□ 기술해설 □

암호기법

순천향대학교 이임영
한국전자통신연구원 박춘식

1. 서 론

최근 퍼스널 컴퓨터의 급속한 보급과 인터넷 사용의 급속한 신장은 정보화 사회의 도래를 앞당기고 있다. 특히, 인터넷의 영향으로 인한 전자화폐, 전자메일 등 EDI, CALS, 전자 상거래에 이르는 정보유통 산업의 물결이 밀려오고 있다.

한편, 공공 기관이나 연구 기관 등의 전산망에 대한 해커의 불법 침입, 컴퓨터 바이러스의 유포, 프라이버시 침해 등 정보화에 따른 역기능들이 속출하고 있다. 현재 역기능 방지 대책으로 알려져 있는 것이 정보보호 기술이며, 이 중 핵심 기술이 암호기법이다. 암호기법과 관련된 국제 동향으로 경제개발협력기구(OECD)에서 논의되어 1997년 5월경에 선포될 암호정책에 관한 가이드라인이 있다. 암호에 관한 국제적인 관심 고조와 암호 제품에 대한 수출 규제 완화의 추세는 국내에도 커다란 영향을 미칠 것으로 생각된다. 국내에서는 현재 전산망 보호대책의 수단으로 고려되고 있는 Firewall 등에 관심이 집중되어 있으나 암호 기법에도 관심이 고조될 것으로 예상된다.

원래 암호는 국방, 외교 등 특수 분야에 한정되어 사용되었으나, 현대에 와서는 인터넷과 전자 상거래의 영향으로 상업용으로 크게 부각되고 있는 실정이다. 본고에서는 이러한 흐름과 관련하여 암호 기법에 관한 기본적인 내용들을 소개하고자 한다.

제2장에서는 암호의 용어에 대해 제3장에서는 비밀키 암호에 대해서, 제4장에서는 공개키 암호, 그리고 인증 및 서명에 대해서는 제5장에서 다루기로 한다.

키 관리에 대해서는 제6장에서 그리고 전자 투표, 전자 화폐 등 암호 프로토콜 등 암호의 응용 분야에 이르기까지 개괄적인 내용을 제7장에서 소개하고자 한다.

2. 암호의 용어

암호(Cryptography)라는 것은 정보의 의미를 당사자 이외에는 알지 못하게 정보를 변환시키는 것이다. 그리고 암호학(Cryptology)이라는 것은 암호에 관한 학문 및 연구를 의미한다. 암호에 있어 본래의 문장을 평문(Plaintext)이라고 하고, 그것을 제3자가 모르게 암호문(Ciphertext)으로 변화시키는 것을 암호화(Encryption, Enciphering), 변환 절차를 암호 알고리즘(Encryption Algorithm)이라 한다. 암호화는 암호화키(Encryption Key)라는 파라미타에 의존한 변환이다. 당사자가 암호화키에 대응하는 복호화키(Decryption Key)를 이용하여 암호문을 본래의 평문으로 변환시키는 것을 복호화(Decryption, Deciphering)라 한다. 암호화와 복호화의 전과정을 총칭하여 암호 시스템(Cryptosystem)이라 하고, 암호화키와 복호화키를 총칭하여 암호키(Cryptographic Key) 혹은 키(Key)라 한다. 당사자들 이외의 제3자가 암호문을 본래의 평문으로 바꾸거나 혹은 키를 발견하고자 하는 일을 해독(Cryptanalysis)이라 한다.

현대 암호는 암호의 안전성을 암호키에 귀착시키고 있기 때문에 그 키를 알지 못하면 암호 알고리즘을 알고 있다 하더라도 평문을 얻기가

어렵다. 현재 많은 암호 알고리즘이 있으며, 그 분류의 관점도 여러 가지가 있다. 예를 들어 암호화키를 공개하는가 아닌가, 처리 대상이 블럭별인가 아닌가, 암호 동기가 필요한가 아닌가 등의 관점이 있다.

암호화키와 복호화키의 어느쪽으로부터 다른 쪽을 쉽게 구할수 있는 암호 시스템을 대칭 암호 시스템(Symmetric Cryptosystem), 쉽게 구할수 없는 암호 시스템을 비대칭 암호 시스템(Asymmetric Cryptosystem)이라 한다. 특히 암호화키로 부터 복호화키를 쉽게 구할수 없는 경우를 공개키 암호 시스템(Public Key Cryptosystem)[1]이라 하며, 이것은 암호화키를 공개하더라도 정보의 비밀을 유지하는 특징이 있다. 비대칭 암호인 공개키 암호 시스템에 대하여, 대칭 암호 시스템을 비밀키 암호 시스템(Secret Cryptosystem) 혹은 관용 암호 시스템(Conventional Cryptosystem)이라 한다.

3. 비밀키 암호

3.1 비밀키 암호 시스템

그림 1은 비밀키 암호 시스템 과정을 나타내고 있다. 암호화 과정은 알고리즘과 키로 구성되는데, 키는 알고리즘을 제어하는 평문과 무관하게 독립된 값이며, 알고리즘은 당시 사용된 특정 키에 따라 상이한 결과를 생성해내게 된다. 키를 바꾸게 되면 그에 따라 알고리즘의 결과도 변하게 된다. 일단 생성된 암호문은 전송되고, 수신된 암호문은 복호 알고리즘과 암호화에 사용됐던 것과 동일한 키를 사용하여 평문으로 재변환된다.

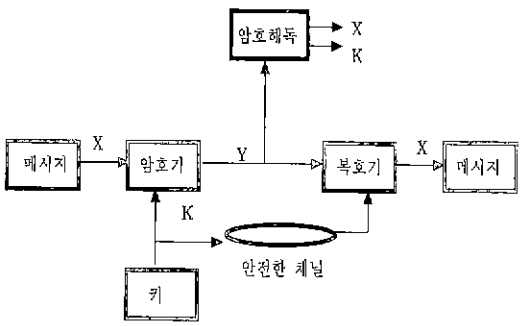

그림 1 비밀키 암호 시스템 모델

비밀키 암호 시스템에 대한 보안은 여러 가지 요소에 의존하게 된다. 첫째, 암호알고리즘은 암호문 자체만으로는 메시지를 해독할 수 없을 만큼 강력해야만 한다. 둘째, 비밀키 암호 시스템의 보안은 알고리즘의 비밀성이 아니라 키의 비밀성 유지에 달려있다. 즉, 암호문과 암호/복호 알고리즘이 주어졌다 해도 메시지의 복호가 불가능하다고 가정하는 것이다.

3.2 DES(Data Encryption Standard)

현재 가장 널리 사용되는 암호 기법은 1977년 미국 표준국(NBS : National Bureau of Standard, 현 NIST의 전신)에 의해 미 연방 정보처리표준46(FIPS PUB46)[2]으로 채택된 DES에 기초를 두고 있다. 비밀키 암호의 대명사인 DES는 64비트 입력을, 56비트 키를 이용하여 64비트 출력으로 변환한다. 복호화에는 동일한 키를 사용하여 동일한 단계가 암호화의 역순으로 사용된다.

DES 암호 기법의 개략적인 구성을 그림 2에 나타내었다. DES는 암호화 단계가 세 단계로 진행된다.

첫째, 64비트 평문의 치환된 입력을 생성하

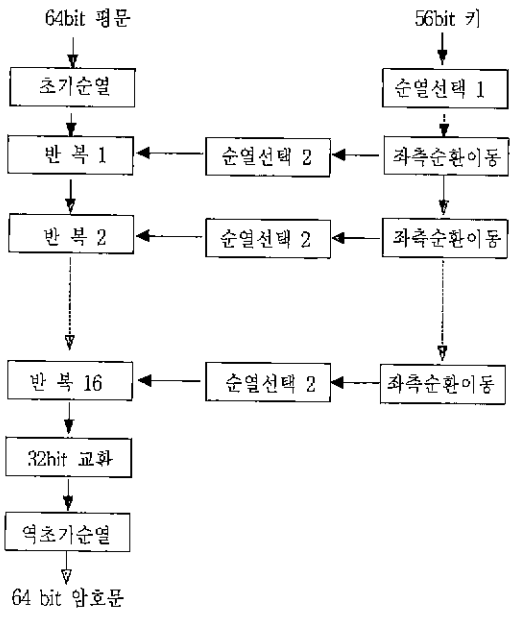

그림 2 DES 모델

기 위해 비트열의 순서를 재조정하는 초기순열(IP : Initial Permutation)단계를 통과한다. 다음엔 라운드 함수의 16회 반복 단계가 수행되는데 순열과 치환 모두가 포함된다. 마지막(16번째) 반복 처리의 출력은 입력 평문과 키의 함수 결과인 64비트로 구성된다. 이 64비트 출력의 좌우 절반은 예비 출력을 생성하기 위해 좌우로 교환된다. 마지막으로 이 예비출력은 64비트 암호문 생성을 위해 초기 순열의 역인 역초기 순열(IP^{-1})을 통과한다.

DES는 56비트의 키가 사용되어진다. 먼저 키가 순열 함수를 통과한다. 다음엔 16회의 각 반복에 대해 부분키(subkey)(Ki)가 좌측 순환 이동과 순열의 혼합 수행으로 생성된다. 순열 함수는 각 반복 과정에서 동일하지만 키 비트의 반복적인 이동으로 다른 부분키가 생성된다.

DES의 핵심부는 라운드 함수내의 f함수로 32비트를 48비트로 확장시키는 선형함수인 E(Expansion), DES에서 가장 중요한 역할을 하는 8개의 S-Box, 32 비트 치환인 P(Permutation)로 구성된다. f함수는 32 비트의 입력을 확장표 E에 의해 48비트로 선형 확장하여 48비트의 부분키와 비트 단위로 XOR 연산을 한 후, 8개의 lookup table인 S-Box로 입력하여 32비트 출력을 얻는다. 32비트의 S-Box 출력은 32비트 치환인 P를 통과하여 최종 32비트 출력을 얻게 된다.

DES에 대한 공격으로는 1990년 Crypto'90 암호학회에서의 입출력 변화 공격법[3]과 1993년 Eurocrypt'93 암호학회에서의 선형 근사 공격법[4]이 발표됨으로써 실질적인 공격이 가능해졌다.

또한 1993년, M.Wiener라는 사람은 Key Search Machine을 설계하여 100만달러를 투입하여 실제로 개발하면 평균 3.5시간만에 키를 찾아낼 수 있다는 논문을 발표하였다[5]. 현재까지의 연구 결과를 고려해보면 DES의 안전성에 문제가 있는 것으로 파악되고 있지만, DES를 3번 중첩하여 112비트의 키를 사용하는 triple-DES는 암호학적인 문제점이 아직 알려져 있지 않아 DES 대용의 표준으로 고려하는 움직임도 있다.

4. 공개키 암호

4.1 공개키 암호의 원리

공개키 암호는 비밀키 암호에서의 문제점들을 해결하고자 하는 시도로부터 발전된 개념이다.

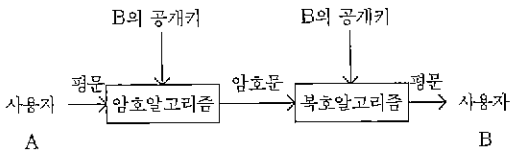

그림 3 공개키 암호의 간략 모델

그림 3은 공개키 암호화 과정을 보여주며 동작 과정은 다음과 같다.

1. 네트워크상에서 각 시스템들은 수신할 메시지의 암호화와 복호화에 사용되는 한 쌍의 키를 생성한다.

2. 시스템은 공개 기록집 또는 공개 파일에 암호키를 공개한다. 이것이 공개키이다. 또 다른 키는 비밀키로 개인이 가지고 있는다.

3. 만일 A가 메시지를 B에게 보내길 원한다면 B의 공개키를 사용해 메시지를 암호화하여 보낸다.

4. B가 암호문을 수신했을때, B의 비밀키를 이용하여 암호문을 복호화한다. 다른 어떤 수신자도 B의 비밀키를 알지 못하기 때문에 암호문을 복호할 수가 없다.

4.2 RSA 알고리즘

RSA 암호는 MIT의 R. Rivest, A. Shamir, 그리고 L. Adleman[6]에 의해 1977년에 개발되었다. RSA 암호는 이후 널리 사용되게 되었고 공개키 암호를 위한 접근 방법에 응용되었다. RSA 암호의 구조는 지수승을 가진 수식을 사용하도록 만들고 있다. 평문은 블럭에서 암호화된다. 이 블럭은 각 블럭이 어떤 수 n보다 적은 이진 값을 가진 블럭이다. 암호와 복호는 평문 블럭 M과 암호문 블럭 C에 대하여 다음의 형태를 따른다.

$$C = M^e \bmod n$$
$$M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n$$

송신자와 수신자는 n의 값을 알아야 한다. 송신자는 e의 값을 알고 수신자는 단지 d의 값만을 알면 된다. 그래서, 이것은 공개키 (e, n)와 비밀키 d을 가진 공개키 암호 알고리즘이다. 공개키 암호를 만족하기 위한 알고리즘은 다음 조건들을 만족해야만 한다.

1. 모든 M<n에 대하여 $M^{ed}=M \bmod n$인 e, d, n값을 찾는 것이 가능한가?

2. 모든 M<n인 값에 대하여 M^e, C^a를 계산하기가 쉬운가?

3. 주어진 e와 n에 대하여 d를 결정하기가 어려운가?

RSA 암호에 있어서 사용되는 변수들은 다음과 같다.

-비밀이며 소수인 p, q와 공개키인 n=pq

-$\gcd(\varphi(n),d)=1$, $1<d<\varphi(n)$인 비밀키 d

-$e\equiv d^{-1} \bmod \varphi(n)$인 공개키 e

사용자 A는 공개키를 공개하고 사용자 B는 메시지 M을 A에게 보내고 싶다고 가정하자. 그러면, B는 $C=M^e \pmod n$를 계산하고 C를 전송한다. 이 암호문을 받으면 사용자 A는 $M=C^d \pmod n$를 계산하여 복호한다.

이것은 RSA 알고리즘의 정의를 요약하기에 충분하다. 수식 $e\equiv d^{-1} \bmod \varphi(n)$에서 d와 e를 선택한다. 그러므로, $ed\equiv 1 \bmod \varphi(n)$이다. 결국, ed는 식 $k\varphi(n)+1$의 형태가 된다. 즉 $M^{k\varphi e(n)+1}=M^{k(p-1)(q-1)+1}\equiv M \bmod n$이 된다. 그래서 $M^{ed}\equiv M \bmod n$이다. 이제, $C=M^e \bmod n$, $M=C^d \bmod n\equiv (M^e)^d \bmod n\equiv M^{ed} \bmod n\equiv M \bmod n$

공개키 암호에는 RSA외에도 ElGamal 암호, Lucas 암호, 타원 곡선 암호, 양자 암호 등 많은 방식들이 제안되고 있다.

5. 인증 및 서명

5.1 메시지 인증

메시지가 송신 또는 전달 도중에 어떠한 변경이나 위조없이 수신자에게 전달되었다는 것을 확인하는 절차로 크게 통신문 복원법과 인증자 조회법으로 대별할 수 있다.

통신문 복원법은 수신측에서 복원된 통신문의 의미가 정당한 지를 인증하는 것이다. 메시지 전체의 암호문에 의해서 인증자를 만드는 것으로, 송신자가 통신문 m과 비밀키를 이용하여 암호화하게 된다. 수신자는 서명문을 복호화하여 복호화된 내용이 의미가 있는 지의 여부를 인증한다. 만일 의미가 없는 랜덤한 내용이면 원래의 메시지와 다른, 변경이나 위조가 발생하였음을 알 수가 있다.

통신문 복원법은 부속 정보로 일련번호나 시간 정보(timestamp)를 이용하여 안전성을 높일 수 있으며, 비밀키 암호나 공개키 암호로도 실현될 수 있다.

인증자 조회법은 패리티 검사 부호와 원리적으로 유사하지만 패리티 비트에 해당되는 인증자를 해쉬함수와 비밀키를 이용하여 발생하는 점이 다르다. 먼저, 송신자가 메시지 m에 비밀키와 일방향 해쉬함수 h를 이용하여 서명문인 인증자 h(m)을 발생하여 메시지 m과 함께 수신자에게 보낸다. 수신자는 수신된 메시지 m과 자신의 비밀키 그리고 해쉬함수 h를 이용하여 새로운 인증자 h(m)을 만들어 수신된 송신자의 인증자와 조회하여 본다. 만일 일치하면 송신자의 메시지는 변형없이 정확한 것임을 인증받게 된다.

인증자 조회법의 대표적인 것으로는 DES를 이용하는 MAC(Message Authentication Code)[7]이 있으며 메시지 인증 방식으로 가장 많이 사용되고 있다.

5.2 사용자 인증

사용자 인증은 사용자의 정당성을 식별하는 기술로 키나 카드 등 본인만이 가지고 있는 것을 식별하는 방법, 패스워드나 비밀키 등 본인만이 알고있는 정보를 이용하여 식별하는 방법 그리고 자문, 음성, 사인, 망막, DNA 정보 등 본인의 신체 특징 정보를 이용하여 식별하는 방법으로 크게 나눌 수 있다. 본인만이 가지고 있는 정보나 본인만이 알고 있는 정보는 분실, 도난, 망각 등의 가능성이 있기 때문에 신체 특징 정보를 이용하는 사용자 인증이 이중 가장 안전한 방법으로 알려져 있다. 그러나 이를 직접 구현하여 사용하기에는 많은 양의 데이터베이스 관리 등 실용상의 문제점이 많이 있어

특수한 용도에 한하여 사용되고 있다.

한편, 본인만이 가지고 있는 정보나 본인만이 알고 있는 정보를 이용하여 식별하는 방법은 암호를 이용할 경우 안전하고 실용적인 사용자 인증 방식이 될 수 있다. 널리 알려져 있는 방식들로는 패스워드 이용 방식, 일회용 패스워드 방식(One time password)[8], 시도 응답 방식(Challenge response), 영지식증명을 이용한 방식들이 있다.

5.3 디지탈 서명

디지탈 서명은 공개키 암호가 제공할 수 있는 하나의 특징으로, 수신자가 받는 메시지의 변조나 위조를 방지하며, 메시지의 송신자가 추후 부인할 수 없도록 하는 것으로 메시지 인증과 사용자 인증을 동시에 수행하는 것이다. 비밀키 암호를 이용한 메시지 인증에서는 송신자와 수신자 사이의 분쟁 발생시 문제 해결이 곤란하지만, 디지탈 서명에서는 제3자의 중재를 통하여 분쟁을 해결할 수 가 있어 전자 상거래 등에 널리 활용될 수 있다.

RSA 공개키 암호를 이용한 디지탈 서명 방식을 간략히 소개하면 다음과 같다.

먼저 서명자는 자신의 비밀키 Dk와 메시지 m을 이용하여 서명문 s=Dk(m)을 발생하여 메시지 m과 함께 수신자에게 보낸다. 수신자는 수신한 서명문 s를 서명자의 공개키 Ek를 이용하여 암호화한 결과와 수신한 메시지를 비교하면 된다. 어느 누구도 서명자의 비밀키는 알지 못하므로 m에 대한 서명문을 만들 수 없게되며, 서명자가 추후 부인할 수 없는 사유가 되기도 한다. 대표적인 디지탈 서명의 표준은 미국의 DSS[9]가 있다.

6. 키 관리

키 관리는 암호 체계에 사용되는 각종 관련 키를 체계적으로 보호하는 것으로 키의 생성에서부터, 저장, 분배, 주입, 사용, 보관, 파기 및 기록 등에 이르기 까지의 일련의 과정을 안전하게 그리고 효율적으로 관리함을 말할 수 있으며, 키의 라이프 사이클과도 관계된다. 암호 체계의 안전성은 키에 의존하므로 암호 시스템 전체의 안전성은 결국은 키 관리에 달려있다고 하여도 과언이 아니나, 실제로 암호 알고리즘의 안전성에 비하여 크게 고려되지 않고 있는 분야이다.

키 관리는 암호 체계에 사용된 암호 알고리즘이 비밀키 암호 알고리즘이든 공개키 암호 알고리즘이든 관계없이 항상 필요하다. 예를들면 비밀키 암호 알고리즘에 사용되는 비밀키와 공개키 암호 알고리즘에 사용되는 비밀키는 불법적인 키의 노출, 수정, 교체로부터 보호되어야 한다. 공개키 암호 알고리즘에 사용되는 공개키는 불법적인 수정과 교체로부터 보호되어야 한다.

키 생성은 주로 난수 발생기를 이용하는 경우로 사용될 키의 랜덤성 등 여러 가지 사항을 고려하여야 하며, 키 분배는 수동 분배나 자동 분배로 크게 분류될 수 있는데 암호 시스템의 사용 환경과 관리를 고려하여 정할 수 있다. 키 주입도 키보드 등의 수동 주입이나 스마트 카드 등의 전자매체에 의한 주입 등을 고려할 수 있다. 키 저장도 저장된 곳에 대한 물리적인 보호 대책이 강구되어야 하며, 키 사용이나 보관, 이력 관리, 그리고 파기 방법 등도 고려되어야 하는 데 이러한 모든 사항을 적용 환경, 장비 관리나 안전상의 조건을 고려하여 효율적으로 운영하는 것을 키 관리라 할 수 있다.

7. 암호 프로토콜

7.1 전자 투표[10]

전자투표는 선거인 명부를 데이터베이스로 구축한 중앙 시스템과 직접 연결한 단말에 자신이 정당한 투표자임을 증명하면 단말이 있는 전국 어디서나 쉽게 컴퓨터망을 통하여 무기명 투표를 할 수 있는 방식이라고 개괄적으로 정의할 수 있다.

현재까지, 암호를 이용하는 안전하고 신뢰성 높은 전자투표 연구가 다자간 프로토콜을 이용한 전자투표 방식, 익명 통신로를 이용한 전자투표 방식 등을 중심으로 행하여져 오고 있다.

Cohen이 제안한 방식[11]은 센터가 신뢰할 만한 경우에는 투표자의 privacy를 만족할 수

있으므로 전자투표의 신뢰성과 안전성이 센터에 크게 의존하게 된다. 이를 보완하여 즉 센터에 대한 의존성을 줄이면서 투표자의 privacy를 향상시켜 주는 방식인, 센터를 복수로하는 방식[12]도 제안되어 있다.

전혀 다른 방향에서의 접근으로, 익명통신로를 이용한 효율적인 전자투표 방식[13]이 있다. 최초로 제안된 것은 Mix형 익명 통신로를 이용한 D.Chaum의 방식[14]이다. 최근에는 이러한 방향에서의 연구가 활발하게 진행되고 있다.

7.2 전자 상거래

자택의 퍼스널 컴퓨터로부터 인터넷을 통해서 가상 상점을 방문하여 물건을 살 수 있는 것을 쉬운 의미에서의 전자 상거래(EC : Electronic Commerce)라 할 수 있다. 이러한 전자 상거래를 실용적으로 하기 위한 핵심은 전자 결제 시스템이다. 그래서 전자 결제 시스템은 신용카드로부터 시작하여 e-cash와 같은 네트워크형 전자 화폐로 발전하고 있다. 그리고 전자 결제 시스템의 중핵 기술은 시큐리티 기술이다. 즉, 전자 화폐의 발행과 결제 등의 단계에서 개인의 프라이버시와 이중 사용 문제를 해결하기 위해서 공개키 암호와 디지탈 서명 그리고 내용은닉서명(Blind Signature)[15] 등의 암호 기술이 사용되고 있다. First Virtual, Cyber Cash 그리고 e-Cash 등으로 대표되는 인터넷형 전자화폐와 이론적으로 연구되고 있는 전자화폐 방식중 최근 가장 관심을 끌고 있는 것 은Brands[16]의 전자 화폐 방식이다. 전자화폐는 사용자가 은행에 구좌를 개설하여 전자화폐를 발행받는 발행단계와 상점에서 물건을 사고 전자화폐를 지불하는 지불단계 그리고 상점이 은행에 전자화폐를 제출하고 자신의 구좌에 돈을 넣는 결제단계로 이루어진다. 전자 화폐에 대한 자세한 내용은 문헌 [17]을 참조하기 바란다.

8. 결 론

정보화 사회의 핵심 기술중의 하나인 암호기법에 대해서 간략하게 정리하였다. 비밀키 암호, 공개키 암호, 인증, 영지식 증명 그리고 전자 상거래에 이르기까지 광범위한 내용을 좁은 지면에 소개하다 보니 부족한 부분이 많은 것 같다. 보다 자세한 내용은 참고문헌[18, 19]을 이용하기 바라며, 관심있는 분들에게 약간의 도움이라도 되었으면 한다.

참고문헌

[1] W. Diffie and M. Hellman, "New Directions in Cryptography", IEEE Trans. on IT, Vol. I IT-22, No.6, pp.644-654, 1976.

[2] American National Standard for Data Encryption ALgorithm(DEA), ANSI X.3.92, 1981.

[3] E.Biham and A.Shamir, "Differential cryptanalysis of DES-like Cryptosystems", Advances in Cryptology, Proceedings of Crypto'90, pp.2-21, 1990.

[4] M.Matsui, "Linear Cryptanalysis Method for DES Cipher", Advances in Cryptology, Proceedings of EUROCRYPT '93, pp.386-397, 1993.

[5] M.J.Wiener, "Efficient DES Key Search", Rump Session in Crypto '93, 1993.

[6] R.L.Rivest, A.Shamir and L.Adleman, "A method for obtaining digital signatures and public key cryptosystem", Comm. ACM, Vol.21, No.2, pp.120- 126, 1978.

[7] ISO/IEC 9797, "Data Cryptographic Techniques-Data Integrity Mechanism Using a Cryptographic Check Function Employing a Block Cipher Algorithm", International Organization for Standardization, 1989.

[8] N.Haller and C.Metz, "A One-Time Password System", IETF RFC 1938, 1996.

[9] NIST, FIPS PUB 186, Digital Signature Standard, US Dept. of Commerce, May,

1994.

[10] 박춘식, "전자투표", 한국통신정보보호학회 학회지, 제6권 1호, pp.5-20, 1996.

[11] J.D.Cohen and M.H.Fischer, "A Robust and Verifiable Cryptographically Secure Election Scheme", Proceedings of the 26th Annual IEEE Symposium on the Foundations of Computer Science, pp.372-382, 1985.

[12] J.C.Benaloh and M.Yung, "Distributing the Power of a Government to Enhance the Privacy of Voters", Proceedings of the 5th ACM Symposium on the Principles in Distributed Computing, pp.53-62, 1986.

[13] C.S.Park, K.Itoh and K.Kurosawa, "Efficient Anonymous Channel and All /Nothing Election Scheme", Advances in Cryptology, Proceedings of Eurocrypt '93, pp.248-259, 1993.

[14] D.L.Chaum, "Untraceble Electronic Mail, Return Addresses, and Digital Pseudonyms", Communications of the ACM, Vol.24, No.2, pp.84-88, 1981.

[15] D.Chaum, "Security without Identification : Transaction Systems to Make Big Brother Obsolete", Comm] of ACM, Vol.28, No.10, pp.1,030-1,044, 1985.

[16] S.Brands, "Untraceable Off-Line Cash in Wallet with Observers", Advances in Cryptology, Proceedings of Crypto '93, pp.302-317, 1993.

[17] 박춘식, 이대기, "전자화폐가 세계를 바꾼다", 한국통신정보보호학회 학회지, 제6권 제2호, pp.53-70, 1996.

[18] 이임영 외 3인, "통신망 정보보호", 그린출판사, pp.1-510, 1996.

[19] B, Schneier, "Applied Cryptography, second edition", John Wiley&Sons, pp. 1-758, 1996.

이 임 영

1984 일본 오오사카대학 통신공학과 석사
1989 일본 오오사카대학 통신공학과 박사
1989～1994 한국전자통신연구원 선임연구원
1994～현재 순천향대학교 컴퓨터학부 교수
1997 한국통신정보보호학회 섭외홍보 이사
관심분야 : 암호이론, 암호응용, 정보이론, 통신이론

박 춘 식

1982～현재 한국전자통신연구원 책임연구원
1984 일본 동경공업대학 박사 (암호학 전공)
1989 일본 동경공업대학 객원연구원
1996 고려대학교 전자계산학과 강사
1997 한국통신정보보호학회 편집이사
관심분야 : 암호 이론 및 응용, 암호 프로토콜