□특집□

암호 기술

박 희 운† 이 임 영††

◈ 목 차 ◈

1 암호의 기초
2 비밀키 암호
3. 공개키 암호
4 디지털 서명 방식
5. 새로운 암호 기술
6. 결 론

1. 암호의 기초

1.1 암호의 개념

현대 사회는 개방형 네트워크의 급속한 발전과 정보 인프라의 구축을 통해 정보화 사회로의 입지를 넓히고 있다. 이러한 컴퓨터 네트워크 환경에서는 수없이 많은 정보의 교류가 진행되고 있으며, 정보의 안전성과 신뢰성을 보장하기 위한 수단으로서 암호가 적용되고 있다.

암호(cryptography)란 일반적인 평문을 해독 불가능한 암호문으로 변형하거나 또는 암호화된 통신문을 복원 가능한 형태로 변환하기 위한 원리, 수단, 방법 등을 취급하는 기술 또는 과학으로 정의하고 있다. 이러한 정의는 단순히 도청자나 그 밖의 요소로부터 통신 내용의 보호를 의미하는 것으로서 기존의 비밀키 암호, 스트림 암호, 블록 암호, 공개키 암호 등이 여기에 속한다.

그러나 정보 인프라의 구축은 단순한 전자 메시지 송·수신의 범위를 넘어서 다양한 부분에서의 응용이 제공 가능하다. 따라서 현대 암호의 범주에서는 기존의 암호 개념을 포괄하여 다음과 같은 분야들을 총칭하는 폭넓은 기술 및 이론을 암호 분야로서 포함하고 있다.

· 키 분배	· 인증(디지털 서명)	· 비밀 분산
· 의사 난수	· 영지식 증명	· 암호 프로토콜
· 전자 투표	· 전자 계약	· 전자 현금
· 양자 암호	· 고속 계산	· 해독법/안전성 증명

1.2 암호해독

개방형 네트워크를 통해 메시지를 전송하는 경우 안전성과 신뢰성을 위해 암호화된 메시지를 전송할 수 있음을 보았다. 이들 메시지는 정당한 수신자, 즉 암호문에 대응되는 키를 가진 사람만이 수신된 메시지를 복호화 할 수 있어야 한다. 그러나, 네트워크의 특성상 도청자 또는 불법적인 제 3자에 의해 공격이 가능하며, 이들을 통해 평문 또는 암호화 키를 발견하려는 시도 및 과정을 암호 해독(cryptoanalysis)이라 한다.

<표 1>은 주어진 정보에 따른 여러 유형의 암호 해독 공격을 요약하고 있다.

물론 암호문만 주어졌을 경우, 해독이 가장 어렵다. 그러나, 대개의 경우 공격자는 암호 알고리즘을 알고 있다고 가정한다. 그 외에도 공격자는 여러 가지 경로를 통해 <표 1>에서와 같은 정보를 보유할 수 있게된다. 예를 들어 평문이 어떠한 언어로 구성되었으며, 네트워크 특성상 패킷 패턴이 어떠한 특성을 갖는지 파악하는 등 다양하다. 만일 암호 해독자가 선택한 메시지를 시스템에

† 준회원 : 순천향대학교 전산학과 박사과정
†† 정회원 : 순천향대학교 정보기술공학부 부교수

삽입하기 위해 접근이 가능하다면 선택 평문(chosen plaintext) 공격이 가능하게 된다.

〈표 1〉 암호 메시지에 대한 공격 유형

공격 유형	요구 정보
Cipertext only	알고리즘, 암호문
Known plaintext	알고리즘, 암호문, 하나 이상의 비밀키에 의한 평문-암호문
Chosen plaintext	알고리즘, 암호문 해독자가 선택한 평문 메시지와 비밀키로 생성된 암호문
Chosen ciphertext	알고리즘, 암호문 해독자가 선택한 암호문과 비밀키로 생성된 그 암호문의 해독된 평문
Chosen text	알고리즘, 암호문 해독자가 선택한 평문 메시지와 비밀키로 생성된 암호문 해독자가 선택한 암호문과 비밀키로 생성된 그 암호문의 해독된 평문

현재 일반적으로 암호 알고리즘은 기지 평문(known plaintext) 공격을 막을 수 있게 설계되고 있으며, 일회용(one-time pad) 암호로 알려진 기법 외에는 절대적으로 안전한 알고리즘은 존재하지 않는 것으로 알려져 있다. 따라서, 암호 알고리즘 설계자들은 다음의 두 기준 중 하나 또는 전부를 만족하게끔 함으로서 안전성을 확득해야 할 것이다.

- 암호 해독 비용의 암호화된 정보 가치 초과
- 암호 해독 시간의 정보 유효기간 초과

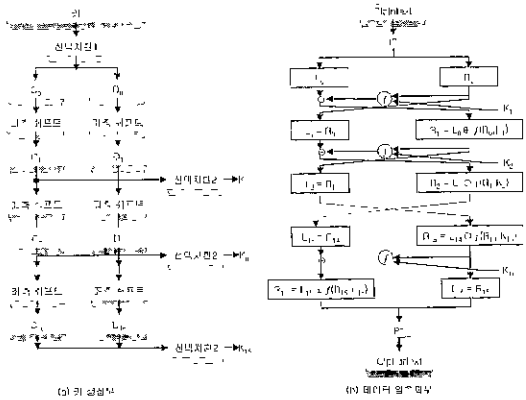
2. 비밀키 암호

암호 시스템은 키 관리 형태에 따라 크게 비밀키 암호 시스템(secret key cryptosystem)과 공개키 암호 시스템(public key cryptosystem)으로 나뉘어질 수 있다. 비밀키 암호화 방식은 다른 말로 대칭키 암호 방식이라고 하는데, 암호화 키와 복호화 키가 일치한다는 특징을 가지고 있다.

본 절에서는 근래까지 국제 표준으로 사용되는 DES와 향후 새로운 표준으로 제정될 AES의 제정 과정과 동향을 살펴본다.

2.1 DES

DES(Data Encryption Standard)는 1974년 컴퓨터 보안의 필요성에 의해 제안된 미 연방 정보처리 표준 46(FIPS PUB46)으로 채택된 대칭키 암호 알고리즘이다[1][2]. 현재 ISO의 표준(DEA-1)으로 제정되어 있으며, 지난 20년 동안 세계적인 표준으로 사용되어 왔다. DES는 56비트의 키를 사용하며, 16단계의 단일 반복 과정을 거쳐 64비트의 암호문 출력을 내는 Feistel 구조를 갖는다. 복호화 시에는 동일한 키를 사용하여 암호화의 역순으로 수행된다. (그림 1)은 DES 기본 구조를 나타낸 것이다.



(그림 1) DES 기본 구조

초기에 128비트의 키 길이로 설계되었던 DES는 NSA에 의해 56비트로 키 길이가 줄어든 이후 꾸준히 키 길이에 대한 논쟁이 있어 왔으며 컴퓨팅 파워가 증가하고 네트워크 기술이 발달하면서 DES에 대한 다양한 공격이 시도되어 왔다. 이에 DES의 대안으로서 안전성이 향상된 3중 DES(Triple DES)가 나오게 되었다. 이 알고리즘은

2개의 키를 사용함으로서 키 길이가 112비트로 늘어나게 되었으며, 이에 따른 안전성의 증가로 인해 키 관리 표준 ANS X9.17과 ISO 8732, 그리고 PEM (Privacy Enhanced Mail) 등에서 채택되어 사용되고 있다. 현재 3중 DES에 대한 실용적인 암호 분석 공격법은 없는 것으로 알려져 있다.

〈표 2〉 DES에 대한 연혁

분 류	내 용
1965-1972	· 컴퓨터 보안의 필요성 대두('68) · NBS는 NSA의 도움을 받아 표준화 작업 착수('72)
1973-1977	· DES 최초 공모 : 지원 없음('73) · 이차 공모 : IBM 지원('74) · DES 표준 공표('77)
1978-1989	· 5년 마다 안전성 평가 예정 · 80년대 논쟁 사항 - DES의 키 크기 논란, S-box의 설계 의혹, Trapdoor 가능성
1990-1995	· 5년간 유효 판전 · DC 및 LC 등장
1995-1999	· 3중 DES 사용 권고 --> AES 준비

2.2 AES

DES는 1977년 미국 연방 표준으로 공표된 후 매 5년마다 안전성 평가를 통하여 1998년까지 안전성을 인정받아 왔다. 그러나 컴퓨터 속도의 비약적 발전으로 56비트 키에 대한 안전성을 보장할 수 없게 됨에 따라, NIST에서는 1998년을 기준으로 DES를 대신할 새로운 128비트 블록 알고리즘 표준으로서 AES(Advanced Encryption Standard)를 공모하였다[3]. <표 3>에서는 NIST에서 제시한 AES에 대한 최소 조건을 명시한 것이다.

〈표 3〉 AES의 최소 조건

형 태	정부 및 상업 부분에서 사용 가능한 강력한 대칭키 블록 암호 알고리즘
안전성	· 3중 DES 보다 안전할 것 · 키 범위 : 128, 192, 256 (비트) · 블록 범위 : 128 (비트)
효율성	· 3중 DES 보다 효율적일 것
평가 방식	· 공개 검증 및 평가(비공식적 코멘트 가능)
비용	· 로열티가 없을 것

이 결과로 1998년에 15개의 알고리즘을 후보로서 선택하였으며 평가 기준에 의거하여 1999년 8월 9일에 5개의 알고리즘을 채택하였다. 평가에 있어 다음과 같은 사항에 대해 주안점을 두었다.

- 구현 측면
  : KAT(Known Answer Test)와 MCT(Monte carlo Test)를 이용해 테스트
- 효율성 측면
  : 메모리 및 계산상 효율성 비교(플랫폼 - 팬티엄 프로-200, 64M-RAM, Win95)
- 안전도
  : 암호학적 분석보다는 수학적으로 최적인지에 중점
  : 암호학적 분석은 공개적으로 수행(제안서 주장과 실질 안전도 비교)
- 알고리즘 구현 특성
  : 유연성 : 다양한 키 및 블록 크기 제공, 응용 환경 적합 여부
  : S/W 및 H/W 적합성 및 설계의 단순성

5개의 후보 알고리즘은 <표 4>에 기술되어 있으며, 2000년 8월에 최종 알고리즘이 채택될 예정이다.

〈표 4〉 AES 후보 알고리즘

알고리즘(국가)	제안자	라운드	형태
MAGENTA(독)	Deutsche Tele.AG	6,6,8	Feistel
MARS(미)	IBM	32(16)	Modified Feistel
RC6(미)	RSA Lab	20(10)	Modified Feistel
SERPENT (영,이,노)	R.Anderson, E.Bihan, L.Knudsen	32	SP
TWOFISH(미)	B.Scneier, J.Kelsey, D.Whiting, D.Wagner, C.Hall, N.Fersuson	16	Feistel

2.3 해독법

1989년 및 1993년에는 암호 분석 분야에서 특기할 만한 두 가지 공격법이 제시되었다. 하나는 Biham과 Shamir가 제안한 차분 해독법(differential cryptanalysis)이며, 다른 하나는 Matsui가 제안한 선형 해독법(linear cryptanalysis)이다.

다음에서는 이들 두 가지 해독법에 대해 다루고자 한다[4].

2.3.1 차분 해독법

DES와 같은 인볼루션을 이용한 블록암호에서는 ⊕의 배타적 논리합 연산이 다수 이용되고 있으며 배타적 논리합은 선형연산을 위해 다음과 같은 성질이 있다.

1) $x = y \oplus z,\ x' = y' \oplus z' \Rightarrow x \oplus x' = (y \oplus y') \oplus (z \oplus z')$

2) $x = y \oplus c,\ x' = y' \oplus c \Rightarrow x \oplus x' = y \oplus y'$

1)은 $x \oplus x'$, $y \oplus y'$, $z \oplus z'$로 표시되는 차분이 원소와 같은 관계를 충족시키는 것을 나타내고 있으며, 2)는 원소의 연산에 포함되어 있는 정수 c가 차분을 취하는 것에 의해 없어지는 것을 나타내고 있다. 이후 2개의 데이터 x와 x′의 차분 $x \oplus x'$를 x로 표시하는 것으로 한다.

상기의 차분에 관한 특성을 이용해 암호를 해독하는 수법으로 차분 해독법이 있다. 이 해독법은 1989년에 Biham과 Shamir에 의해 제안된 것이며 어느 일정한 차분을 가진 평문쌍과 그것에 대응한 암호문쌍을 다수 입수하고 이것을 이용해 키를 구하는 해독법이다. 따라서 차분해독법은 선택평문공격으로 분류된다.

16번의 단수를 가지는 DES의 경우, 단수 n이 증가하면 특수한 차분을 가지는 평문을 이용해도 n번째 단의 f함수의 입출력 차분이 어느 일정치가 될 확률은 단수와 함께 대단히 작아져 간다. 그로 인해 진짜 키의 출현빈도가 다른키와 구별할 수 있기 위해서는 그만큼 많은 평문상과 쌍이 필요해진다. 16단의 DES에서는 $(L_0,R_0) = ((1B600000)_H, (00000000)_H)$ 또는 $((19600000H, (00000000)_H)$가 차분해독법을 위한 가장 좋은 차분이 되고 있다. 또한 DES나 FEAL을 비롯한 각종암호 시스템에 대한 차분해독법의 상세한 해설이 문헌[4]에 소개되어 있으니 참고하기 바란다.

2.3.2 선형 해독법

차분 해독법은 선택 평문 공격이며 해독자는 자신에게 좋은 일정의 차분치를 가진 평문쌍과 그것에 대응한 암호문쌍을 다수 입수할 필요가 있다. 이것에 대하여 1993년에 Matsui에 의해 제안된 선형 해독법은 해독자가 평문을 자유롭게 선택할 수 없어도 평문과 대응하는 암호문을 다수 입수할 수만 있으면 암호키를 구할 수 있는 공격법이며 DES등의 인볼루션형의 블록암호에 유효한 해독법이다. 암호 알고리즘에 따라 해독법의 성능에 차이가 있겠지만, 일반적으로 선형 해독법이 더 효율적인 것으로 알려져 있다.

DES의 경우 정확히 키를 추정하기 위해서는 245개 정도의 평문 및 암호문 쌍이 필요하다고 추정되고 있으나, 선형 해독법의 경우 실제 243개의 평문과 암호문 쌍에서 56비트의 키 해독에 성공하고 있다.

3. 공개키 암호

공개키 암호 시스템은 비대칭 암호 시스템이라고도 불리우며, 수학적 함수를 기반으로 한다. 이 시스템은 비밀키 암호 시스템과는 달리 공개키와 개인키 쌍이 존재하며, 공개키는 누구나 사용 가능하고 개인키는 비밀리에 보관하는 방식을 의미한다. 이 방식의 배경에는 비밀키 암호 시스템의 키 관리 및 분배의 문제점을 해결하는데 중점을 두고 있으며, 동시에 디지털 서명에도 사용 가능

하다는 측면에서 그 응용 범위가 매우 넓다.

다음은 이들 중 대표적인 방식들을 소개한 것이다.

3.1 RSA암호

1978년 R. Rivest, A. Shamir, L. Adleman이 제안한 RSA암호는 수년 동안에 제안된 모든 공개키 알고리즘 중에서 이해 및 구현하기가 가장 용이한 알고리즘으로 평가받고 있다. 또한 이 알고리즘은 가장 대중적으로 알려졌으며, 아직까지 수많은 암호 분석을 이겨내고 있다[5]. 비록 암호분석이 RSA암호의 안전성을 증명하지도 반증하지도 못했지만, 나름대로의 알고리즘의 신뢰 수준을 제시하고 있다.

RSA암호는 큰 수의 인수분해의 어려움에서 안전성을 얻고 있으며, 공개키 및 비밀키 쌍은 큰 소수를 사용한다. 다음은 메시지 암호화 및 복호화를 위한 키 생성 단계를 나타낸 것이다.

· 키 생성 단계

1) 두개의 큰 소수 p와 q를 선정하여 합성수 n=pq를 법(public modulo)으로 한다. (pq는 비밀)
2) n을 공개하고 $\varphi(n)$과 서로소인 임의의 정수 e를 선택, 공개키로 한다.
(n이 두 소수의 곱일때 $\varphi(n)=(p-1)(q-1)$)
3) $ed \equiv 1 \pmod{\varphi(n)}$이 되는 d를 구해 비밀키로 삼는다.

이러한 절차를 거쳐 공개키와 유클리드 알고리즘을 이용한 비밀키가 생성되고 다음과 같이 암호화 및 복호화가 수행된다.

· 공개키 : n, e
· 비밀키 : p, q, d
· 암호화 : $C \equiv M^e \pmod{n}$
(공개키로 암호화)
· 복호화 : $M \equiv C^d \pmod{n}$
(비밀키로 복호화)

여기서, 만약 공개키 n과 e로부터 비밀키 d를 구할 수 있다면 RSA암호는 해독되게 된다. 이렇게 되기 위해서는 공개키 n으로부터 $\varphi(n)=(p-1)(q-1)$을 구해내야 한다. $\varphi(n)$을 구하게 되면 유클리드 알고리즘을 이용하여 쉽게 d를 구할 수가 있게 됨으로 RSA암호 알고리즘의 안전성은 n의 소인수 분해, 즉 p와 q를 구해내는 것에 달려 있다.

다음은 이와 관련하여 RSA암호의 안전성을 결정하는 조건들을 기술한 것이다.

1) 소인수 분해 문제와의 관계
RSA암호 암호의 안전성의 필요조건은 소인수 분해의 어려움이다. 현재까지 소인수 분해를 수행하지 않고 RSA암호를 해독하는 방법은 나와있지 않다.
2) 부분 정보의 안전성
RSA암호의 암호문에서 평문의 최하위의 1비트를 구하는 일은 암호문을 완전히 구하는 것과 같은 정도로 어렵다는 것이 증명되어져 있다.
3) e가 작은 값을 갖는 경우의 안전성
통상의 이용환경에서는 안전하지만 여러 사용자가 동일한 공개키를 사용할 경우, 중국인의 나머지 정리를 적용하여 M은 쉽게 구하여지고, 2개의 평문이 선형관계를 갖고 e가 작다면 암호문으로부터 메시지를 쉽게 구할 수 있다.
4) 소수의 조건
RSA암호에서 사용되는 소수는 아래와 같은 조건을 충족해야 한다.
· p-1이 커다란 소수를 포함. (그 커다란 소수를 r이라 한다.)
· p+1이 커다란 소수를 포함.
· r-1이 커다란 소수를 포함.
5) 키 사이즈
1996년 이후 소인수분해 알고리즘의 진보와

계산 능력의 향상에 의해 키 사이즈는 1024 비트까지 커졌다. 앞으로도 키 사이즈는 계속 증가할 것이다.

6) 안전성을 높인 이용방법

RSA 암호 방식을 이용할 경우, 평문이 한정된 공간에서 선택된다면 암호문에서 평문을 쉽게 구하는 것이 가능하다. 이러한 공격을 피하기 위해서는 난수 성분을 도입하여 해결 할 수 있다. RSA사의 PKCS#1는 이러한 생각에 근거한 RSA암호의 이용 방법을 제시하고 있다.

만약 RSA암호를 응용 분야에 적용하고자 한다면, 상기 조건들을 고려하여 사용함으로서 안전성을 유지해야 할 것이다. 그러나 현재 사용되는 RSA암호는 키를 선택함에 있어 계산상 큰 수를 사용함으로써 속도가 느리다는 단점을 가지고 있다.

3.2 Rabin 암호

Rabin 암호 방식은 합성수 모듈러에 관하여 제곱근을 찾기 어렵다는 사실로부터 안전성을 얻는다. 이러한 문제는 인수 분해 문제를 푸는 어려움과 동등한 문제이다. RSA 암호 방식에서 공개키 (n, e)의 e를 2로 바꾼 것이 Rabin 암호 방식이다[6]. 먼저 소수 p, q를 선택해 비밀로 한다. n = pq의 합성수 n과 $0 \le b < n$에서 임의로 선택한 b를 공개한다. 메시지 M의 크기는 n보다 작아야하며, 이때 암호문 C는 다음과 같이 계산된다.

$C = M(M+b) \bmod n$

메시지를 복호화하는 방법은 $f(x) = x^2 + bx - C$의 근을 GF(p)와 GF(q)에서 구한 후 중국인의 나머지 정리를 이용해 메시지 M을 구한다. Rabin 암호 방식은 평문 x의 이차식임으로 복호시 mod (p, q)에 의해 네 개의 평문이 구해지는 결점이 있다.

3.3 ElGamal 암호

ElGamal 암호 방식은 복호화시 Diffie-Hellman 방식을 그대로 응용하고 있으며, 이산대수 계산의 어려움으로부터 안전성을 얻는다[7]. 키 쌍을 생성하기 위해서, 우선 소수 p를 선택하고, p보다 작은 두 개의 랜덤수 g와 x를 선택한다. 그리고 다음을 계산한다.

$y = g^x \bmod p$

그런 후에 다음과 같이 암호화 및 복호화를 수행하게 된다.

- 공개키 : y, g, p (단, g와 p는 모든 사용자에게 분배)
- 비밀키 : x
- 암호화 : p-1과 서로소인 랜덤한 k 선택
  $a = g^k \bmod p,\ b = y^k M \bmod p$
- 복호화 : $M = b/a^x \bmod p$
  $b/a^x \equiv y^k M/a^x \equiv g^{xk} M/g^{xk} \equiv M \pmod p$

3.4 ECC

ECC(Elliptic Curve Cryptosystem)는 유한체 상의 타원 곡선이 유한군을 가지며 그 위에서 이산대수 문제가 구성될 수 있음에 착안되어 제시된 암호 알고리즘이다[8]. Diffie-Hellman 키 분배나 ElGamal 암호는 이산대수문제에 근거한 방식이며, 그러한 방식에 대응하는 암호 키 분배를 타원 이산대수 문제상에서 구성할 수 있다. 이러한 타원 곡선 암호는 1985년에 Koblitz와 Miller에 의해 독립적으로 제안되었다. 타원 이산대수 문제는 키의 크기를 비교적 작게(100~200비트)할 수 있는 실용상의 이점이 있다. 또한 장래 소인수 분해문제나 이산대수 문제에 대한 해법에 극적인 진전이 일어날지도 모르는 것에 대한 보험을 거는 의미에서도 그러한 것과 별도의 문제에 근거한 타원 곡선 암호의 의의는 크다.

다음은 이러한 타원 곡선에 근거한 ElGamal암호를 살펴보도록 한다. 이 방식은 ElGamal암호에 있

어서 유한체 상의 승법 연산을 타원곡선상의 가법 연산에 대응시키는 것에 의해 구성되며, 유한체의 r 승은 타원곡선상의 r배를 계산하는데 이용된다.

· 키 생성 단계

1) 공통 변수 (q, a, b, P, k, t)를 미리 정해 공개
2) GF(q)상에서 정의되어진 타원 곡선 선정
   $E_q(a, b) : y^2 = x^3 + ax + b$
3) 타원곡선상의 점 P의 위수 k가 커다란 소인수 t를 가지는 것으로 함
4) 이용자는 $x \in_U Z_k$를 정하고 $E_q(a, b)$상에서 키 Y = xP를 계산

키 생성이 이뤄진 후에는 다음과 같이 암호화 및 복호화가 수행된다.

· 공개키 : Y
· 비밀키 : x
· 암호화 : m : 평문, $r \in_U Z_k$: 난수
  $c_1 = rP$, $c_2 = rY + m$
· 복호화 : $m = c_2 - x_{c_1}$

4. 디지털 서명 방식

정보 인프라의 구축은 일반 생활에 있어 혁신적인 형태의 발전을 보이고 있지만, 동시에 전자 문서의 인증과 관련하여 다양한 요구 사항들이 창출되었다. 즉 송·수신 문서의 출처와 수신자의 확인 및 문서의 위·변조 방지 등은 필수적으로 요구되는 사항으로서 상당히 중요한 사안이 아닐 수 없다.

디지털 서명이란 전자화된 문서에 대해 메시지 내용이 수정 및 변조되지 않았음을 보장하는 동시에 메시지의 주체인 사용자들이 정확함을 제 3자가 확인할 수 있게끔 하는 인증 방식으로서 상기 요구 사항들을 만족하고 있다.

그러나 디지털 서명 역시 안전성이 결여될 경우 여러 공격이 가능하게 된다. 그러므로 디지털 서명의 안전성에 대한 고찰은 필수적이다. 디지털 서명과 관련하여 안전성은 위조불가성과 공격법이라는 관점에서 고려해 볼 수 있다. 위조불가성은 경우에 따라 다음과 같이 분류한다.

· 일반적 위조불가 : 서명의 위조가 불가능한 문서가 존재한다.
· 선택적 위조불가 : 정해진 문서 외에는 서명의 위조가 불가능하다.
· 존재적 위조불가 : 어떠한 문서에 대해서도 서명의 위조는 불가능하다.

또한 공격자에게 허용하는 공격법은 다음과 같다.

· 수동 공격 : 공개키만을 사용하여 위조하는 공격이다.
· 일반 선택문 공격 : 공격자는 미리 선택한 문서에 대해 진짜 서명자에게 서명시킨 후에 그것을 이용하여 제3의 문서에 서명을 위조하는 공격이다.
· 적응적 선택문 공격 : 서명위조자가 매회 임의로 선택한 문서에 대해 진짜 서명자에게 서명시키고, 마지막에 그것으로부터 얻은 정보를 이용하여 제3의 문서에 서명을 위조하는 공격이다.

따라서 가장 안전한 디지털 서명은 적응적 선택문 공격에 대하여 존재적 위조가 불가능해야 함을 알 수 있다. 현재 많은 종류의 디지털 서명 방식이 나와 있는 상태이며, 각 국의 특성과 환경에 맞게 다양한 형태를 보이고 있다.

다음에서는 이들 디지털 서명 방식들에 대해 살펴보기로 한다.

4.1 DSS

DSS(Digital Signature Standard)는 미국의 NIST (National Institute of Standards and Technology)에서 1991년 8월 30일 발표한 표준 디지털 서명안이다[9]. 그 핵심 알고리즘은 DSA (Digital Signature

Algorithm)으로서 약 6개월의 공개 검토를 거친 결과, 검토자의 90%정도가 문제점이 있다는 답을 한 것으로 알려졌다.

이러한 우려들은 여러 분야에서 일고 있는데, 트랩도어가 존재할 가능성과 기존 512비트의 법(modulo)의 값을 1024비트로 늘려야 한다는 주장이 나오고 있으며, 특허권에 있어 Schnorr의 특허에 걸려 있어 문제점으로 지적되고 있다.

다음은 서명 생성을 위한 공개 시스템 계수를 나타낸다. 서명자별로 다르게 만들 수도 있고, 공동으로 사용할 수도 있다.

· 키 생성 단계

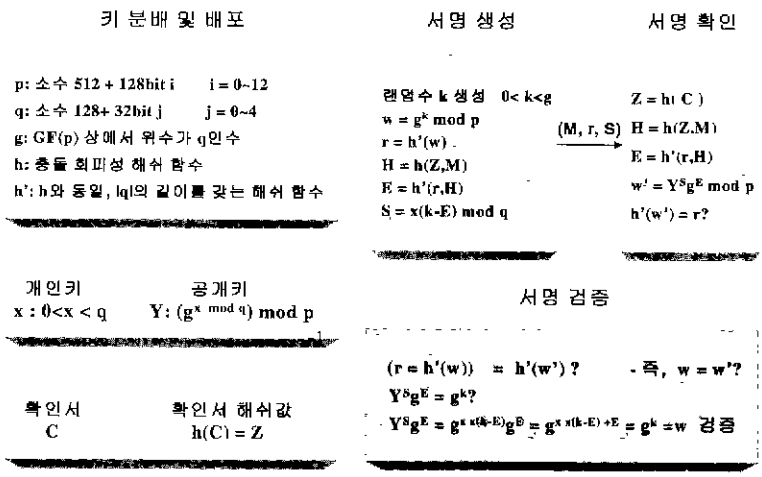
1) 우선 소수이면서 법이 되는 수 p (512 bit≤ p ≤1024 bit)를 생성하고, (p-1)의 소수가 되는 q (159 bit< q ≤160 bit)를 만들어 낸다. 그리고 다음을 생성한다.
   $g = h^{(p-1)/q} \mod p \ (1 \le h \le (p-1))$
2) 해쉬 함수 H를 이용하여 출력으로 160비트를 생성한다.
3) 비밀키 X(0< X <q)는 난수 또는 의사 난수 정수를 채택한다.
4) 사용자 공개키는 비밀키 X와 g를 이용해 다음과 같이 계산해 낸다.
   $Y = g^X \mod p$

그런 후에 다음과 같이 서명 및 검증을 수행하게 된다.

· 메시지 비밀 계수 K(0< K <q)를 랜덤하게 선택
· 서명 : 복호화시 비교 대상이 되는 $R = (g^K \mod p) \mod q$ 을 계산
  $S = K^{-1}(RX + H(M)) \mod q$
  : {R, S, M}을 검증자에게 전송
· 검증 : H(M)을 계산
  $(Y^{RS^{-1}} g^{H(M)S^{-1}} \mod p) \mod q = R$인지 확인

4.2 KCDSA

디지털 서명에 대한 중요성이 날로 증가하면서 국내에서는 1994년부터 디지털 서명 표준화에 대한 연구가 시작되었다. KCDSA(Korean Certificated Digital Signature Algorithm)는 국내 디지털 서명 표준화의 일환으로 개발된 서명 방식으로 1998년에 한국정보통신기술협회에서 그 표준을 규정하고 있으며, 여기서는 임의의 길이를 갖는 메시지 정보에 대해 부가형 전자서명을 생성 및 검증할 수 있게 해 주는 확인서를 이용한 부가형 전자서명 알고리즘을 규정하고 있다[10]. 공개 검증키는 CA라 불리는 모든 사람이 인정하는 제 3자가 공개 검증키 정보를 CA의 비밀키로 서명한 확인서를 배포함으로써 공개 검증키의 소유자를 보증한다.



(그림 2) KCDSA 서명 방식 구성도

(그림 2)는 KCDSA의 서명 과정을 도식화한 것이다.

이미 살펴보았던 DSS와 KCDSA를 비교해 보도록 한다. 이들 두 방식은 모두 이산 대수 문제를 푸는 어려움에 근거하고 있고, 오직 비밀키에 의해서만 서명이 생성되고 있으며, 결코 공개키를 통해서는 비밀키를 유출해 낼 수 없다는 특징을 가지고 있다. 이는 디지털 서명을 수행하는데 있어 안전을 위해 중요한 요소가 된다.

국외로 수출하는 부분에 있어 DSS와 Schnorr방식은 특허가 걸려 있는 관계로 제약이 있으며, 수출을 위해 그만큼 기능면에서 우수해야 할 것이라는 지적이 나오고 있다. 현재, 위 두 가지 방식은 어떤 해쉬 함수를 사용할 것인가에 대한 아무 정보도 없는 것이 특징이며, 아직은 고려 사항이다.

이상에서 살펴본 것 외에도 많은 디지털 서명 방식들이 존재하고 있으며, 이들의 응용 분야 또한 다양하다. 이러한 디지털 서명은 사소하게는 개인간의 안전한 통신에서부터 크게는 국가 기간 전산망을 위하여 꼭 필요한 요소이며, 그러기에 외국 기술의 의존보다는 국내 고유의 기술이 필요한 부분이라 하겠다.

4.3 특수 서명

디지털 서명은 일반 디지털 서명 방식과 특수 디지털 서명 방식이 있다. 특수 디지털 서명 방식은 서명자의 목적과 기능을 고려하여 다양한 범위에서 디지털 서명을 응용하여 사용할 수 있다. 다음은 이러한 특수목적을 가지는 디지털 서명 방식들에 대해 기술한 것이다.

4.3.1 부인 방지 서명

이 방식은 서명자의 도움 없이는 서명 검증이 불가능한 서명 방식이다. 이렇게 함으로서 서명자는 자신의 서명임을 검증자에게 확인시키며, 부인 과정을 통해 불법적인 서명에 대해 자신이 서명하지 않았음을 증명한다. 서명의 정당성을 확인하기 위해 대상이 되는 모든 서명자들에게 서명 확인을 수행하게 된다면, 서명자는 서명에 대한 확인이 불가피하게 되고 결국에는 서명자의 신원이 노출되는 문제점을 안고 있다[11].

4.3.2 의뢰 부인 방지 서명

부인 방지 서명이 서명자의 익명성을 보장하지 못하는 점을 부분적으로 개선한 방식으로 임의의 검증자가 부인 과정을 수행할 수 없도록 함과 동시에 오직 특정인만이 부인 과정을 수행하도록 함으로서 취약성을 부분적으로 제거한 방식이다[12].

4.3.3 수신자 지정 서명

수신자 지정 서명 방식은 지정된 수신자만이 서명을 확인할 수 있는 방식으로 서명자조차도 서명을 확인할 수 없도록 구성되어 있다. 이러한 특성을 통해 필요시에 제 3자에게 서명이 서명자에 의해 자신에게 발행된 정당한 서명임을 증명할 수 있게 된다.

그러나 서명에 대한 안전성이 수신자에게 의존하고 있기 때문에, 서명자에 대한 비밀 정보의 안전성이 완벽하게 보장될 수 없다는 문제점을 안고 있다[13].

4.3.4 은닉 서명

이 방식은 서명자가 서명문의 내용을 확인하지 못한 상태에서 서명을 수행하는 방식이다. 이를 통해 메시지 제공자의 신원을 보장하게되며, 메시지와 서명 사이에 연결성을 가질 수 없기 때문에 익명성은 유지될 수 있는 서명 방식이다[14].

4.3.5 대리 서명

본인의 부재 중 자신을 대신하여 다른 사람이 자신의 서명을 수행할 수 있도록 하는 서명 방식으로 검증자는 대리 서명자가 서명자의 위임 사

실을 확인할 수 있다[15].

4.3.6 그룹 서명

그룹 서명은 자신이 특정 그룹의 서명자임을 제 3자에게 증명할 수 있는 방식이다. 그러나 이 방식은 서명자를 알 수 없다는 특징이 있으며, 누구나 서명자를 확인할 수 있다[16].

4.3.7 다중 서명

다중 서명은 한 명 이상의 서명자가 동일 문서에 서명 수행이 가능한 방식으로 전자 결재나 전자 계약 등에 사용된다. 그러나 서명자가 n명이기 때문에 제약 사항이 따르게 되어 서명문의 길이 고정, 부정 조기 검출성, 비밀 유지성 및 공통성 등을 갖추어야 한다[17].

5. 새로운 암호 기술

5.1 양자 암호

양자암호(quantum cryptography)의 아이디어는, 1970년경에 쓰여진 Wiesner의 논문에서 시작되지만, 그 시점에서는 채택되지 못하고, 1983년에 Sigact News에서 소개되었다[18]. 양자암호는 불확정성 원리를 통신에 도입함으로써, 비밀키를 필요로 하지 않는 암호 시스템이 실현 가능하다는 것을 보여준 한 예가 된다.

양자 암호시스템에서는 통신매체로써 광자나 전자 등을 이용한다. 현재 고속 대용량의 통신기술로써 광통신이 많이 이용되고 있다. 그러나, 종래의 광통신 시스템은 기본적으로는 빛의 on, off에 의해 통신이 이루어지고, on일 때는 한번에 대용량의 광자가 송신되기 때문에 양자효과가 생기도록 한 개의 광자로 1 비트의 정보를 전송할 경우를 고려한다. 편광된 한 개의 광자를 송신했을 때 그 편광 방향에 적합한 측정기를 사용하지 않고 도청자가 그 광자를 관측하면 광자의 편광 상태에 변화가 생긴다. 따라서, 그 변화의 유무를 알아보는 것에 의해, 전송한 정보가 도청자에게 도청됐는가를 알 수 있다. 양자암호에서는 기본적으로 이 원리를 이용해서 암호시스템을 구성하고 있다.

Bennett-Brassard가 제안한 키 분배 프로토콜을 살펴보도록 한다. 빛은 편광 필터를 통과시키는 것에 의해 어는 특정 방향으로 편광시킬 수 있다. 또, 결정축 방향을 조정한 방해석에 수평(0°) 방향과 수직(90°) 방향으로 직선편광(linear polarization)한 빛을 통과시키면, 각각 굴절률이 다르기 때문에 그 편광 방향을 식별할 수가 있다. 이와 같은 수평수직 방향의 편광을 식별할 수 있는 장치를 0° 계 측정기라고 한다. 0° 계 측정기를 45° 기울여서 사용하면, 마찬가지의 원리로 45° 와 135° 의 경사진 방향으로 직선 편광한 빛을 식별할 수 있다. 이것을 45° 계 측정기라고 한다.

이와 같이, 수평수직방향으로 편광한 빛은 0° 계 측정기로, 또 45°/135° 로 편광한 빛은 45° 계 측정기로, 각각 정확하게 식별할 수 있다. 그러나, 45°/135° 로 편광한 빛을 0° 계 측정기에 통과시키면, 수평방향과 수직방향의 편광이 각각 랜덤하게 0.5의 비율로 출력된다. 그렇기 때문에, 그 출력을 관측해도 측정한 빛이 45° 로 편광되는지 135° 로

〈표 5〉 편광의 식별

측정전의 편광	0° 계 측정기	45° 계 측정기	식별불가일 때 측정기 통과후의 편광
수평편광	식 별 가	식별불가	45°/135° 가 동일확률로 출현
수직편광	식 별 가	식별불가	45°/135° 가 동일확률로 출현
45° 편광	식별불가	식 별 가	수평/수직이 동일확률로 출현
135° 편광	식별불가	식 별 가	수평/수직이 동일확률로 출현

편광되는지를 식별할 수 없다. 또, 식별 후에는 수평방향 또는 수직방향으로 편광되기 때문에, 식별 전·후에서 편광방향이 서로 다르게 된다. 마찬가지로, 수평 또는 수직방향으로 편광되고 있는 빛을, 45°계 측정기로 통과시키면, 45°로 편광되고 있는 빛과 135°로 편광되고 있는 빛이 0.5의 확률로 출력되고, 수평방향으로 편광되는지 수직방향으로 편광되는지를 식별할 수 없다.

이와 같은 식별능력의 한계는 측정장치의 결함이 아니고, 어떤 물리량을 측정하면 그것에 공역의 물리량이 랜덤화 된다는 불확정성 원리로부터 필연적으로 생기는 한계이다. 그렇기 때문에, 어떻게 측정기를 개량해도 이 특성을 개선할 수 없다. 공역의 물리량으로써 수평수직편광과 45/135 직선편광을 쌍으로써 사용하는 것 이외에, 수평수직편광과 좌우 원 편광을 쌍으로써 사용하기도하고, 또는 빛의 평광 대신에 전자를 비롯한 spin-1/2입자의 spin등을 사용할 수 있다.

Bennett 와 Brassard는 상기의 성질을 이용해서 도청자 W가 알 수 없도록 송신자 A와 수신자 B 사이에 비밀정보를 공유하는 방법을 제안했다. 비밀정보를 공유한 후에는 그 비밀정보를 비밀키 암호의 비밀키로써 사용하는 것에 의해 정보를 안전하게 전송할 수 있다. 그리고, 송신자 A와 수신자 B는 양자통신로 이외에 쌍방향의 공개 통신로(도청자 W도 도청할 수 있는)를 이용할 수 있다고 한다.

5.2 워터 마킹

전자상거래의 발전으로 멀티미디어 컨텐트(동영상, 오디오등)의 지적 소유권, 저작권의 보호에 대한 요구가 증가되고 있다. 워터 마킹(water-marking)은 멀티미디어 컨텐트에 사용자 정보를 감춤으로써 저작권 및 소유권을 보호하는 하나의 도구이다. 디지털 정보의 경우 복사시 화질의 저하가 없으므로 비디오 신호를 암호화하는 한정 접속 유니트에 개개의 워터마크를 포함하여 수신측에서의 불법적인 복사나 배포를 확인할 수 있다.

워터 마킹 기법이란 컨텐트의 불법 복제를 막고, 데이터 소유자의 저작권과 소유권을 효율적으로 보호하기 위한 방법으로써 데이터에 일정한 기밀정보를 숨겨서 부호화하는 과정으로 이러한 부호를 워터마크라 한다.

워터 마킹 기법은 외관상으로 거의 차이가 없고, 삽입된 워터마크는 컨텐트에 변형을 가해도 쉽게 없어지지 않는다는 특징이 제공되어야 한다. 이런 특성을 유지할 수 있는 것 중에 하나가 대역 확산을 이용한 방법이 있다. 워터마크를 많은 주파수 성분에 걸쳐서 분산시켜 삽입함으로써 결론적으로 에너지가 분산되어 한 주파수에서 보면 측정이 어렵게 만드는 것이다.

워터 마킹에 요구되는 특성에는 비 가시성(invisibility)과 강인성(robustness)이 있다. 비 가시성은 워터마크가 외관상 보이지 않고, 질 또한 감퇴되지 않아야 하지만 제공자는 워터마크 추출이 가능해야 한다는 것을 나타내고, 강인성은 워터마크가 컨텐트에 변형(압축, 자르기등)이 가해져도 컨텐트 내에서 추출이 가능해야 한다는 것을 나타낸다. 이러한 성질을 만족하기 위해서는 컨텐트의 중요한 부분에 워터 마킹을 해야 하는데 이것은 컨텐츠의 질을 감퇴시킨다. 이성질은 위의 비 가시성과 상반되므로 적절히 조정하여야 한다.

워터마크를 영상에 삽입 및 검출하기 위해서는, 원 영상에 임의로 만든 노이즈 형태의 신호 또는 가우시안 노이즈를 삽입한다. 대표적인 워터마크 삽입 방법에는 공간 영역과 주파수 영역에서 각각 원래의 신호에 선형적으로 워터마크를 더하는 방법이 있다.

워터마크의 검출시에는 자신이 소유권을 가지고 있는 컨텐트가 불법적으로 배포되었을 때, 변형된 영상에서 원래의 영상을 제거한 나머지와 원래 영상에 입혔던 워터마크의 상관계수를 구하

여 이 값이 어떤 임계치 이상이면 자신의 워터마크라고 판명하게 된다. 현재 워터 마킹 분야는 기존의 기술 외에 암호화 기법을 적용함으로서 더욱 안전하면서 신뢰성을 높일 수 있는 방법들을 모색하고 있다.

6. 결 론

정보화 사회의 급속한 발전을 통해 새로운 인프라의 시대상이 열리고 있다. 이러한 시대상은 사회 전반의 모습을 변화시키고 있으며, 동시에 의식의 변화를 수반하고 있다. 즉 실 시간적인 정보의 교류 속에서 개인 및 국가의 안전성과 신뢰성을 확보하기 위한 노력이 경주되었고, 그러한 가운데 암호의 필요성과 중요성이 대두되고 있는 상황이다.

본 고에서는 현대 암호의 큰 범주 내에서 자주 등장하는 주제들 중 몇 가지를 소개하였다. 기본적으로 암호와 암호 해독에 대한 상관성을 기술하였으며, 비밀키 및 공개키 암호 기법과 정보 교류에 있어 필수적인 디지털 서명 기법들을 간략하나마 살펴보았다. 동시에 근래 새로운 암호 기술로 등장하고 있는 양자 암호와 워터 마킹 기법 등을 소개하였다.

이 외에도 다양한 부분에서 적용 가능한 여러 암호 기법들이 연구되고 있으며, 향후 새로운 패러다임에 적응할 수 있도록 많은 관심과 지원이 부과되어야 할 것이다.

참고문헌

[1] ANSI X3.92, "American National Standard for Data Encryption Algorithm(DEA)," American National Standards Institute, 1981.

[2] National Bureau of Standards(U.S.), "Data Encrypt- ion Standard," Federal Information Processing Standards Publicatoin 46, National Technical Information Services, Springfield, VA(1977).

[3] "Advanced Encryption Standard (AES) Development Effort" http://csrc.nist.gov/ encryption/aes/, 1999.

[4] E. Biham and A. Shamir : Differential Cryptoanalysis of the Data Encryption Standard, Springer-Verlag, 1993.

[5] R. Rivest, A. Shamir and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems," Communications of the Association of Computer manufactures, vol. 21, no.2, pp. 120-126, Feb. 1978.

[6] M. Rabin, "Digitalized signatures and public-key functions as intractable as factorization," MIT Laboratory for Computer Science, MIT/LCS/TR-212, Jan. 1979.

[7] T. ElGamal, "a public key cryptosystem and a signature scheme based on discrete logarithms," IEEE Trands. Infor. Theory, vol. IT-31, pp. 469-472, 1985.

[8] N. Koblitz, "Elliptic Curve Cryptosystems," mathematics of Computation, v.48, n.177, 1987, pp. 203-209.

[9] "Specification for a Digital Signature Standard," NIST, FIPS XX. Draft, August 1991[1].

[10] 정보통신단체표준 "부가형 전자서명 방식 표준 - 제 2부: 확인서 이용 전자서명 알고리즘," www.kisa.or.kr., 1998.

[11] D. Chaum, "Undeniable Signature Systems," U.S. Patent #4,914,689, 3 Apr 1990.

[12] S. J. Park, K. H. Lee and D. H. Won, "An Entrusted Undeniable Signature," Proceedings of the 1995 Japan-Korea Workshop on Infor-

mation Security and Cryptography, Inuyama, Japan, 24-27 Jan 1995, pp. 120-126.

[13] S. J. Kim, S. J. Park and D. H. Won, "Nominative Signatures," Proc. ICEIC'95, pp. II-68 ~ II-71, 1995.

[14] D. Chaum, "Blind Signature Systems," US. Patent #4,759,063, 19 Jul 1988.

[15] M. Mambo, K. Usuda, and E. Okamoto, "Proxy Signatures," Proceedings of the 1995 Symposium on Cryptography and Information Security (SCIS 95), Inuyama, Japan, 24-27 Jan 1995, pp. B1.1.1-17.

[16] D. Chaum, "Group Signature," Advances in Cryptology-EUROCRYPT 91 Proceedings, Springer-Verlag, 1991, pp.257-265.

[17] C. Boyd, "Digital Multisignatures," Cryptography and Coding, H.J. Beker and F.C. Piper, eds, Oxford:Clarendon Press, 1989, pp.241-246.

[18] S. Wiesner, "Conjugate Coding," Manuscript written crica 1970, unpublished until it appeared in Sigact News, vol. 15, no.1, pp.78-88, 1983.

박 희 운

1997년 순천향대학교 전산학과 졸업
1997년-1999년 순천향대학교 전산학과 대학원 졸업 (공학 석사)
1999년-현재 순천향대학교 전산학과 박사과정 재학 중
관심 분야 : 암호이론, 컴퓨터 보안

이 임 영

1981년 홍익대학교 전자공학과 졸업
1986년 일본 오사카대학교 통신공학과(석사)
1989년 일본 오사카대학교 통신공학과(박사)
1989년-1994년 한국전자통신연구원 선임연구원
1994년-현재 순천향대학교 정보기술공학부 부교수
관심분야 : 암호이론, 정보이론, 컴퓨터 보안