여 일정 단계의 법칙 등에 의해 암·복호화 과정을 수행하는 알고리즘에 관한 부분으로 이루어져 있다.

(4) 암호문 단독 공격(Ciphertext Only Attack, COA) : 암호 해독자는 오직 암호문을 이용하여 암호 시스템의 키나 평문을 구하는 공격 방법으로 평문이 일정한 패턴을 갖지 않는다면, 암호 키나 평문을 구하는 것은 어렵다.

(5) 기지 평문 공격(Known Plaintext Attack, KPA) : 평문이 일정한 패턴을 갖는 문장일 경우, 암호 해독자는 전체 암호문중에서 일부 암호문에 대응하는 평문을 알고 있다는 가정 하에 이들을 이용하여 키를 구하여 다른 평문을 구하는 공격 형태이다.

(6) 선택 평문 공격(Chosen Plaintext Attack, CPA) : 암호 해독자가 임의로 선택한 평문을 임의의 키를 갖는 알고리즘에 입력시켜서 이에 대응하는 암호문을 구한 다음, 도청된 암호문과 비교하여 키를 구하는 공격 방법이다.

(7) 수동 공격(Passive Attack) : 해독자가 통신망의 정보를 단순한 도청에 의해 해독하려고 하는 행위를 말하며, COA는 여기에 해당된다.

(8) 능동 공격(Active Attack) : 해독자가 통신망에 직접 관여하여 정보를 변조하거나 위장 삽입하는 행위를 말하며, KPA, CPA가 여기에 해당된다.

(9) 확산(Diffusion)과 혼동(Confusion) : 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.

(10) 대칭형 암호 시스템(Symmetric Cryptosystem) : 암호화 키와 복호화 키가 동일한 암호 시스템이다. 이 키는 쌍방이 공유하는 비밀키이므로 전체 암호 시스템의 안전성을 결정하

는 절대 요소이다. 따라서 안전한 키의 분배 및 키의 초기값 결정이나 갱신을 위한 키의 관리가 요구된다. 이것을 재래식(Conventional) 암호 시스템, 또는 키가 동일하므로 단일키(one-key) 또는 비밀키(Secret Key) 암호 시스템이라고 한다.

(11) 비대칭형 암호 시스템(Asymmetric Cryptosystem) : 암호화에 사용되는 키와 복호화에 사용되는 키가 서로 다르며, 암호화(복호화) 키는 공개하고, 복호화(암호화) 키는 자신이 비밀로 간직하는 것이므로 키의 분배 절차가 요구되지 않는다. 이것을 서로 다른 두개의 키가 사용되어 two-key 암호 시스템, 또는 두 키 중 하나는 공개되므로 공개키(Public Key) 암호 시스템이라고도 한다.

3. 비밀키 암호 시스템

3.1 DES(Data Encryption Standard)

1949년 Shannon[2]은 확산과 혼동을 교대로 사용하는 변환(mixing transformation)을 이용한 암호 시스템의 구성을 제시하였으며, 이 Shannon의 구성 방법을 충실히 따른 것이 바로 DES이다[3]. 혼돈과 확산 함수 자체는 암호학적으로 약한 함수이나 여러 회 반복 사용하면 암호학적으로 강한 함수를 구성 할 수 있다는 점을 이용하였다. 또한, 복호화를 위하여 동일 함수를 2회 동작시키면 원래의 정보를 복원하는 Involution 함수를 사용하였다.

DES의 동작을 간단히 살펴보면, 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 바이트당 한 비트는 패리티 비트로 사용된다. DES는 16라운드(round)의 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 32 비트 블럭을 자리바꿈(Swapping)해

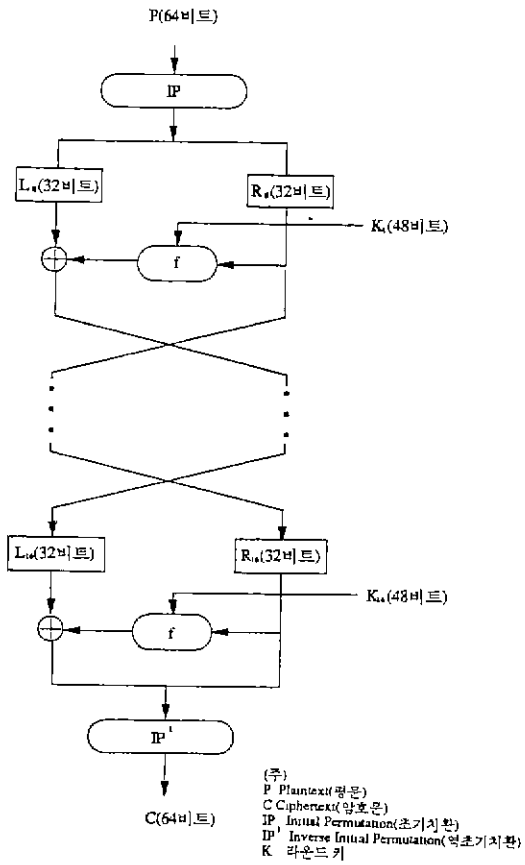

그림 1 DES의 개요

가면서 처리하고, 오른쪽 32비트 블럭은 라운드 키와 f 함수라는 비선형 동작을 하는 연산을 통과하게 된다(그림 1 참조).

3.2 DES의 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 점이다.

1990년대에 들어와서 DES를 해독하기 위한 구체적인 방법으로 입출력 변화 해독법(Differ-

ential Cryptanalysis, DC)[4, 5]과 선형 해독법(Linear Cryptanalysis, LC)[6]에 대하여 언급한다. 1990년 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. DC를 발표한 이래 DES와 비슷한 비밀키 암호 시스템 중 일본에서 제안한 FEAL(Fast data Encipherment ALgorithm)[7] 암호의 31단까지 CPA에 의해 해독에 성공하였다.

1993년 Matsui는 LC로 DES를 분석했다. 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 [8]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[9]도 제안되었다.

또한, Wiener[10]는 숨겨진 외부 키를 시행착오 식으로 검색한 기계(Key Exhaustive Search Machine)를 1백만 불을 투입하면 제작이 가능하여 DES의 안전성을 경고하였다. 위와 같이 DES의 안전성에 치명적인 해독 방법에 대하여 DES의 안전성을 증가시키는 방법으로 3중 DES를 이용하는 방법 또는 DC와 LC에 안전한 S-box로 현행 DES의 S-box를 대치하여 사용하고 외부 키를 증가시키는 방법 등이 제안되었다.

3.3 기타 비밀키 암호 시스템

DES와 유사한 암호로는 일본의 FEAL, 호주의 LOKI[11], 스위스의 IDEA(International Data Encryption Algorithm)[12], 러시아의 GOST(GOvernment STandard) [13], SAFER K-64[14] 등이 있으며 이들은 라운드 수가 다르거나 내부의 f 함수가 DES의 f 함수와 다른 구조를 가지고 있다. 이러한 비밀키 암호 시스템의 안전성에 대하여는 지속적인 연구가 진행되고 있다.

4. 공개키 암호 시스템

비밀키 암호 시스템에서는 암호화 키와 복호화 키가 동일하여, 키를 반드시 비밀로 유지하여야 암호 시스템의 안전성이 보장된다. 따라서, 송수신이 이루어지기 전에 송수신자간에 비밀키를 공유할 수 있도록 키 분배 (distribution) 방법을 약속하여야 한다. n명이 가입된 통신망에서 서로 비밀 통신을 할 경우 $n(n-1)/2$개의 키를 각자가 안전하게 관리하여야 하며, 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 공개키를 알려주고 자신의 비밀키만을 철저히 관리하면 된다.

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 공개키 등의 공개 정보로부터 비밀 키를 찾아낼 수 없도록 하여야 한다. 본 절에서는 대표적인 공개키 암호 시스템인 DH(Diffie-Hellman) 공개키 암호 시스템[14]과 RSA 공개키 암호 시스템[16]에 대하여 기술한다.

4.1 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 α^0, α^1, α^2,....들을 법 p에 관하여 간단히 하면 1,2,...p−1의 정수들로 되는 정수이다. 예를 들면 법이 7인 경우 3이 원시근이다.

$$3^0\equiv1,\ 3^1\equiv3,\ 3^2\equiv2,\ 3^3\equiv6,$$
$$3^4\equiv4,\ 3^5\equiv5\ (\mathrm{mod}\ 7)$$

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 α^{X_A}(mod p)를 계산한 결과 Y_A를 B에게 (또는 공개키들의 저장소에)보내고, B도 역시 α^{X_B} (mod p)를 계산한 결과 Y_B를 A에게 (또는 공개키들의 저장소에) 보낸다.

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

$$K1=Y_B^{X_A}\ (\mathrm{mod}\ p)$$

B도 같은 방법으로

$$K2=Y_A^{X_B}\ (\mathrm{mod}\ p)$$

를 만든다. 이때 $Y_B^{X_A}$나 $Y_A^{X_B}$는 모두 $\alpha^{X_AX_B}$ 이어서 서로 같은 키를 갖게되어 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 Y를 계산하여 X를 계산하기는 아주 어렵다는 것이다.

위의 단계 2에서 Y_A 또는 Y_B가 공개되어도 X_A 또는 X_B를 구하는데 걸리는 계산 시간이 커지게 되어 이에 근거하는 암호 시스템은 안전하다는 논리가 되는 것이다. 소수 p의 길이가 1,000비트일 때 X_A 로부터 Y_A를 계산하거나 Y_B와 X_A를 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.

4.2 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 φ(n)으로 나타내고, 이를 Euler의 φ−함수라 한다. 특별히 소수인 p에 대하여 φ(p) = p−1이다. 큰 정수 n에 대하여 φ(n)값을 구하기 위하여는 n의 소인수 분해가 필수적이다. 즉 n이 두 소수 p와 q의 곱일 때 φ(n) =(p−1)(q−1)이다. 따라서, 소인수 분해 없이 φ(n)을 구하기는 매우 어렵다. Euler의 정리란 서로 소인 두 양의 정수 a와 n에 대하여

$$a^{\varphi(n)}\equiv1(\mathrm{mod}\ n)$$

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=pq인 n을 공개하고 $\varphi(n)$과 서로 소인 임의의 정수 e를 선택하여 공개키로 한다.

단계 3 : e d≡1 (mod $\varphi(n)$)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.

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

여기서, t는 ed≡1(mod $\varphi(n)$)에서 유도되는 $ed=t\varphi(n)+1$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 $\varphi(n)$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 386비트에서 1024비트까지 사용되고 있다.

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. 150자리의 특별한 정수는 인수분해가 되기도 하는 등 많은 수학자들이 큰 정수의 인수분해에 관한 연구를 하고 있다 [21-25].

4.3 기타 공개키 암호 시스템

소인수 분해의 어려움에 근거하는 RSA 공개키 암호 시스템들과 비슷한 암호 시스템들이 많이 제안되었다. 1979년 Rabin의 암호 시스템[18], 1980년 William의 암호 시스템[19], Lucas 수열을 이용한 Lucas 암호[20], 타원곡선을 이용한 공개키 암호[26] 등이 있으나, RSA 암호 시스템에 비하여 그리 널리 사용되고 있지 않다.

이상과 같이 공개키 암호 시스템은 정보의 기밀성 유지뿐만 아니라 정보의 디지탈 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 문헌 [26-28]을 참조하시기 바랍니다.

5. 국제 학술 활동

1980년 초반부터 공개적인 암호학 연구를 위하여 국제암호학학회(IACR, International Association for Cryptologic Research)가 설립되어 1981년 이후 매년 8월경 미국의 UCSB (Univ. of California, Santa Barbara)에서 CRYPTO라는 국제회의가 개최되고 있으며 1982년에는 유럽의 각국을 순회하면서 매년 5월경 EUROCRYPT라는 국제회의가 개최되고 있으며, IEEE가 주최하는 시큐리티와 프라이버시에 관한 심포지엄이 1980년 이후 매년 5월경에 개최되고 있다. 1990년 이후에는 일본과 호주에서 각각 ASIACRYPT '91과

표 1 1990년 이후 정보보호 관련 국제 회의 개최 현황

연도	CRYPTO		EUROCRYPT		ASIACRYPT		AUSCRYPT	
	개최국	일 정	개최국	일 정	개최국	일 정	개최국	일 정
1990	미 국	8.11~15	덴마크	5.21~24			호 주	1.8~11
1991	미 국	8.11~15	영 국	4.8~11	일 본	11.11~14		
1992	미 국	8.16~20	헝가리	5.24~28			호 주	12.13~16
1993	미 국	8.22~26	노르웨이	5.23~27				
1994	미 국	8.21~25	이태리	5.9~12	호 주	11.28~12.1		
1995	미 국	8.27~31	프랑스	5.21~25				
1996	미 국	8.18~22	스페인	5.12~16	한 국	11.3~7		

AUSCRYPT '90, AUSCRYPT '92, ASIACRYPT '94를 개최하였으며 금년에는 11월 3일부터 7일까지 한국통신정보보호학회가 주관하여 경주 힐튼 호텔에서 정보통신부의 후원과 IACR의 협조 하에 ASIACRYPT '96을 개최하기로 되어 있다.

표 1에는 1990년 이후 정보보호 관련 국제 회의 개최 현황을 요약하였다.

한편, IACR이 개최하는 암호학회는 다소 이론에 치중한 결과가 발표되는 데 반하여 실제적인 정보보호의 응용에 주안점을 두어 1990년대에는 ACM(Association for Computing Machinery)이 주축이 되어 컴퓨터와 통신에 관한 시큐리티라는 국제 회의가 개최되고 있다. 한일간의 정보보호와 암호에 관한 공동 워크샵(JW-ISC, Joint Workshop on Information Security and Crytology)이 1993년 10월에 서울에서 최초로 개최되었으며 1995년 2월에는 일본의 이누야마에서 개최되었고 1997년에는 한국에서 개최 예정으로 되어 있는 바, 한일간의 정보보호에 관한 학술 교류 활동도 증대 일로에 있다. 다소 국부적이기는 하지만 캐나다를 중심으로 SAC(Workshop on Selected Areas in Cryptography) 등도 있다.

6. 미국과 일본의 정책 동향

6.1 미국의 정책

미국은 첨단 기술로 분류된 정보보호 기술과 관련 장치는 대공산국 수출 규제 품목으로 지정하고 있어 수출 규제가 가장 엄격하다. 전술한 바와 같이 1990년대에 DES가 암호 알고리즘으로서의 안전성이 위협받음에 따라 이에 대비하여 새로운 시책을 발표하였다. 즉, 1993년 미국의 클린턴 행정부는 Clipper Project라고 하는 새로운 개념의 정보보호 시책을 발표하였다. 이 Project의 핵심은 범죄 단체나 불법 마약 거래자가 암호를 이용한 불법 정보에 대하여 정부의 감청권을 고려한 암호 알고리즘의 표준을 추진하는 것이다(이미 미국의 연방수사국은 1970년대에 법원의 영장을 받아 범죄 가능성이 있는 통신 내용을 합법적으로 감청할 수 있도록 법적 근거 규정이 있다). 이 표준을 EES(Escrowed Encryption Standard)[29]라고 하며 80 비트 키와 입출력이 64비트인 블록 알고리즘으로 Skipjack이라는 내부 구조가 비공개인 알고리즘이 이용되고 있고 현재 ISO/IEC JTC1/SC27의 국제 표준 알고리즘 등록 절차(ISO/IEC9979)에 의해 이름만이 등록되어 있다. Skipjack을 반도체 칩화한 것을 Clipper Chip[30]이라고 부르며 부가적으로 미국의 디지털 서명 표준인 DSS(Digital Signature Standard)[31]를 포함한 반도체 칩을 Capstone Chip[32]이라고 부른다.

Clipper Chip의 제조 과정과 경찰의 합법적인 감청 과정의 개요는 다음과 같다. Clipper Chip의 제조 회사는 칩별로 고유 번호를 관리하고 고유 번호에 대응되는 암호키를 chip에 주입하도록 되어 있다. 주입된 암호키의 부분 정보는 국가적으로 공신력이 높은 2개의 기관에 분산 보관하도록 되어 있다. 경찰이 불법 통신 내용에 대한 감청권을 법원으로부터 허가를 받으면 Clipper Chip이 초기 동작 시에 반드시 전송하는 칩의 고유 번호를 경찰이 인식하고, 2개의 기관에 인식한 칩의 고유 번호를 전달하여 각각 분산 관리하고 있는 키 정보를 접수하여, 부분 키 정보를 조합하여 암호 통신에 사용된 키 정보를 추출하는 메커니즘으로 되어 있다.

또한, 1995년 10월 미국은 NSA의 요청에 의해 주요 정보의 종합적인 보호를 효율적으로 구현하고 PCMCIA 형태인 Fortezza 카드를 발표하였다. Fortezza 카드는 정보의 기밀성, 무결성, 부인 봉쇄성, 인증 기능을 효과적으로 수행하기 위하여 Skipjack, DSA(Digital Sig-

nature Algorithm), SHA(Secure Hash Algorithm), KEA(Key Exchange Algorithm)을 내장하고 있으며 파일 보호, 접근 제어 등을 가능하게 하였고, Telnet, Ftp를 비롯한 WWW 서비스에도 활용하도록 하였다.

6.2 일본의 정책[33]

통상성과 우정성이 각각 다른 시책을 검토하고 있는 일본의 정책을 소개한다.

우선, 통상성은 1994년 말부터 정보 시스템에 있어서 시큐리티와 프라이버시에 문제를 다루는 "시큐리티 프라이버시 문제 검토 위원회"를 설치하였고 1995년 3월의 중간 보고 내용을 살펴보면, 동위원회 산하에 해커,바이러스 대책 위원회,암호,인증 문제 검토 위원회, 프라이버시 문제 검토 위원회, 안전 대책 기준 위원회, 시큐리티 평가 기준 위원회가 설치되어 있다.

특히 암호, 인증 문제 검토 위원회에는

(1) 암호, 인증 기술의 발전과 이용 보급의 촉진을 위한 환경 정비

① 암호, 인증 기술에 관한 정보 제공, 조사 연구

② 키 등록 시스템

③ 암호의 표준화

④ 법, 제도 등 환경 검토

(2) 국제적인 협력

등을 검토 과제로 결정하였다.

①에 관하여는 IPA(정보처리진흥사업협회)가 암호 알고리즘에 관한 정보 제공 사업의 실시를 위하여 체제를 정비하고 1995년부터 IPA에 사무국을 설치하여 민간 기업, 대학, 연구기관 등이 수행하는 암호 알고리즘, 응용 등의 연구 개발을 일반에서부터 공모하여 지원하는 시책을 개시한다. ②에 관하여는 기술적인 문제 해결과 대규모 네트워크 환경 하에 실험의 실시 등을 검토한다. 1995년 3월에는 네트워크 제공자, 메이커 등이 주축이 되어 설립된 인증 실용화 실험 협의회의 활동을 지원 및 협력 가능성을 검토한다. ④에 관하여는 전자상거래환경정비위원회를 설치하여 1995년 중 시책을 정비한다고 한다.

(2)에 관하여는 전세계적인 네트워크 환경을 활용하여야 하는 관점으로부터 암호, 인증 기술의 국제적인 협력이 중요하지만 암호 통신의 규제와 암호 장치의 수출 규제가 심한 미국과 제약이 없는 유럽이나 일본과의 합의점을 찾기가 쉽지 않기 때문에 일본 내 관련 법규를 정비하고 있다고 한다.

또한, 암호, 인증 기술의 확산에 따른 관련 지적 재산권간의 관계를 명확히 하는 것이 중요하다고 지적되어 있다.

한편, 우정성에서는 시큐리티 기능을 보유한 정보통신 기반 구축을 위하여 멀티미디어 사회에 있어서 시큐리티 기술에 관한 검토 연구회를 1995년 2월에 설치하여 산하에 암호 인증 기술전문회를 두어 구체적인 검토가 이루어지고 있다. 또한, 1995년부터 우정성의 설립 법인인 통신, 방송 법인은 우정성으로부터 출자를 받아 암호화 기술, 인증 기술, 접근 제어 기술, 사용자 정합 기술 등을 포함한 정보통신 시큐리티 기술의 체계적인 개발을 추진 중에 있다.

7. 발전 전망

정보보호 기술은 크게 나누어 통신 정보의 보호(Communication Security, COMSEC)와 컴퓨터 정보의 보호(Computer Security, COMPSEC)와 망 보호(Network Security, NETSEC)로 나눌 수 있다. 통신 정보라 함은 음성 정보를 포함하여, 각종 데이타 통신방식 등에서 소통되는 모든 정보를 말하며 이를 효과적으로 보호하고 통신로 상의 불법적인 정보 누출을 방지하는 것이 통신 정보보호의 목적이다. 이러한 통신 정보의 위협은 대부분의 경우 단순한 도청이나 시도로 개인이나 기업의 기밀을 악용하는 방법으로, 대부분의 경우 수동 공격 방법이 사용된다. 우리 나라에는 현재 통신비밀 보호법에 의해 불법적인 도청은 금지되어 있다.

통신 정보보다 복잡한 형태인 컴퓨터 정보는 은행, 기업, 관공서 등에 컴퓨터 보급의 확대로 각종 주요한 정보가 자동 생산, 가공, 처리, 관리됨에 따라 컴퓨터 내부 정보의 변조나 악용의 우려가 높다. 더불어서 통신망의 확장으로

지금은 컴퓨터 통신을 통하여 세계 어느 곳과도 통신이 가능하다. 가장 널리 알려진 Internet를 통하여, 해커의 불법적인 침입으로 컴퓨터 내에 저장된 귀중한 정보가 파괴되거나 조작된 사례는 무수히 많다. 우리 나라에서도 1993년도에 해커가 청와대의 컴퓨터에 불법으로 위장 침입하여 허위 문서를 하달하여 사회 문제가 된 바도 있다. 따라서, 컴퓨터 정보보호 기술은 파일 보호 기술, 접근 제어 기술, 신분 확인 기술, 패스워드 관리 기술 등이 요구되며, 이러한 보호 기술들은 학문적으로나 기술적으로 많은 연구가 이루어져 있다. 컴퓨터 정보의 위협은 능동 공격의 경우가 많아 재래식 암호 시스템만으로는 해결이 불가능하며 공개키 암호 시스템과 암호 프로토콜 기법 등을 활용하여야 안전한 정보보호가 가능하다.

또한, 무역 정보 거래에서 효율적인 처리 방식으로 대두하고 있는 EDI시스템에서의 보호 기술, 컴퓨터 통신망을 통하여 메시지를 자동 전달하는 MHS(Message Handling System)의 보호 기술, Internet등을 통하여 전달되는 전자 우편 시스템의 보호 기술, 향후 전산망을 통하여 서비스가 예상되는 전자 선거 시스템의 보호 기술 등 다양한 컴퓨터 정보의 보호 기술이 요구된다. 은행 업무의 전산화에 따라 은행간 전자 자금 송금(Electronic Funds Transfer, EFT)시스템이나 슈퍼마켓의 거래 시점 자동 결재 (Point Of Sail, POS) 단말의 보호 기술 등이 절실히 요구된다. 그 이외에 정보보호 기술은 정보가 발생되는 시간적, 공간적인 어떠한 곳에서 정보보호가 요구되는 정보 유통에 있어 필수 불가결한 기술로 대두되고 있으며 컴퓨터 범죄나 컴퓨터 바이러스 대책으로도 정보보호 기술이 활용된다.

정보보호 기술의 실제 도입 시에는 본고에서 살펴본 각종 보호 기술을 단독으로 사용하는 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.

향후, 정보보호 기술의 발전은 암호 설계와 해독 기술간의 상호보완적 발전이 지속될 것이며 최신 신경망 이론, 인공지능 이론과 카오스 이론 등을 이용한 새로운 암호 시스템의 구성이 검토되고 있으며 Machine Learning 기술 또는 Quantum Computing 기술을 응용한 해독 기술도 가능하리라 본다.

참고문헌

[1] 한국전자통신연구소, "현대암호학", 1991.

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

[3] "Data Encryption Standard(DES)", National Bureau of Standards(U.S.A), Federal Information Processing Standard Publication 46, Apr. 1977.

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

[5] E. Biham and A. Shamir, "Differential Cryptanalysis of the full 16-round DES", Advances in Cryptology-Crypto 92, Springer-Verlag, pp.487-496, 1993.

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

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

[8] 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.

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

[10] M.J.Wiener, "Efficient DES Key Search",

Crypto'93 Rump Session, Aug.,1993.

[11] 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.

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

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

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

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

[16] 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.

[17] R.C. Merkle and M.E. Hellman "Hiding Information and Signatures in Trapdoor Knapsacks", IEEE Trans. Inform. Th., Vol. 24, pp. 525-530, Sep. 1978.

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

[19] H. C. Williams, "A Modification of the RSA Public-Key Cryptosystem", IEEE Trans. Inform. Th., Vol. 26, pp. 726-729, Nov. 1980.

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

[21] 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.

[22] H. W. Lenstra, Jr., "Integer Programming with a Fixed Number of Variables", Math. Operations Res., pp. 15-24, 1979.

[23] A. K. Lenstra and H. W. Lenstra, Jr., "Algorithms in Number Theory", in Hand-book of Theoretical Computer Science, J. Van Leeuwen, Ed.. Cambridge, MA : MIT Press, pp. 673-716, 1990.

[24] 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.

[25] C. Pomerance, "Fast, Rigorous Factorization and Discrete Logarithm Algorithms", in Discrete Algorithms and Complexity, D. S. Johnson, T. Nishizeki, A. Nozaki, and H. S. Wilf, Eds., New York : Academic Press, pp. 119-143, 1987.

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

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

[28] C.Kaufmann, R.Perlman, M.Speciner, Network Security, PTR Prentice Hall, 1995.

[29] NIST Pub. 185, "Escrowed Encryption Standard", U.S. Department of Commerce, Feb. 1994.

[30] NIST, "Clipper Chip Technology", Apr. 30, 1993.

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

[32] NIST, "Capstone Chip Technology", Apr. 30, 1993.

[33] 電子 認證 情報 セキュリティ大研究, pp.19-23, エレクトロニクス 1995년 9월호.

김 광 조

1973.3~1980.2 연세대 전자공학과 졸업(학사)
1981.9~1983.8 연세대 대학원 전자공학과 졸업(석사)
1988.2~1991.3 요꼬하마국립대 전자정보공학 졸업(박사)
1995.9~1996.2 충남대 자연과학대 대학원 컴퓨터 공학과(시간강사)
1979.12~현재 한국전자통신연구소 실장, ASIACRYPT '96 공동프로그램 위원장 충남대 컴퓨터 공학과 겸임교수, TTA JSC-27 의장, IEEE, IACR, IEICE, 한국통신정보보호학회 각 회원
관심분야 : 정보보호 기술 및 응용 분야, M/W 통신