特輯

# 정보보호 이론의 발전

金 光 兆 , *金 鐵
韓國電子通信研究所, * 光云大學校

## 요 약

정보사회로의 발전에 따라 부수적으로 발생하는 정보의 불법도청, 악용, 개조 등 역기능에 대비하기위한 정보보호의 필요성이 증대하고 있다. 본고에서는 이를 위한 정보보호 이론의 역사적 발전과정을 고찰하였다.

사용하는 용어를 정의한 후 각종 대칭형 및 비대칭형 암호 시스템에 대하여 소개하며, 개인 식별 정보를 이용한 암호 시스템, 그리고 영지식 상호증명에 대하여 기술하였다. 또한 정보사회의 정보 보호 기술의 응용분야를 기술하며, 향후 정보보호 이론의 발전 방향을 제시하였다.

## Ⅰ. 서론

개방화(Open System)와 분산화(Downsizing)의 확산과 개인 통신 시스템의 실현, 초고속 통신망의 구축 등, 급속히 다가오고 있는 정보사회에서 정보의 효용성과 중요성에 대한 언급은 재론의 여지가 없다.

저장중이거나, 전송중인 정보의 보호를 위해 많은 방법들이 이용된다. 정보에 물리적인 접근을 통제하는 것으로부터, 패스워드의 다단계 이용, 컴퓨터 운영체계의 강화 등 많은 수단이 있을 수 있다. 그러나 무엇보다도 on-line 통신망의 정보에 대한 직접적인 보호가 가장 효과적인 방책이 된다.

이 직접적인 보호방법은 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 대별하여 볼수있다.

이들 분야의 이론적인 배경은 정수론 (Number Theory), 추상 대수론(Abstract Algebra), 통계 및 확률론등 수학의 많은 분야에 기초하고 있다. 이들 이론을 응용하여 정보 자체의 암호화에 의한 보호와 나아가 정보 사회의 필수요소인 문서인증(Message Authentification), 위조할수 없는 전자 서명(Digital Signature), DB(Database)의 보호등에 활용하고 있다.

특별히 전자 서명은 EDI(Electronic Data Interchange)에 필수적인 요소가 되며, 이밖에도 앞으로 광범위하게 이용될 IC 카드등에 이 정보보호 이론은 핵심 이론으로 활용되고 있다.

본 고에서는 고대의 Caesar 암호 이후 제 1, 2차 세계대전을 거치면서 사용된 각종 기계식 암호 시스템, 1950년대 이후 통신과 컴퓨터 기술의 발달에 맞추어 등장한 전자적인 암호 시스템을 포함한 정보보호 이론의 발전과정을 고찰하고자 한다.

제 2절에서 는 용어를 정의하고, 고대로부터 1970년대까지의 기간을 대칭형 암호 시스템으로 묶어서 제 3절에서 살펴본다.

제 4절에서는 1970년대 후반 등장한 비대칭형 암호 시스템에 대하여 살펴보고, 이어서 제 5절에서는 ID-Based(개인 식별 정보에 기초한 암호 시스템, 그리고 영지식 상호증명(Zero Knowledge Interactive Proof, ZKIP)에 대하여 제 6절에서 살펴본다. 또한 제 7절에서는 정보보호 이론의 응용분야를 기술하며, 끝으로 결론을 맺는다.

## Ⅱ. 용어의 정의

(1) 정보보호(Information 또는 Data Security) : 시스템내의 각종 형태의 정보를 불법적인 제3자의 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 암호 분석학(Cryptanalysis)을 포함하는 것을 말한다.

(3) 암호시스템(Cryptosystem) : 적절한 암호화 기법을 채용하는 암호화, 복호화 과정으로 구성된 시스템으로, 암호화 및 복호화를 위한 키에 관한 부분과 이 키를 사용하여 일정 단계의 법칙등에 의해 암복호화 과정을 수행하는 알고리즘에 관한 부분으로 이루어져 있다.

(4) 암호문 단독공격(Ciphertext Only Attack, COA) : 암호 해독자는 오직 암호문을 이용하여 암호 시스템의 키나 평문을 구하는 공격방법으로 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 가정하에 이들을 이용하여 키를 구하여 다른 평문을 구하는 공격형태이다.

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

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

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

(9) 암호 프로토콜(Cryptographic Protocol) : 서로의 신뢰성을 확인하지 못하는 쌍방 혹은 다자간에 암호 시스템을 이용,정보의 기밀성과 인증을 만족시키는 안전한 통신절차를 가리킨다.

(10) 확산(Diffusion)과 혼동(Confussion) : 안전한 암호 시스템은 평문의 정보를 암호문의 전체에 고루 분산시켜야 한다. 평문의 각 사용문자에 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 대응관계를 알 수 없도록 하여야 하는데 이러한 특성을 혼동이라 한다.

(11) 대칭형 암호 시스템(Symmetric Cryptosystem) : 암호화 키와 복호화 키가 동일한 암호 시스템이다. 이 키는 쌍방이 공유하는 비밀 키이므로 전체 암호 시스템의 안전성을 결정하는 절대요소이다. 따라서 안전한 키의 분배 및 키의 초기값 결정이나 갱신을 위한 키의 관리가 요구된다. 이것을 재래식(Conventional) 암호 시스템, 또는 키가 동일하므로 단일키(one-key) 암호 시스템이라고 한다.

(12) 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 분배절차가 요구되지 않는다. 이것을 서로 다른 두개의 키가 사용되어 two-key 암호 시스템, 또는 두 키중 하나는 공개되므로 공개키(Public Key) 암호시스템이라고도 한다.

## Ⅲ. 대칭형 암호 시스템

본 절에서는 고대의 Caesar 암호인 단순 대치 암호시스템에서부터 시작하여, 1,2차 세계대전에서 사용한 기계식 암호 시스템, 계속하여 현대 암호 알고리즘의 대표격인 DES(Data Encryption Standard)등을 살펴보도록 한다.

## 1. 대치 암호 시스템

1)단순 대치 암호 시스템

본 방식은 평문의 각 문자를 영문의 알파벳순에서 일정한 거리만큼 앞 또는 뒤의 문자로 대치시키는 방법이다. 이때 그 대치간격이 키(key)로서 작용하게 되며, 비밀로 유지하여야 한다. 고대에 사용되었던 Caesar 암호 시스템에서는 이 키의 값이 3 이어서, 평문 MATH는 암호문 PDWK가 된다. 그러나 이 암호 시스템은 문자의 출현 빈도가 암호문에도 그대로 나타나기 때문에 표 1과 같이 문자의 빈도수를 이용하여 CPA가 가능한 단점이 있다.

표 1. 각 언어의 단문자 빈도 (%)

| | | | | | |
|---|---|---|---|---|---|
| 영 어 | E(12.31) | T( 9.59) | A( 8.05) | O( 7.94) | N( 7.19) |
| 독 일 어 | E(18.46) | N(11.42) | I( 8.02) | R( 7.14) | S( 7.04) |
| 불 어 | E(15.87) | A( 9.42) | I( 8.41) | S( 7.90) | T( 7.26) |
| 이탈리아어 | E(11.79) | A(11.74) | I(11.24) | O( 9.83) | N( 6.88) |
| 스페인 어 | E(15.15) | A(12.69) | O( 9.49) | S( 7.60) | N( 6.95) |
| 핀란드 어 | A(12.06) | I(10.59) | T( 9.76) | N( 8.64) | E( 8.11) |

2) 그밖의 대치 암호 시스템

단순한 대치 암호 시스템인 Caeser 암호 시스템이외에 이의 범주에 들어갈 수 있는 동음이의(Homophonic) 대치암호, 다표식(Polyalphabetic) 대치암호, 다문자 (Polygram) 대치암호 등이 있다. 먼저 동음이의 대치암호는 평문의 각 문자에 여러개의 문자를 대응시켜 암호문을 만드는 것으로써 평문의 문자 빈도와는 반비례하는 만큼의 대응 두자리 숫자들을 지정하여 암호화 하는 방법이다. 즉, 빈도수가 많은 A에는 23, 56, 34, 98등의 8개 숫자를, 빈도수가 A의 1/4인 P에는 59, 91의 2개 숫자를 부여하여 암호문 작성에 사용하는 것으로 미국의 Beale이 고안한 Beale암호가 그 예이다. 이러한 동음이의 대치암호에서는 평문의 각 문자에 대한 빈도가 위에서 언급된 빈도를 따르지 않게되며 암호문의 각 문자의 빈도차도 줄어든다. 따라서 암호문이 갖는 단문자 빈도의 특성이 감소하게 되나, 평문에서 보이는 두 문자 묶음, 또는 세 문자 묶음의 통계적인 특성은 여전히 암호문에서도 나타나게 되어있어 이러한 암호문 역시 COA가 가능하다. Gaine에 의하면, 두 문자 묶음의 빈도수는 표 2와 같다.

표 2. 두 문자 묶음의 빈도(%)

| | | | | | |
|---|---|---|---|---|---|
| TH (6.3) | IN (3.1) | ER (2.7) | RE (2.5) | AN (2.2) | HE (2.2) |
| AR (2.0) | EN (2.0) | TI (2.0) | TE (1.9) | AT (1.8) | ON (1.7) |
| HA (1.7) | OU (1.4) | IT (1.4) | ES (1.4) | ST (1.4) | OR (1.4) |

## 2. 다표식 대치 암호

다표식 대치암호는 다중 대치를 통하여 단순대치 암호와 동음이의 대치 암호시스템의 문제점을 보완한 암호 시스템이다. 이 다표식 대치암호의 대표적인것은 프랑스의 암호학자인 Vigenere (1523-1596)에 의해 제시된 Vigenere 암호이다. 이것은 표 3과 같이 26개의 영문자의 순서대로 이루어진 가로 26문자 세로 26문자의 표를 사용한다.

표 3. Vigenere 암호표

```
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
B C D E F G H I J K L M N O P Q R S T U V W X Y Z A
C D E F G H I J K L M N O P Q R S T U V W X Y Z B C
D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
.
.
.
Z A B C D E F G H I J K L M N O P Q R S T U V W X Y
```

이 표를 이용하여 암호화와 복호화의 예를 들어보자. 평문이 ADDDZ이고 사용하는 키가 ABC라 하면, (평문의) A행과 (키의) A열이 만나는 A, (평문의) D행과 (키의) B열이 만나는 E, (평문의 다음) D행과 (키의) C열이 만나는 F등이 되어, 암호문은 AEFDA가 되며, 복호화과정은 행과 열을 바꾸어 복호화하면 된다. 이와 유사한 다표식 암호 시스템으로는 다른 순서의 영문자를 사용하는 Beaufort 암호 시스템 등이 있다. 이러한 주기적 대치 암호를 풀기 위해서는 먼저 암호 시스템에 사용된 키의 주기(위의 예에서는 ABC이므로 주기는 3 이다. 를 결정하는 일이다. 주기를 비밀로 하는 주기적 대치암호는 1860년경 독일의 암호 해독가인 Kasiski가 주기를 찾는 방법을 제시하기 이전까지는 비교적 안전한 것으로 알려져 있었다.[1]

대치암호의 안전성은 키의 주기에 비례하므로 암호화 키를 평문의 길이만큼 길게하여 평문이 동일한 키로 암호화되는 경우를 없게 하면, 보다 안전한 대치

암호 시스템을 구축할 수 있다. 긴 주기를 이용하는 다표식 대치 암호 시스템을 실제의 기기로 구현한 것으로는 50년대초까지 미 육군에서 사용되었던 Hagelin의 Hagelin Machine이 있는데, 이는 주기가 각각 다른 6개의 휠(wheel)을 사용하고 있다. 이 외에도 널리 사용된 암호기계(물론 전기-기계식 기계이다.)로는 독일의 ENIGMA, 미국의 SIGABA, 일본의 RED, PURPLE 등이 있다.

그림 1. Hagelin Machine

그러나 Hagelin Machine 등은 키가 큰 주기를 갖는 암호 시스템이지만, 난수성을 갖는 키를 사용하고 있지 않으므로 문자의 통계적인 특성의 파악에 의한 공격에는 취약하다. 대치암호의 키가 큰 주기의 비주기성과 난수성을 가진다면, 이러한 암호시스템은 높은 안전도를 가지고 있으며, 이러한 암호 시스템을 One-Time Pad라 한다. 이때 키는 이 암호시스템의 이름 One-Time Pad에서도 알 수 있듯이 단 한번만 사용하여야 최대 안전도를 얻을 수 있다. 물론 이 One-Time Pad의 가장 불리한 점은 키의 운영이다. 키도 최소한 평문의 크기만큼의 정보를 안전한 통로를 통해 암호문과는 별도로 전달하여야 하는 점이 있다. 이 One-Time Pad는 1918년경 미국 AT&T의 Verman에 의하여 처음 제시된 이래 그 원리는 현재까지도 계속 응용되고 있다. 1970년대부터 사용하기 시작한 스트림 암호 시스템은 비주기성과 난수성을 가진 긴 키수열을 선형 쉬프트레지스터를 이용하여 발생시키는 암호 시스템이다. 키가 Hagelin Machine과 같이 어떤 주기를 갖고 반복되는 방식을 주기적 스트림암호(Periodic Stream Cipher), Verman의 암호 시스템에서처럼 키가 One-Time Pad인 방식을 비주기 스트림암호(Nonperiodic Stream Cipher)라 한다. 또한, 스트림암호는 평문과 키와의 관계에 따라 외부동기식(Synchronous)과 자체동기식(Self-Synchronous)으로도 나누어볼 수 있다.

이러한 스트림암호의 장점으로는, 각 Bit들은 평문의 다른 Bit의 영향을 받지 않고 즉시 암호화되므로 속도가 빠르다는 것과 각 Bit단위로 암호화되기 때문에 암호화 과정에서 발생될 수 있는 에러는 한 Bit에만 영향을 미치므로 에러 확산이 적다는 것이다. 반면, 이 스트림암호는 어떤 Bit의 삽입이나 변경에는 대처하기 어렵다는 단점을 가지고 있다.

### 4. 다문자 대치 암호 시스템과 전치 암호 시스템

앞서 언급된 암호방식과는 달리 평문을 한 문자씩이 아닌 보다 큰 문자 블럭단위로 암호화하여 해독을 어렵게하는 다문자(Polygram) 대치 암호 시스템이 있다. 이 암호 시스템의 대표적인것으로는 영국의 Playfair의 암호 시스템과 미국의 Hill의 암호 시스템이 있다. Playfair 암호는 영국의 Wheatstone에 의해 개발되어, 1854년 그의 친구인 Playfair에 의하여 발표된 암호 시스템으로 Boer전쟁과 1차 세계대전에서 사용되었다. 이 암호 시스템은 다음과 같은 25개 문자의 5x5 행렬을 이용하며, I와 J중 I만을 선택하고 나머지 24개 영문자를 중복없이 임의로 배열한것이다.

H A R P S
I C O D B
E F G K L
M N Q T U
V W X Y Z

원래의 Playfair 암호에서는 이 키 행렬의 생성을 위한 간단한 키 단어(Keyword)를 사용하기도 하였다. 이 키 행렬을 이용하여 암호화되는 과정을 살펴보자. 먼저 평문을 두 문자씩 나누어, 그 첫 문자를 @, 둘째 문자를 #라하면,

경우 1: @와 #가 같은 행에 있으면 암호문은 각각 바로 오른쪽 문자로 하고 마지막 열의 문자의 오른쪽은 첫째 열의 문자로 한다.

경우 2: @와 #가 같은 열에 있으면 암호문은 각각 바로 아래의 문자로 하고 마지막 행의 문자의 아래는 첫째행의 문자로 한다.

경우 3: @와 #의 열과 행이 모두 다를 경우, 암호문은 @과 #으로 그릴수 있는 사각형의 꼭지점의 문자로 하되 암호문의 첫째 문자는 @과 같은 행의 문자로, 암호문의 둘째 문자는 #와 같은 행의 문자로 한다.

경우 4: @와 #가 같은 문자이면, 그 사이에 임의의 문자를 넣는다.

경우 5: 평문의 문자의 수가 홀수이면, 평문의 끝에 임의의 문자를 넣어 암호화 한다.

Playfair 암호의 예로 평문 MATHEMATICS를 위의 키 행렬을 사용하여 암호문으로 만들어 보자. 먼저 두 문자씩 나누고, 위의 경우를 적용하면 암호문은 다음과 같이 만들어 진다.

평 문 : MA TH EM AT IC SZ
암호문: NH MP MV PN CO BS

이와같이 Playfair 암호는 평문 단문자의 통계적 특성이 암호문에서는 나타나지 않지만, 평문의 두 문자 묶음등의 통계적 특성은 암호문에서도 그대로 나타나게 되어 COA에 의해 해독될 수 있다.

다문자 대치 암호시스템의 다른 하나는 Hill의 암호이다. 이 Hill의 암호는 1920년경 미국의 수학 교수인 Hill에 의하여 제안된 암호 시스템으로 대수학(Algebra)를 이용하는 진정한 의미의 다문자 대치 암호 시스템이다.

## 5. 기계식 암호 시스템

위의 두가지 전치와 대치 기법을 합성시킨 암호시스템의 가장 현대적인 형태가 바로 후술할 DES이다. 이러한 합성 기법은 최초로 제 1차 세계대전시 독일의 ADFGVS암호를 들 수 있으며, 컴퓨터의 발달과 더불어 1970년에 IBM의 Feistel에 의해 개발된 Lucifer암호를 거쳐 DES에 이르고 있다. [1]

제 1,2차 세계대전을 거치면서 많은 암호화 장비가 등장하였다. 새로운 전기기계식 장치들은 보다 강한 암호를 생성할 뿐 아니라 정보를 암호화하고 해독하는 기술을 비약적으로 단축시켰다. 그중에서도 Enigma라고 불린 기계는 새로운 암호시대의 한 발판을 마련했으며, 세계 최초의 컴퓨터 제작에 간접적인 영향을 미쳤다. 1920년대 초반 독일의 Scherbius에 의해 상용목적으로 발명되어 30년대말 독일군에 의해 활용되었다. 이것은 타자기처럼 생긴 키보드와 한 개의 공통 축에 달린 세개의 회전자들을 복잡한 전기배선에 의해 연결한 전기기계식 암호장치이다. 사용자가 원문의 한 글자를 치면 회전자가 작동하여 그것을 암호화된 글자로 바꾸어 기계의 패널위에서 반짝이게 되는데 그 나타난 글자를 종이위에 옮겨 적으며 한 글자씩 암호화 하는 것이다. 이 암호문을 해독하기 위해서는 똑같은 기계를 가져야 함은 물론이고 회전자들의 원위치가 어디였는지도 정확히 알아야 한다.

이외에도 위에서 언급된 Hagelin의 M-209, Siemens와 Halske의 T-52 인쇄 가능 암호장비 등이 있다.

## 6. DES

Shannon은 그의 1949년 논문[4] 에서,본고 제 2절에서 정의한 확산(diffusion)과 혼동(confusion)을 교대로 사용하는 변환(mixing transformation)을 이용한 암호 시스템의 구성을 제시하였으며, 이 Shannon의 구성방법을 충실히 따른 것이 바로 DES이다.[5] DES는 64비트의 평문을 64비트의 암호문으로 만드는 블럭 암호시스템으로 64비트의 키를 사용한다. 이 64비트의 키-외부 키-중 56비트는 실제 키-내부 키-가 되고 나머지 8비트는 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 사용되는 키만 역순으로 작용하는 것이다.

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

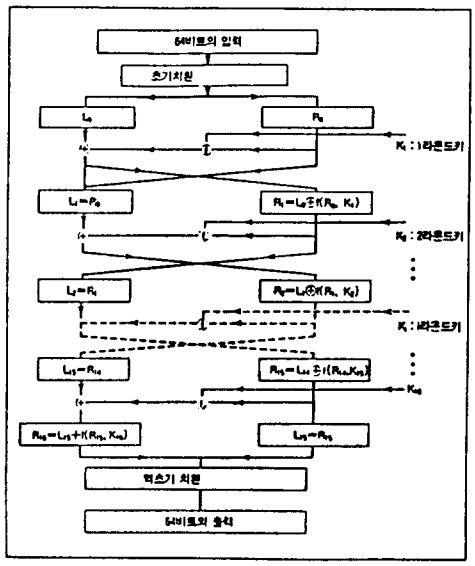



그림 2. DES의 암호화 과정

그후 DES를 해독하기 위한 H/W적인 혹은 이론적인 연구들이 계속되어 왔다. 대표적인 Differential 해독법(DC)과 선형 해독법(Liear Cryptanalysis. LC)에 대하여 언급한다. 1990년 Biham과 Shamir가 발표한 DC는 DES 뿐만 아니라 대부분의 관용 암호시스템을 쉽게 공격할 수 있는 새로운 공격방법으로 실용적 가치에 주목받고 있다.[6],[7]

DC를 발표한 이래 DES와 비슷한 비밀키 암호방식에 관한 해독법 연구가 상당히 진보되었다고 생각된다. 그들은 이어서 논문에서 FEAL 암호를 31단까지 CPA에 의해 해독하고, 최근의 논문에는 16단의 DES에 대한 CPA가 성공함을 제시 하였다.

한편, Dawson과 Tavares[8] 는 DES가 DC에 견디기 위해서는 S-box의 XOR 분포가 균일해야 한다고 하였으나 완전하게 균일한 XOR 분포는 오히려 균일하지 않을 때보다 더 취약하다고 언급된 연구결과도 있다. 결국, DES가 DC에 대응하기 위해서는 S-box만의 재설계로는 부족하며 암호함수 자체를 수정해야 할 것이다. 또한 DES의 비판과 논란의 대상이 되어왔던 문제를 해결하기 위해서는 키 길이를 늘리는 방안과 S-box를 재설계하고 그 방법을 공개하여야 할 것이다.

1993년 Matsui는 LC로 DES를 분석했다. LC는 DES에서 유일한 비선형 구조인 S-box를 적당히 선형화시켜 암호분석하는 KPA로 CPA인 DC와 유사한 방법이다. DC와 비슷하게 DES를 선형 암호 분석하기 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 암호분석은 어렵다.이 방법을 이용하여 1994년 1월 12대의 워크스테이션을 사용하여 50일 만에 16라운드의 DES를 해독한 실증적인 결과가 발표되는등 DES는 이제 암호 알고리즘으로서의 가치를 상실하고 있다. 이러한 DC나 LC는 키의 전수 탐색방법보다 효율적이나[9] 에 의하면 DC및 LC 방법이 키 전수 탐색방법보다 더 효율적이지 못한 S-Box의 설계조건을 제시하였다.

DES와 유사한 암호로는 일본의 FEAL(Fast data Encipherment ALgorithm)[10], 호주의 LOKI [11], 스위스의 IDEA(International Data Encryption Algorithm)[12], 러시아의 GOST(Government STandard) [13] 등이 있다.

## Ⅳ. 공개키 암호 시스템

대칭 암호 시스템에서는 암호화 키와 복호화 키가 동일하여, 키를 비밀로 유지하여야 한다. 따라서 송수신이 이루어지기 전에 송수신자간에 비밀키를 공유할 수 있도록 키 분배 (distribution)방법을 약속하여야 한다. 따라서 n명이 가입된 통신망에서 서로 비밀통신을 할 경우 n(n-1)/2개의 키를 각자가 안전하게 관리하며, 이때 n이 커질수록 상당량의 정보가 된다.

이러한 키 관리문제를 해결할 수 있는 암호 시스템이 바로 공개키 암호 시스템이다. 공개키는 이름과 전화번호가 나열되어 있는 전화번호부처럼 공개되는 것이다. 따라서 송신자와 수신자가 사전에 키의 분배를 할 필요가 없어 디렉토리 화일등에 공개 키를 알려주고 자신의 비밀키만을 철저히 관리하면 된다. 물론 공개 키와 비밀키의 두 키 사이에는 수학적인 관계가 있고 공개키에 의해서는 비밀키를 찾아내기가 거의 불가능하다. 송신자는 수신자의 공개키로 평문을 암호화 하여 공개적으로 보낸다.이 경우 수신자만이 자신의 비밀키로 그 암호문을 해독할 수 있다.

그리고 공개키 암호 시스템은 전자서명의 인증문제를 해결할 수 있다. 즉, 송신자가 자신의 이름등을

자신만의 비밀키로 암호화하여 전자문서에 첨부하여 보낸다. 그러면 수신자는 송신자가 공개한 공개키로 그 서명을 해독하여 그 서명이 송신자로부터 온 것인지의 여부를 알 수 있다. 다른 사람이 송신자의 이름을 도용하여 보내더라도 송신자의 비밀키를 모르므로 수신자가 송신자의 공개키로 다른 사람이 보낸 것을 해독하면 엉뚱한 이름이 나오게 된다.

대표적인 공개키 암호 시스템인 DH(Diffie-Hellman)의 공개키 암호 시스템과 RSA 공개키 암호 시스템에 대하여 기술한다.

### 1. DH 공개키 암호 시스템

Diffie와 Hellman은 1976년 공개된 채널상에서의 비밀키의 교환에 관한 다음 개념을 제안하였고 [14][15][16] 언급된 트랩도어 개념의 필요성을 역설하였다. 이러한 동일한 비밀키를 얻게 되면 송신자와 수신자는 이 키를 공유하여, 각기 자신의 평문을 암호화하거나 암호문을 해독할 수 있게 된다.

소수 p를 법으로 하면 법에 관한 덧셈 등의 그 연산의 결과는 0,1,2,…p-1 사이의 p개의 정수들이 된다. 이 p개의 정수중에는 원시근(primitive element)이라 불리는 정수 $\alpha$가 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.

$$3^0\equiv1,\ 3^1\equiv3,\ 3^2\equiv2,\ 3^3\equiv6,\ 3^4\equiv4,\ 3^5\equiv5 \pmod 7$$

이제 네트워크의 두 가입자 A,B 사이의 비밀키 생성 알고리즘을 살펴보자.

단계 1 : 가입자 A와 B는 1,2,…,p-1의 정수 중 임의로 각각 $X_A$와 $X_B$를 선택하고 이를 비밀로 한다.

단계 2 : 가입자 A는 $\alpha^{X_A} \pmod p$를 계산한 결과 $Y_A$ 를 가입자 B에게 (또는 공개키들의 저장소에)보내고, 가입자 B도 역시 $\alpha^{X_B} \pmod p$를 계산한 결과 YB 를 가입자A에게 (또는 공개키들의 저장소에) 보낸다.

단계 3 : 가입자 A는 받은 $Y_B$를 사용하여 가입자 B와 공유할 수 있는 비밀키 k를 다음과 같이 만든다.

$$k = Y_B^{X_A} \pmod p$$

B도 같은 방법으로

$$K = Y_A^{X_B} \pmod p$$

를 만든다. 이때 $Y_B^{X_A}$ 나 $Y_A^{X_B}$는 모두 $\alpha^{X_A X_B}$ 이어서 서로 같은 키를 갖게 되어 이 키 k를 사용하여 암호문을 만들고 해독할 수 있다.

이 DH 공개키 암호시스템의 안전성은 이산대수(Discrete Logarithm)문제에 근거하고 있다. 이산대수 문제란 X를 알고 있을 때 $Y = X$ 를 계산하여 Y를 알기는 쉬워도, Y를 알고 있을 때를 $X = \log_a Y$ 계산하여 X를 계산하기는 아주 어렵다는 것이다.

위의 단계 2에서 $Y_A$ 또는 $Y_B$ 가 공개되어도 $X_A$ 또는 $X_B$ 를 구하는데 걸리는 계산시간이 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 k를 계산하는데 1,000비트길이의 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 있다.

### 2. RSA 공개키 암호 시스템

1978년 Rivest, Shamir, Adleman에 의하여 제안된 RSA 공개키 암호 시스템[17]은 약 200자리 정수의 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 서로소의 관계에 있는 원소들의 개수를 $\phi(n)$으로 나타내고, 이를 Euler의 $\phi$ -함수라 한다. 특별히 소수인 p에 대하여 $\phi(p) = p-1$이다. 큰 정수 n에 대하여 $\phi(n)$값을 구하기 위하여는 n의 소인수 분해가 필수적이다.

즉 n이 두 소수 p와 q의 곱일때 $\phi(n) = (p-1)(q-1)$이다. 따라서 소인수 분해 없이 $\phi(n)$을 구하기는 매우 어렵다. Euler의 정리란 서로소인 두 양의 정수 a와 m에 대하여

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

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 = pq인 n을 공개하고 $\phi(n)$과 서로소인 임의의 정수 e를 선택하여 공개 키로 한다.

단계 3 : $e.d \equiv 1 \pmod{\phi(n)}$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 Me한 다음 법 n으로 간단히 한다. 즉 암호문 C는 다음과 같다.

$$C \equiv Me \pmod{n}$$

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

$$C^d \equiv (M^e)^d \equiv M^{t\phi(n)+1} \equiv M^{\phi(n)t}M \equiv M(\text{mod } n)$$

여기서 t는 $ed \equiv 1 \pmod{\phi(n)}$에서 유도되는 $ed = t\phi(n) + 1$ 을 만족하는 정수이다.

이제 간단한 보기를 살펴보도록 한다.

단계 1 : p = 11, q = 3 이라 하자.

단계 2 : 33을 공개하고 $\phi(33) = (11-1)(3-1) = 20$과 서로 소인 정수중 임의로 e = 3을 선택하여 공개한다.

단계 3 : $3.7 \equiv 1 \pmod{20}$ 이므로 d = 7 이다.

(이 보기는 간단하여 쉽게 7이 구해지지만 실제로 이렇게 간단하지는 않다.이 계산은 두 소수를 알고 있는 자신만이 할 수 있다.) 비밀키는 p = 11, q = 3, d=7 이며, 공개 키는 n = 33과 e = 3 이다.

암호화 단계 : 어떤 가입자가 자신의 공개 키 a = 33과 e = 3을 마치 전화번호부에서 찾듯이 찾아내어 평문 M = 5를 암호화 하여 암호문 $C \equiv 5^3 \equiv 125 \equiv 26 \pmod{33}$을 보낸다.

복호화 단계 : 이러한 암호문 C = 26을 받았다면 자신은 자신만의 비밀키 d = 7을 이용하여 $26^7$ 을 법 33에서 계산하여 평문 M = 5를 얻을 수 있다.

보다 안전한 RSA 공개키 암호 시스템을 위하여 p와 q를 선택하는 조건, e와 d에 대한 조건등이 부가적으로 필요하다.

RSA 공개키 암호 시스템은 공개키 n과 e를 가지고 비밀키 d를 구할 수만 있다면 무용지물이 된다. d를 찾기 위하여는 $\phi(n)$을 계산할 수 있어야 하는데 이를 위해서는 n의 소인수 분해가 필요하다. p와 q가 100자리의 소수이고 따라서 n이 200자리의 합성수라면 현재의 알고리즘과 전자기술로 n을 소인수 분해하는 것은 거의 불가능하다고 알려지고 있다. RSA 공개키 암호 시스템을 구현한(표 4참조) 현재의 상용 장비들은 512비트의 키, 즉 약 154자리 키들을 사용하고 있다. 이것이 56비트의 키를 사용하는 DES의 속도-약 100만 bps에 비하여 RSA의 속도는 1000bps로 늦은 이유 중의 하나이다.

소인수 분해의 어려움에 근거하는 RSA 공개키 암호 시스템들과 비슷한 암호 시스템들이 많이 제안되었다. 1979년 Rabin의 암호시스템[18], 1980년 William의 암호 시스템[19]등이 있다.

최근 1993년 초에는 RSA 공개키 암호 시스템의 PC상의 구현이 어렵고 전자서명상의 취약성이 발견되었기때문에 RSA 공개키 암호 시스템과 같은 소인수 분해의 어려움에 기초하는 LUC공개키 암호 시스템[20]이 제안되기도 하였다. 이는 Lucas(1842-1891)의 수열등을 이용하여 제안된 공개키 암호 시스템으로 뉴질랜드의 콘소시엄에 의해 특허로 보호받으며 구현되고 있다. RSA가 제안된 이래 특별한 경우를 제외하고는 일반적으로 이 RSA는 해독되지 않는다고 밝혀지고 있다. Alexi 등은 RSA에 의한 암호문 전체를 해독하는 것만큼 RSA에 의한 암호문의 한 비트를 회복하는 것도 어렵다는 연구결과를 내었다.

RSA의 해독은 전적으로 큰 수의 소인수 분해에 달려 있다. 빠른 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. 컴퓨터가 쉬는 시간을 이용 몇 십개의 컴퓨터를 네트워크로 연결하여 수주안에 인수분해할 수 있다고 주장 하였는데, 특별한 목적의 컴퓨터를 만들어서 해결하려는 종래의 사고방법과는 다른 개념이었다. 150자리의 특별한 정수는 인수분해가 되기도 하는 등 많은 수학자들이 큰 정수의 인수분해에 관한 연구를 하고 있다.[21-25]

RSA 암호시스템에 관한 기본적인 질문은 이 RSA가 과연 소인수 분해만큼 안전한가 하는 것이다. 물론 RSA를 해독하기 위하여 RSA에 법으로 사용되는 큰 정수를 인수분해 하는 것보다 빠른 방법은 없으리

표 4. 상용 RSA 칩 성능 비교

| 제 품 | 클럭 속도 (MHz) | 보드율 /512 비트(K) | 클럭사이클 /512비트 암호화(M) | 기 술 (마이크론) | 칩 당 비 트 | 직접도 Tr. 수 | CRT 사용 여부 | 발 표 년 도 |
|---|---|---|---|---|---|---|---|---|
| 알파 | 25 | 13 | 0.98 | 2 | 1.204 | 18,000 | ○ | - |
| AT&T | 25 | 13 | 0.98 | 1.5 | 298 | 100,000 | × | 1987 |
| 브리티시 텔레콤 | 10 | 5.1 | 1 | 2.5 | 256 | - | ○ | 1988 |
| 비즈니스 심 | 5 | 3.8 | 0.67 | 게이트어레이 | 32 | - | ○ | 1985 |
| 칼모스시스템 | 20 | 28 | 0.36 | 2 | 593 | 95,000 | × | - |
| CLET | 25 | 5.3 | 2.3 | 1 | 1,024 | 100,000 | ○ | 1988 |
| 크리프테크 | 14 | 17 | 0.4 | 게이트어레이 | 120 | 33,000 | × | 1988 |
| 시링크 | 16 | 6.8 | 1.2 | 1.5 | 1,024 | 150,000 | × | 1987 |
| 피즈넨버그 | 25 | 50 | 0.256 | 1.0 | 1,024 | 400,000 | × | - |
| 플래시크립토 | - | 10.2 | - | - | 512 | - | ○ | 1989 |
| 샌디아 | 8 | 10 | 0.4 | 2 | 272 | 86,000 | × | 1989 |
| 필립스 | 16 | 2 | 4.1 | 1.2 | 512 | - | ○ | 1989 |

출처 : Arto Salomaa, Publec-key Cryptography, 1990
(*) CRT(Chinese Remainder Theorem, 중국인의 나머지 정리)

라 추측되고 있지만, RSA가 그 안정성은 전적으로 소인수 분해의 어려움에 기인한다고는 증명되어 있지 않다.

## V. ID-Based 암호 시스템

대칭형 암호 시스템에서의 키 관리 어려움을 해결할 수 있는 것이 바로 공개키 암호 시스템이었다. 그러나 공개키 암호 시스템에서도 다수의 가입자가 사용할 때 각 사용자들의 키를 생성하고 분배하고 보관하는 키 관리의 어려움이 있다. 이러한 단점을 보완하기 위해 Shamir는 1984년 공개키 암호시스템으로서 사용자 개인의 고유한 개인 식별정보(Identity)를 키 생성 단계에 도입한 ID-Based 암호시스템과 디지틀 서명방식을 제안하였다.

그 후 개인식별 정보를 이용한 암호 시스템들이 다수 제안되었는데, 수신자의 공개 키를 수신자의 이름, 주소, 성별, 전화번호 등의 조합으로 구성된 함수로부터 공개 키를 도출함에 의하여 통신망내 별도의 키 센터를 유지하지 않아도 된다. 이는 다른 공개키 암호 시스템이 공개키 저장을 위한 전화번호부와 같은 키 보관 화일을 유지함으로써 통신시작시에 키 관리센터와의 과도한 통신량과 메모리가 요구되는 단점을 보완한다.

ID-Based 암호 시스템의 기본개념은 송신자의 ID를 이용하여 공개키를 계산하며 이를 이용해 문서를 암호화하고, 수신자는 자신의 ID로서 비밀키를 계산하여 문서를 다시 복호화한다. 이러한 ID-Based 암호 시스템의 개념을 이용한 ID-Based 서명방식도 가능하다. 즉 ID-Based 서명방식에서도 별도의 공개키 보관함이 필요하지 않다. 공개키 암호 시스템을 이용한 서명 방식에서는 송신자 자신의 비밀키를 이용하여 자신만의 서명을 생성하고 수신자는 송신자의 공개키를 사용하여 서명문의 인증을 결정한다. 반면 ID-Based 서명방식에서는 통신망이나 시스템에 가입할때 믿을 수 있는 키 생성/관리 센터(trusted key

distribution center)로부터 받은 비밀키를 이용하여 서명을 생성하고 수신자는 송신자의 ID로부터 공개 키를 계산하여 서명문의 인증을 결정한다.

이러한 ID-Based 암호 시스템이나 ID-Based 서명 및 인증방식도 많은 종류가 제안되어 있다. Shamir의 ID-Based 서명방법을 살펴보도록 한다.

믿을수 있는 키 생성/관리 센터에서는 가입자들을 위한 다음과 같은 키를 생성한다.

n : 임의로 선택한 큰 소수 p와 q의 곱

e : n의 Euler 함수값 $\phi(n)$과 서로소인 임의의 수

H : 해쉬함수(hash function)로, 한쪽으로는 계산하기 쉬우나, 그 역으로는 쉽게 계산되지 않는 함수를 말한다.

IDi : 각 가입자 i의 개인적인 식별정보

Si : 가입자 i만을 위한 비밀서명으로, $IDi\ (Si)^e \pmod n$를 만족하는 비밀키이다.

여기서 키 생성/관리 센터는, e, H, IDi는 사용하려고 등록한 모든 가입자에게 공개하고, p와 q는 센터가 비밀로 보관하며, Si는 사용자 i만이 갖고 있다.

가입자 i는 가입자 j에게 다음과 같은 단계를 거쳐서 문서 M에 서명한다.

서명단계 1 : 가입자 i는 임의의 난수 k를 선택한다.

서명단계 2 : 서명문 쌍 S와 T를 다음과 같이 계산한다. 여기서 처음 서명문의 계산 결과 S와 문서 M을 이용하여, 공개된 해쉬함수 값 H(S,M)을 계산한다.

$$S \equiv k^e \pmod n$$
$$T \equiv Si.k^{H(S,M)} \pmod n$$

송신자는 문서 M과 서명문 S,T를 수신자에게 보낸다.

인증단계 : 가입자 j는 받은 T와 공개된 e를 이용하여 구한 Te가 법 n에 관하여 $IDi.S^{H(S,M)}$와 합동인지를 검사한다. 가입자 i의 개인 식별정보에 대응하는 Si를 아는 가입자 i만이 문서 M에 대한 서명을 생성할 수 있으므로, 가입자 i는 문서 M을 가입자 j에게 자신이 보냈다는 사실을 부정할 수 없다.

인증이 되는 이유는 다음과 같은 관계식이 성립하기 때문이다.

$$\begin{aligned} Te &\equiv [Si.k^{H(S,M)}]^e \pmod n \\ &\equiv [Si]^e.k^{eH(S,M)} \pmod n \\ &\equiv IDi.S^{H(S,M)} \pmod n \end{aligned}$$

Shamir의 ID-Based 서명기법의 안전성은 $IDi \equiv (Si)^e \pmod n$를 만족하는 Si를 구하는 것이 어렵다는, 즉 IDi의 e차 제곱근을 구하는 것이 어렵다는 것에 근거하고 있다. 그러나 n의 소인수 분해를 안다면, CRT등을 이용하여 IDi의 e차 제곱근을 구할 수 있다.

## Ⅵ. 영지식 상호증명

정보보호 이론의 또 다른 응용으로서 이 암호 프로토콜(Cryptographic Protocol)을 들수 있다. 암호 프로토콜이란 기존의 통신 프로토콜에 정보보호 이론을 부가하여 안전한 정보처리 및 통신을 하는 알고리즘을 의미한다. 따라서 이 암호 프로토콜은 단순한 암호 알고리즘과는 달리 서로 알고 있지 않은 송신자와 수신자라도 통신망을 이용하여 서로의 목적을 이루는 상호 통신 알고리즘을 의미한다.

1980년대 중반부터 활발히 연구되고 있는 이 암호 프로토콜은 정보화 사회에 필수적인 개념이고 기술이며, 이의 많은 응용이 예견되고 있다. 문서의 전자서명과 인증은 안전한 공개키 암호 시스템에 의하여 문서에 서명을 하고 신분을 확인하였다. 그러나 이 기술은 그 서명이나 신분확인이 상호 동시에 균등히 행하여져야 할 필요성이 있을 때는 그 사용에 한계가 있다. 즉, 자신의 신분만을 노출시킨채, 상대방의 신분을 알 수 없으면 안되는 경우가 있을 수 있으며, 이렇게 서로 동시에 서명과 신분확인이 요구되는 경우 등의 동시성의 필요에 부응하는 것이 암호 프로토콜이 가진 큰 특성들 중의 하나가 되겠다.

좀 더 실제적인 예를 들면 다음과 같은 경우가 있겠다. 두 기업이나 사람간에 계약을 하는 경우를 보면 계약문서에 쌍방은 서로 서명을 받으려 한다. 상대방의 서명이 확인되지 않는 상태에서 먼저 일방적으로 서명을 하기는 어려운 일이다. 물론 약속된 장소에서 서로 만나 서로 지켜보는 가운데 서명을 한다면 모르겠으나, 통신망상에서의 계약의 경우 이러한 서명의 동시성, 상대방의 속임을 방지하고자 하는 기술에 대한 필요성은 지대하다. 이러한 필요에 부응할 수 있는 것이 암호 프로토콜이다.

또 다른 예로는 보물섬의 비유를 들 수 있다. 소년이 보물섬의 지도를 갖고 있다고 하자. 배가 없는 이 소년은 선장에게 보물섬의 지도가 있음을 말하고 배

를 타야한다. 그러나 소년은 그 지도를 배의 선장에게 보여줄 수는 없다. 지도를 보여줌이 없이 소년은 선장에게 보물섬의 지도가 있음을 증명하여야 하고, 또 선장은 그 사실을 확인할 수 있어야 한다. 이러한 경우도 역시 암호 프로토콜에 의하여 해결을 할 수 있다.

물론 전자 투표등의 경우에는 물론 암호 프로토콜 기술은 필수적이다. 이러한 암호 프로토콜의 예는 동전 던지기(coin flipping), Oblivious Transfer(알아채지 못하는 전송), 영지식 상호증명(Zero Knowledge Interactive Proof,ZKIP)등이 있다. 특히 영지식 상호증명기술은 암호 프로토콜의 안정성에 관한 모델로 통칭되기도 하며, 영지식 상호증명방식의 암호 프로토콜은 많은 응용 분야를 가지고 있다. 위의 보물지도의 예가 바로 영지식 상호증명의 비유가 되겠다. 영지식, 즉 그 지식을 누출함이 없이 상호증명할 수 있는 기법이다. 이 기법은 다음과 같이 스마트 카드에서 활용될 수 있다.

일반적인 여러 암호 시스템을 사용하는 방법은 키의 관리가 큰 문제점으로 대두되고 있다. 이에 대하여 서로의 비밀정보를 알 필요없이 인증을 하는 영지식 인증방법은 상대적으로 연산수가 작아 고속연산이 가능한 장점이 있어 스마트 카드에의 사용이 비교적 용이하다. 그러나 이 방법은 사용자 개개인의 정보에 근거하여 영지식 증명과정에서 사용될 비밀정보를 발생시켜 주는 믿을 수 있는 키 관리 센터(Key Management Center,KMC)가 필요하다. 이 인증방법으로 대표적인 Fiat-Shamir 방법[26]에 대하여 알아보자. 먼저 사용자에게 카드를 발급하는 단계는 다음과 같은 단계와 계산을 요한다.

단계 1: KMC에서는 카드의 개별적 식별을 위해 256비트 길이의 큰 두개의 소수 p,q를 생성하여 비밀로 한 후, p와 q의 곱인 n과 난수발생 함수 f를 공개한다. 여기서 f는 계산된 결과로서 원래의 초기 입력값을 찾을 수 없는 함수이다. 여기서 p,q는 후에 인증을 위하여 사용된다.

단계 2 : 카드를 발급받기를 원하는 사용자는 자신의 이름, 주민등록번호 등을 KMC에 제출하고 KMC는 이들 개인 정보에 유효기간, 사용의 범위 등을 부가하여 사용자 개개인의 식별정보 I를 계산한다.

단계 3: 먼저 KMC는 j = 1, 2, …, k와 I를 f에 대입하여 k개의 fj들을 얻는다.

즉, $sf_j = f(I, j)$, 여기서 j = 1, 2, … k

이후, 중국인의 나머지 정리를 이용하여 다음식을 만족하는 k개의 비밀정보 sj를 얻는다.

$s_j^2 = f_j^{-1} \bmod n$ 여기서 j = 1, 2, … k

단계 4 : KMC는 I와 k개의 비밀정보 $s_j$를 포함하는 카드를 보낸다. 카드는 또한 공개되는 n을 저장하고 있다.

이제 스마트 카드와 호스트 시스템 사이의 인증을 알아보자.

단계 1 : 스마트 카드는 호스트 시스템에 I 를 전송한다.

단계 2 : 호스트 시스템은 KMC와 같은 방법으로 j = 1, 2, …, k와 I를 f에 대입하여 k개의 fj들을 얻는다. 즉, $f_j = f(I, j)$, ( 여기서 j = 1, 2, … k )를 계산한다.

단계 3: 다음 단계를 t번 반복한다. 여기서 i = 1, 2, … t이다.

단계 3.1 : 스마트 카드는 0 에서부터 n-1 사이에 있는 임의의 난수 $r_i$를 선택하여 $x_i = r_i^2 \pmod n$을 계산하여 호스트 시스템에 이 $x_i$ 를 전송한다

단계 3.2 : 호스트 시스템은 길이가 k인 임의의 이진 벡터 $e_{i1}e_{i2}\cdots e_{ik}$를 발생시켜 이를 스마트 카드로 전송한다.

단계 3.3 : 스마트 카드는 받은 이진 벡터중 몇 번째가 1인지를 가려내어서 1에 해당하는 순서의 가지고 있는 비밀 정보 sj 들을 선택한다. 이렇게 선택된 $s_j$들과 단계 3.1에서 선택된 난수 ri들을 계속 곱하여 $y_i$들을 법 n에서 계산한 후 호스트 시스템으로 전송한다.

단계 3.4 : 호스트 시스템은 같은 방법으로 이진벡터중 몇 번째가 1인지를 가려내어서 1에 해당하는 순서의 $f_j$ 들을 k개 선택한다. 이들과 수신한 $y_i$의 제곱을 계속 곱하여 그 결과를 법 n에서 얻는다. 그 결과가 $x_i$와 동일한 지를 검증한다.

단계 4 : 단계 3을 t번 반복하는 동안 단계 3.4의 결과가 모두 동일하면 스마트 카드를 인증한다.

이외에도 영지식 인증방법에는 GQ(Guillou-Quisquater)방법[27]등이 있다.

## Ⅶ. 응용

정보보호 기술의 응용분야는 크게 나누어 통신 정보의 보호(Communication Security, COMSEC)

와 컴퓨터 정보의 보호(Computer Security, COMPSEC)로 나눌 수 있다. 통신 정보라함은 음성 정보를 포함하여, 각종 데이타 통신방식등에서 소통되는 모든 정보를 말하며 이를 효과적으로 보호하고 통신로 상의 불법적인 정보누출을 방지하는 것이 통신 정보보호의 목적이다. 이러한 통신 정보의 위협은 대부분의 경우 단순한 도청이나 도시로 개인이나 기업의 기밀을 악용하는 방법으로, 대부분의 경우 수동 공격 방법이 사용된다. 우리나라에는 현재 통신비밀보호법에 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 컴퓨터내에 저장된 귀중한 정보가 파괴되거나 조작된 사례는 무수히 많다. 우리나라에서도 1993년도에 해커가 청와대의 컴퓨터에 불법으로 위장 침입하여 허위문서를 하달하여 사회 문제가 된 바도 있다. 따라서, 컴퓨터 정보보호 기술은 파일보호 기술, 접근제어 기술, Network 시큐리티 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 기법등을 활용하여야 안전한 정보보호가 가능하다.

또한, 무역 정보거래에서 효율적인 처리방식으로 대두하고 있는 EDI시스템에서 보호기술, 컴퓨터 통신망을 통하여 메세지를 자동 전달하는 MHS(Message Handling System)의 보호기술, Internet등을 통하여 전달되는 전자 우편 시스템의 보호기술, 향후 전산망을 통하여 서비스가 예상되는 전자 선거시스템의 보호기술등 다양한 컴퓨터 정보의 보호기술이 요구된다. 은행 업무의 전산화에 따라 은행간 전자 자금 송금(Electronic Funds Transfer, EFT)시스템이나 슈퍼마켓의 거래 시점 자동 결재 (Point Of Sail, POS) 단말의 보호기술 등이 절실히 요구된다. 그 이외에 정보보호 기술은 정보가 발생되는 시간적, 공간적인 어떠한 곳에서 정보보호가 요구되는 정보유통에 있어 필수불가결한 기술로 대두되고 있으며 컴퓨터 범죄나 컴퓨터 바이러스 대책으로도 정보보호 기술이 활용된다. 이를 위한 정보보호 기술의 구체적인 내용은 본 특집호의 기타 논문을 참조하기 바라며 본 절에는 정보보호 기술의 각종 응용분야를 중심으로 기술하였다.

## Ⅷ. 결 론

본고에는 정보보호 이론의 기본 개념과 고대 암호 시스템으로부터 현대 암호 시스템에 이르기까지 개괄적인 소개를 하였다. 정보보호 이론의 역사는 유구하며 현대적인 암호는 통신과 컴퓨터의 발달과 더불어 끊임없이 발전을 거듭하였다. 재래식 암호 시스템은 주로 제 3 자에 의한 불법적인 도청을 방지하는 데 효과적이며, 공개키 암호 시스템은 정보사회에서 요구되는 안전한 정보 전달시 요구되는 인증이라는 새로운 문제를 해결하게 되었다. 키 관리상의 새로운 개념을 도입하여 개인 식별 정보를 공개키로 활용하는 ID-Based 암호 시스템은 정보보호 기술의 도입을 더욱 용이하게 하였다. 쌍방간 또는 화상회의 등의 다자간 통신이 요구됨에 따라 암호 프로토콜을 응용하여 불특정 다수의 통신자간의 전기 통신망을 통하여 서로의 프라이버시를 유지하면서 통신을 할 수 있도록 하게 되었다.

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

향후, 정보보호 기술의 발전은 암호설계와 해독기술간의 상호보완적 발전이 지속될 것이며 최신 신경망 이론, 인공지능 이론과 카오스 이론 등을 이용한 새로운 암호 시스템의 구성이 검토되고 있으며 Machine Learing 기술을 응용한 해독 기술도 가능하리라 본다.

최근 21세기를 대비하여 미국의 Super Highway 계획, 일본의신사회 자본 계획, 싱가포르의 IT-2000 계획등에 부흥하여 우리나라도 초고속 통신망 구현 계획이 발표되었는데, 통신망의 고장이나 사고가 발

생하였을 때 서비스의 중단을 방지하고 안전한 망의 유지 관리를 위하여 종합적인 정보보호 기술의 도입을 필연적으로 검토하여야 할 것이다.

## 參 考 文 獻


[1] 한국전자통신연구소, "현대암호학", 1991 한국전자통신연구소

[2] D. E. Denning," The Data Encryption Standard :Fifteen years of public security", Dist. Lecture, 6th Annual Comp. Security Appl. *Conf., IEEE Comp.* Soc. Press pp. x-xv 1990.

[3] H.Feistel,"Cryptography and Computer Privacy", Sci. Amer., vol. 228, no.5, pp. 15-23. May 1973.

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

[5] "Data Encryption Standard(DES)" , National Bureau of Standards(U.S.), Federal Information Processing Standard Publication 46, National Technical Information Service, Springfield, VA, Apr. 1977.

[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", Proc. of Crypto 92, 1992.

[8] M. H. Dawson and S. E. Tavares ,"An Expanded Set of S-Box Design Criteria Based on Information Theory and Its Relation to Differential-Like Attack", Proc. of Eurocrypt 91, 1991.

[9] K.Kim, S.Lee, S.Park and D.Lee, "DES can be Immune to Linear Cryptanalysis", To appear in 1994 Workshop on Selected Areas in Cryptography, Kinsgton, Canada, May 5~6, 1994.

[10] A.Shimizu and S. Miyaguchi "Fast Data Encipherment Algorithm FEAL", Proc. of Eurocrypt 91, 1991.

[11] L. Brown, K. Pieprzyk and J. Seberry, "LOKI - A Cryptographic Primitive for Authentication and Secrecy", Proc. of Auscrypt 90, 1990.

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

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

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

[15] W. Diffie and M. E. Hellman, "Multiuser Cryptographic techniques", in proceedings of AFIPS National Computer Conference, pp. 109-112 N.Y, June 7-10, 1976.

[16] 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.

[17] R.L. Riest, A. Shamir and L. Adleman, "A Method for obtaining Digital Signatures and Public Key Cryptosystems", vol. 21, no. 2, pp. 120-126 Feb. 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] A. K. Lenstra and M. S. Manasse, "Factoring by Electronic Mail", Proc. of Eurocrypt 89, 1989.
[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] A. Fiat and A. Shamir, "How to Prove Yourself : Practical Solutions to Identification and Signature Problems", Proc. of Crypto 86, 1986.
[27] L. C. Guillou and J. J. Quisquater, "A Paradoxical Identity Based Signature Scheme Result from Zero Knowledge", Proc. of Crypto 88, 1988.

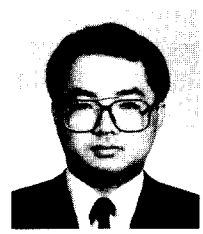
## 筆 者 紹 介

**金 光 兆**

1980年 2月 연세대 전자공학과 졸업(학사)
1983年 8月 연세대 대학원 전자공학과(석사)
1991年 3月 일본 요꼬하마 국립대 전자 정보공학과(박사)

1979年 12月 ~ 현재 한국전자통신 연구소 실장

주관심 분야 : 암호학 및 응용분야, M/W통신



**金 鐵**

1984年 2月 연세대 수학과졸업(학사)
1989年 12月 미국North Carolina 주립대 수학과(석사, 박사)
1988年 8月 ~ 1990年 6月 미국 Shaw University(전임강사)
1989年 8月 ~ 1990年 6月 미국 North Carolina주립대(시간강사)
1990年 8月 ~ 1991年 1月 미국 University of South Dakota(조교수)
1991年 3月 ~ 현재 광운대학교 수학과 (조교수)

주관심 분야 :부호 이론 및 암호 이론과 응용, 응용 대수학