韓國通信情報保護學會誌
第1卷, 第1號, 1991. 4

암호학 개요

정 진 욱*

1. 서 론

정보 보호의 문제는 유사이래로 많은 사람의 관심이 되어 왔으나, 최근 정보의 대부분이 컴퓨터에 의해 집중처리되고 이로 말미암아 정보보호의 파괴현상에 의한 부작용의 범위가 널리 확대되어 그 피해정도가 심대해짐에 따라 초미의 관심사로 재등장하고 있다.

정보보호에서 문제가 되는 중요 서비스로는 보관중이거나 전송중인 정보가 우연히 혹은 의도적으로 인가되지 않은 제3자에게 노출되는 것을 예방하는 기밀성(confidentiality), 정보가 변조되지 않고 원래의 상태를 유지하는 것을 보증하는 무결성(integrity), 통신하는 상대방이 정당한 상대방인가를 확인하는 인증(authentication), 인가되지 않은 사람이 정보에 접근하지 못하도록 하는 접근제어(access control), 정보의 발신 및 수신 사실을 사후에 부정하지 못하도록 하는 부인봉쇄(nonrepudiation) 등이 있다.

이러한 서비스들은 ISO 등의 국제 표준화 기구 등에 의해서도 컴퓨터 네트워크에서 수행될 기본 서비스로 표준화되고 있는데, 이들 서비스를 구현하기 위한 중요한 기술로 암호화가 가장 큰 비중을 차지한다. 실제로 접근제어 서비스와 부인봉쇄 서비스를 제외하고는 모두 암호화 기술을 응용하여 구현가능하다.

따라서 암호화 기술은 시저의 시대부터 관심의 대상이 되어왔고 계속 발전과정을 거쳤으며 제1, 2차 세계대전을 치르면서 큰 진전을 이루었다. 그러나 컴퓨터의 상용화에 따라 암호공격이 컴퓨터에 의해 행해질 수 있게 되어 그 이전의 대부분의 암호화 기술로는 정보보호를 효과적으로 수행할 수 없게 되었으며 본질적인 컴퓨터 암호화시대가 도래하게 되었다. 이에 따라 컴퓨터에 의한 공격에도 방어가 가능한 오늘날의 암호화 방식들이 등장하게 된 것이다.

가. 용어의 정의

□ 데이터 보호(data security)란 컴퓨터 및 통신시스템내에서 각종 데이터 및 메시지, 소프트웨어와 같은 고도의 정보를 제3의 침해로부터 보호하는 것으로, 데이터 보호의 목적은 데이터의 불법적 노출을 방지하여 합법적인 상대에게만 데이터를 전달해 주는 secrecy(혹은 privacy)와 데이터의 불법조작을 방지함으로써 송신자의 합법성을 보증시켜주는 authenticity(혹은 integrity)에 있다.

□ 암호학(cryptography)은 바로 이러한 pri-

* 정회원, 성균관대학교 정보공학과 부교수

vacy와 authenticity의 두가지 데이타 보호 문제를 해결하기 위한 수학적 시스템에 대한 연구분야이다. 또 암호(cipher 혹은 cryptogram)란 평문(plaintext)을 암호문(ciphertext)으로 변환하는 데이터 보호수단이며, 평문을 암호문으로 변환시키는 과정을 암호화(encipherment, encryption), 또 그 역과정을 복호화(decipherment, decryption)라 한다.

□ 암호계(cryptographic system)란 암호기법을 적용한 암호화 및 복호화 과정으로 구성된 시스템으로, 코드북을 사용하여 메시지를 암호화하는 코드시스템(codesystem)과 암호시스템(cipher system)으로 대별된다. 암호시스템은 또한 사용자에 의하여 선택되는 비교적 짧고 알려지지 않은 숫자 혹은 문자들의 순열로서 이루어진 암호키(cryptographic key)와 일정한 단계 혹은 법칙으로 이루어진 암호알고리즘(cryptographic algorithm)의 두가지 기본요소로 구성된다.

□ 한편 암호해독학(cryptanalysis)이란 암호시스템을 공격(attack)하는 기술에 대한 연구분야이며, 이를 연구하는 사람을 암호해독자(cryptanalysist)라 한다.

□ 혼동(confusion)과 확산(diffusion) : 좋은 암호는 평문의 정보를 암호문 전체에 고루 분산시켜야 하고 평문의 변경은 암호문의 여러 부문에 영향을 미쳐야 한다. 평문의 각 문자정보가 암호문 전체에 분산되는 특성을 확산이라 하며, 이 확산 정도가 커질수록 암호 해독자는 더 많은 양의 암호문을 필요로 하게 된다. 또한 암호 해독자는 평문의 어떤 문자가 암호문에서 어떤 문자로 바꾸어질 지 알 수 없어야 하는데 이런 특성이 혼동이다.

□ 암호화 프로토콜(cryptographic protocol)이란 신뢰할 수 없는 2자 이상간에 있어서 암호알고리즘을 이용, 정보의 secrecy와 정보와 사용자에 대한 authenticity를 만족시키는 안전한 통신절차를 가르킨다.

나. 암호의 역사적 배경

암호는 인류역사가 시작되기 이전부터 사용되어 왔으나, 국가가 형성되기 이전에는 비밀보전의 필요성이 극히 적어 암호의 이용이 거의 없었다. 그 후 국가가 만들어지면서 국가와 국가간의 이권, 그리고 상업의 발달에 따른 개인과 개인간의 이권이 개입되기 시작됨에 따라 암호의 필요성이 점차 증가하여 중세에 이르러서는 급속히 발전하였다.

하지만 중세에는 어떤 암호알고리즘에 의하여 정보를 알아보지 못하도록 숨긴다는 의미에서의 암호라기 보다는, 단지 남들이 알아 보지 못하도록 덮는다든가 혹은 감춘다는 의미에서의 steganographic method가 주로 많이 사용되었다. 그러한 기법중 자주 사용되었던 것중에는 종의 머리를 깎아 정보를 적은 다음 그 머리카락이 길어날 때까지 기다렸다가 이를 상대에게 보내는 방법을 비롯하여, 나뭇가지를 이용하여 열매가 달린 가지의 수에 따라 정보를 표현한 방법 등이 있다.

그후, 19세기 후반부터는 전기통신의 발달에 따라 유통되는 정보의 양이 급증하면서 이와 더불어 암호의 사용이 급증하였고, 20세기에 들어서면서 무선통신의 사용으로 암호의 사용은 극에 달하고 있다. 특히 세계 제 1 차대전과 2 차대전을 기점으로 암호수요는 크게 증가되었으며, 이에 따라 암호장비의 개발 등 암호발전에도 새로운 변화를 가져왔다.

더우기 최근에는 컴퓨터통신 및 데이터통신기술의 발달과 더불어 네트워크를 통한 정보교환이 널리 확산됨에 따라 통신망 또는 컴퓨터시스템내에서의 데이터 보호와 통신상대에 대한 합법성 확인(인증)을 위해, 컴퓨터 및 통신망상에서의 암호가 크게 주목을 받고 있다.

여기서는 이들 암호의 변천과정을 전기통신의 등장을 기점으로 그 이전 시대와 그 이후 시대로 나누어 살펴보도록 한다.

1) 전기통신이전의 시대

전기통신이 등장하기 이전에는 상호간에 정보를 전달하는 수단이 주로 사람이 종이에 쓴 문서에 의존할 수 밖에 없었다. 따라서 이 시대의 암호알고리즘으로는 종이상에서 그 조작이 가능한 문자들의 환자(substitution)와 전치(transposition)가

주류를 이루고 있다. 이 암호의 기본알고리즘은 그리스, 로마시대에 확립되었으며, 그중 시저의 암호, 라이산의 암호가 유명하다. 이들 암호방식은 문자 단위로 암호처리가 수행되었으며, 보다 암호화를 용이하게 하기 위해 암호키 테이블이나 실린더와 같은 간단한 기계적 장비가 사용되었다. 이 시대는 대부분 복잡하지 않은 환자나 전치방식에 의존하고 있었으므로 암호해독이 통계적 수단에의해 비교적 손쉽게 이루어졌다.

2) 전기통신의 시대

전기의 발명이후 암호는 기계화가 진행되어 본격적인 암호장비의 실용화시대를 맞게 됨으로써, 현대적 암호시대의 지표를 열게 되었다. 이 시대에는 주로 전기통신 선로를 통해 정보가 유통되었으므로 여기서의 정보보호를 위한 메카니즘 연구가 그 주류를 이루고 있다.

이 시대의 암호는 테이블에 의한 암호방식으로 기계적인 암호의 처리과정이 손쉬었으며, running key와 같이 키스트림을 길게 하여 암호강도를 높이기 위한 노력도 강구되었다. 또한 암호방식은 스트림암호이면서 알고리즘은 환자기법에 의한 모듈러연산의 합암호 알고리즘의 전성기였다.

대표적 암호장비로는 세계대전시 독일에 의해 발명된 ENIGMA를 비롯하여 인쇄기능을 부가한 M209 암호기, 9/7식 암호기 등이 여기에 속하는 암호기이다.

3) 컴퓨터의 시대

범용 디지탈 하드웨어가 개발되기 이전의 암호는 간단한 전동기(mechatronics)시스템으로 수행될 수 있는 동작에 국한되었다. 그후 디지탈 컴퓨터가 등장하면서 이를 이용한 암호해독 능력이 크게 배가되었으며, 암호해독 정도를 평가하는 파라미터, 즉 암호가 수학적으로 얼마나 계산하기 어려운가를 측정하는 난도(complexity)를 유도할 수 있게 되었다.

따라서 이 시대에는 보다 계산적으로 암호해독이 불가능한 암호기법에 대한 연구개발에 많은 관심이 모아졌으며, 이를 기점으로 암호학은 상당한 진전을 보게 되어, 1960년경에는 제 3 자가 알려진 평문만으로 암호문을 해독할 수 없을 정도로 암호시스템이 강하게 됨으로써 암호가 실제적으로 널리 사용되었다.

1960년대 후반에는 컴퓨터의 발전이 사회의 정보화를 급속하게 발전시킨 결과 프라이버시의 침해, 컴퓨터의 부정사용 등이 사회적으로 큰 문제를 야기시켰다. 따라서 비밀을 요하는 영역에서는 데이터를 안전하게 보호하기 위한 강한 암호의 필요성이 급증하게 됨에 따라, LSI 기술의 발달에 힘입어 상당히 복잡한 암호알고리즘을 단일칩상에 구현할 수 있게 됨으로써, 데이터처리에 필수적인 고속암호가 가능케 되었다.

1968년부터 1976년 사이에는 각 기업에 의해 보다 강도가 큰 암호가 등장하였는데, 1970년 IBM의 Feistel이 개발한 LUCIFER라는 블럭암호도 그 하나이다.

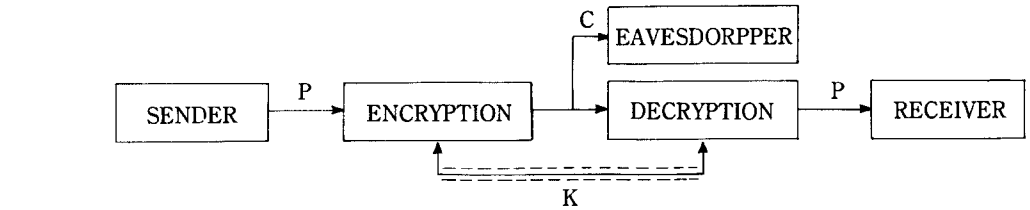
그후 Lucifer에 기초를 둔 새로운 암호방식이 IBM사의 Tuchman에 의해 개발된 환자와 전치알고리즘으로, 이는 미국 연방표준국에 의해 표준으로 채택되어 오늘날까지 가장 많이 사용되고 있는데, 이를 DES(Data Encryption Standard)라 한다. 그러나 DES와 같은 기존 암호방식은 오늘날에 이르러서는 이미 그 안전성을 신뢰할 수 없게 되었을 뿐만아니라, 키분배 등의 문제점을 안고 있었다.

이를 해결키 위한 새로운 암호방식인 공개키 암호방식에 대한 제안이 1976년 Diffie, Hellman에 의한 "New Direction in Cryptography"라는 초청논문에서 발표된 이래, Merkle, Hellman이 개발한 유한체상에서의 지수계산에 의한 암호알고리즘을 비롯하여, Riverst, Shamir, Adleman이 개발한 대표적 공개키 암호방식인 RSA방식 등이 등장함으로써 현대 암호이론의 근저를 이루고 있다.

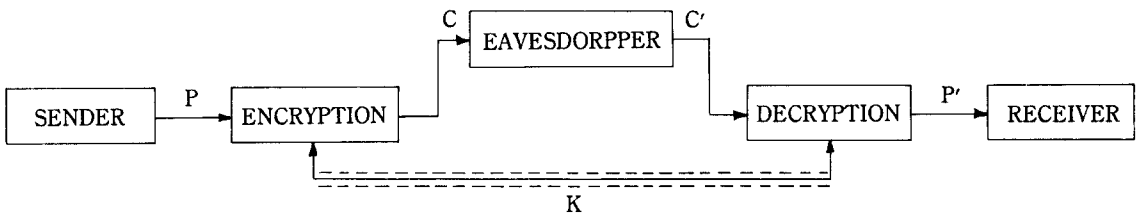
2. 암호학의 기초

가. 암호계의 기본 개념

암호학이 데이터 보호를 위한 두가지 기본적인 시큐리티문제, 즉 프라이버시와 인증문제를 해결하기 위한 수학적 시스템에 관한 학문이란 점은



(a) 프라이버시 암호계



(b) 인증암호계

그림 1. 암호계의 기본 구성

이미 앞에서 설명한 바 있다. 따라서 본절은 그 수학적 시스템인 암호계가 프라이버시와 인증문제를 어떻게 해결할 수 있는지를 언급하고자 한다.

먼저 그림 1(a)는 프라이버시를 보호하기 위한 암호계의 기본구성으로서, 송신자는 평문 P를 암호알고리즘 E와 암호키 K로 암호문 C를 생성하여 인정되지 않은 침해자가 감시하고 있는 통신채널을 통해 수신자에게 보내게 된다. 그러면 수신자는 이 암호문을 받아 복호알고리즘 D와 키 K에 의해 원래 송신자가 보내고자 했던 평문을 받게 된다.

만일, 이때 침해자가 채널을 도청하여(이를 passive wiretapping이라 한다) 암호문을 가로채게 되더라도 침해자가 복호알고리즘 특히 키를 알지 못한다면 암호문으로 부터 평문을 얻을 수 없게 되어 데이터에 대한 프라이버시를 보증할 수 있게 된다.

또 그림 1(b)는 침해자가 채널을 통해 흐르는 데이터에 대해 단순한 감시 뿐만 아니라 데이터의 추가삭제 및 조작을 할 수 있는 경우(이를 active wiretapping이라 한다)로서, 이 경우에 대해서도 침해자가 불법적인 복호알고리즘과 키를 가지고 채널에 흐르는 암호문을 조작하게 된다면, 수신자는 암호문을 복호시에 이것이 인정된 송신자에게서 온 정보인지를 확인할 수 있게 된다. 따라서 송신자에 대한 인증문제를 해결할 수 있다.

나. 암호해독(cryptanalysis)

암호해독자는 암호방식을 깨뜨리기 위하여 암호문으로 부터 평문을 찾아내기 위한 노력, 즉 암호분석을 행하게 되는데, 이때 암호해독자는 암호알고리즘을 알고 있다고 가정하고 이로부터 키를 찾기 위한 시도에 들어간다. 일반적으로 암호분석을 위한 기본적인 공격방법은 다음 세가지로 나눌 수 있다.

1) ciphertext only attack

암호해독자는 단지 암호문만을 갖고서 이로부터 키를 찾아내야 하는 공격법으로, 이때 평문이 용장도(redundancy)나 일정한 형식을 갖는 텍스트가 아니라면 여기서 키를 찾는 것은 거의 불가능한 가장 힘든 공격법이다.

2) known plaintext attack

평문이 어떤 프로그램언어로 쓰여진 formal structure를 갖는다던가 혹은 일정한 양식의 텍스트라면 암호해독자는 암호문으로부터 쉽게 평문을 찾아낼 수 있게 되는데, 이 공격방법은 찾아낸 평문과 도청한 암호문을 가지고 키를 찾아내는 것으로, 암호해독자는 암호문과 평문을 대칭시켜봄으로써 비교적 쉽게 키를 찾아낼 수 있다.

3) chosen plaintext attack

암호해독자가 임의로 선택한 평문을 암호알고리즘에 삽입하여 암호문을 얻은 다음, 이로부터 키를 찾는 공격방법으로서, 암호해독자들이 가장 즐겨 쓰는 방법이다.

다. 암호강도

암호계가 얼마나 안전한가를 측정하는 암호강도에는 Shannon이 정의한 무조건안전(unconditional secure)과 계산적 안전(computational secure) 두 가지가 있다.

무조건 안전이란 암호해독자가 이용할 수 있는 연산능력은 무한하다고 할지라도 그가 암호해독에 이용할 수 있는 정보의 양이 불충분하여 암호해독이 불가능할 경우의 암호강도를 지칭한다. Shannon은 자신이 정리한 정보이론에서 무조건 안전한 암호계를 「유일해를 얻기 위해 요구되는 텍스트의 최소길이인 unicity distance가 무한한 이상적인 랜덤키를 이용하는 암호계」라 정의하고 있다. 즉 이 암호계에서의 랜덤키 길이는 최소한 메시지 길이보다 더 커야함을 의미하는 것으로, one-time tape을 일례로 들 수 있다.

계산적 안전이란 암호해독자가 이용할 수 있는 정보의 양이 충분하여 언젠가는 암호를 풀 수는 있으나, 그 해독과정이 복잡하고 시간과 경비가 많이 요구되어 경제적으로 불합리한 경우의 암호강도를 일컫는 것으로, 현대 대부분 암호알고리즘이 여기에 속한다. 따라서 이러한 암호계의 암호강도는 그 알고리즘의 계산적 복잡도에 의해 결정되며, 이 복잡도는 complexity theory에 그 기반을 두고 있다.

라. 암호계의 분류

암호계는 암호방법과 그 형태에 따라 그림 2에서와 같이 구분할 수 있다.

먼저, 암호와 방법에 따른 분류를 살펴보면, 앞의 용어의 정의에서 설명하였듯이, 코드북과 같은 코드표에 의해 암호화하는 코드시스템과 일정 알고리즘에 의해 암호화하는 암호시스템으로 대별할 수 있으며, 이 가운데 암호알고리즘은 관용암호방식과 공개키암호방식으로 나눌 수 있다.

여기서 관용암호방식은 암호화키와 복호화키가 동일한 암호방식으로 대표적인 알고리즘으로는 DES(Data Encryption Standard)를 들 수 있다. 또 공개키 암호방식은 관용암호방식에서 문제가 되고 있는 키전송이 필요없을 뿐만 아니라 디지탈 서명이 가능한 암호방식으로서, RSA 암호계, Knapsack 암호계 등으로 대표된다.

또한, 데이터를 어떤 형태로 암호화시킬 것인가에 따라 크게 스트림암호와 블럭암호로 나뉜다. 스트림암호는 문자단위 혹은 비트단위로 암호화하는 방식으로, Vegenere암호와 Vernam암호가 여기에 속한다. 블럭암호는 평문을 일정 길이의 블럭으로 잘라 이를 암호알고리즘에 따라 암호화하는 방식으로, 일례로 DES의 운용모드 가운데 ECB(Electronic Code Book), CBC(Cipher Block Chaining) 등을 들 수 있다.

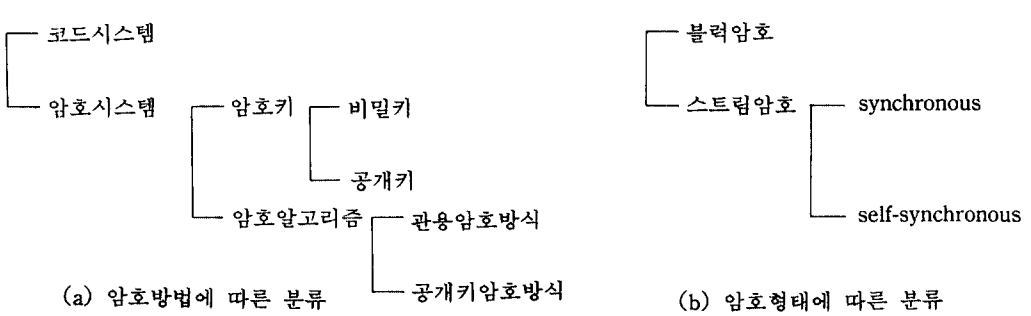


그림 2. 암호계의 분류

3. 기본 암호알고리즘

암호알고리즘은 암호화에 수행되는 기본요소에 따라 환자(substitution)암호, 전치(transposition) 암호, 혼합암호(product cipher), 지수암호 및 Knapsack암호방식으로 분류될 수 있다. 본 절에서는 이들 각 암호알고리즘의 기본적인 개념과 특징을 설명한다.

가. 환자 암호(Substitution Cipher)

환자암호는 평문의 각 문자를 다른 문자나 심볼로 일대 일 대응시킴으로써, 평문의 문자가 어떠한 암호문자로 변환되는지를 알 수 없도록 하는 혼동에 그 목적이 있다.

가장 기본적인 환자암호방식은 평문의 각 문자를 영문의 알파벳순으로 정렬한 다음 일정한 거리만큼 앞 또는 뒤의 문자로 대치시키는 방법이다. 즉, 다음 (식 1)과 같은 알고리즘으로 암호화가 수행되는데, 일예로서 시저암호(Caesar Cipher)에서는 이 키 값을 3으로 하고 있다.

$$C_i = E(P_i) = P_i + k \quad \cdots\cdots\cdots\cdots \text{(식 1)}$$

(여기서 C_i는 암호문, P_i는 평문, k는 키를 나타내며, $E(P_i)$는 암호화 알고리즘을 의미한다.)

그러나 이 방법은 문자의 출현빈도가 암호문에도 그대로 나타나기 때문에, 평문의 통계적 성질을 이용한 암호해독을 가능케 하는 단점이 있다. 따라서 이러한 단점을 보완한 환자암호기법으로서 Polyalphabetic 환자암호와, Homophonic 환자암호 등이 있다.

Polyalphabetic 환자암호는 출현빈도가 높은 문자와 낮은 문자의 출현빈도를 조합해서 좀더 균일한 출현빈도를 만들어 암호화하는 방법이다. 예를 들어 출현빈도가 높은 T가 어떤 때는 a 또 어떤 때는 b로 암호화되고 출현빈도가 낮은 X도 a 혹은 b로 암호화하면 균일한 출현빈도를 얻을 수 있게 된다. 대표적인 암호방법으로는 Vigenere암호가 있다.

Polyalphabetic 환자암호는 평문의 통계적 성질을 어느 정도 분산시킬 수는 있지만, 키의 길이를 공격하는 방법에 의해 해독할 수 있게 된다. 이 암호방법에 대한 공격은 사용된 순열의 갯수, 즉 키의 길이를 알아내는데서 부터 시작한다. 키의 길이를 알아낸 다음, 암호문을 키길이의 여러개의 블럭으로 순서대로 나누면 각각의 블럭은 키와 같은 길이를 갖게 된다. 각각의 블럭은 같은 키를 이용해서 암호화가 되었으므로 쉽게 평문을 찾아낼 수 있게 된다.

또한 Homophonic 환자암호는 한 평문의 문자에 대해 그 문자의 빈도수에 비례하는 갯수의 암호문 집합(이를 Homophones라 한다)을 할당하고 그 가운데 하나를 랜덤하게 선택하여 평문 메시지를 암호문 메시지로 변환하는 것이다. 일례로 미국의 암호해독자인 Thomas Jefferson Beale이 고안한 Beale암호가 있다.

이외에도 앞서 설명한 방식들과 달리 평문을 한 문자씩 아닌 보다 큰 문자 블럭단위로 암호화함으로써 해독을 어렵게 하는 Polygram 환자방식이 있다. 이 방식으로 대표적인 것으로는 영국과학자인 Lyon Playfair의 이름을 따서 만든 Playfair 암호와 Hill 암호가 있다.

그러나 이상의 환자암호방식은 단지 평문에 대한 통계적 성질을 분석하는데 드는 노력의 정도만이 차이가 있을 뿐으로, 환자암호 자체가 갖는 통계적 공격에 대한 허점(weakness)을 완전하게 방어할 수는 없다.

따라서 이러한 단점을 해결하기 위해서는 평문의 통계적 성질이 암호문에 나타나지 않도록 하는 방법을 고려해야 한다. 그러한 하나의 해결방법으로서, 환자암호에 사용하는 키의 길이를 무한히 길게 함으로써, 동일한 평문의 각 문자에 대해서도 항상 다른 암호문을 얻도록 하는 방법을 생각할 수 있다.

완전(perfect) 환자암호 방식이 이에 해당하는 것으로서, 이 방식은 암호키의 길이를 무한대로 길게 함으로써, 어떠한 암호공격도 불가능하게 하는 무조건 안전한 암호방식이다. 반복되지 않는 키 집합을 이용해서 암호화하는 방법인 One-Time Pads가 그 일예이다. 그러나 이 방식은 현실적으로 무한대에 달하는 암호키열을 생성 및 관리하거나

분배하는 문제를 안고 있어, 실용 가능성은 거의 없다.

AT&T의 Gilbert Vernam에 의해 고안된 Vernam 암호는 One-Time Pads 암호방식의 일종으로서, 기본 알고리즘은 반복되지 않는 숫자열을 사용해서 평문을 암호화하는 것이다. 천공카드 테이프를 이용해서 반복되지 않는 랜덤한 숫자열을 얻어내고 각 테이프는 오직 한번만 사용된다. 키테이프가 반복되지 않거나 다시 사용되지 않는 이상 반복되는 문자열은 같은 키를 이용해서 암호화되지 않기 때문에 이 종류의 암호는 어떤 공격에 대해서도 안전하다. 그러나 이 방법 역시 실용성이 크게 결여되는 것으로, 가능한한 보다 긴 키열을 만들기 위해 몇개의 랜덤발생기를 조합함으로써 Vernam 암호를 구현한 pseudo Vernam 암호가 오늘날 많이 사용되고 있다.

나. 전치암호(Transposition Cipher)

앞절에서 살펴 보았듯이 환자암호의 목적은 혼동, 즉 평문과 키가 어떻게 암호문으로 바뀔지 알 수 없도록 하는 것이다. 반면에 전치암호는 평문의 문자를 다시 재배열하는 암호방식이다. 따라서 전치암호의 목적은 확산, 즉 평문과 키가 가지고 있는 정보를 암호문 전체에 분산시키는 데 있다. 영문에서 어떤 구나 단어의 형태를 바꾸고 암호해독자가 암호를 해독하기 위해서 더 많은 암호문을 필요로 하게 만드는 것이 확산의 목적이다.

전치암호는 크게 Columnar transposition과 Double transposition으로 나눌 수 있다.

Columnar transposition은 평문을 열을 통해서 다시 재배열하여 암호화하는 방법이다. 예를 들어 평문이 $C=C_1C_2C_3\cdots C_n$일 때 5-열 전치암호를 한다면 다음과 같다.

$C_1\ C_2\ C_3\ C_4\ C_5$
$C_6\ C_7\ C_8\ C_9\ C_{10}$
$C_{11}\ C_{12}$ etc.

따라서 암호문은 $C_1C_6C_{11}\cdots C_2C_7C_{12}\cdots$이 된다. 평문의 길이가 행의 길이의 배수가 아닐 때 출현빈도가 적은 문자로 채워 암호화한다. 이 알고리즘은 평문 하나의 문자당 다른 특별한 연산을 행하지 않으므로 연산시간은 평문의 길이에 비례한다. 하지만 다른 알고리즘과는 달리 평문을 저장할 기억장소를 필요로 한다. 또 모든 평문을 다 읽어들인 다음에야 출력이 나올 수 있으므로 지연이 발생하고 이 지연시간은 평문의 길이에 비례한다.

Double transposition은 다른 열의 수를 가진 두 Columnar transposition을 이용해서 암호화하는 방법이다. 일단 전치암호에 의해 나온 결과를 다시 암호화하는 방법이다.

전치암호에 대한 공격방법은 환자암호에서 처럼 명확하지는 못하지만 암호문이 평문의 문자를 그대로 갖고 있기 때문에 환자암호보다 강한 암호강도를 갖지는 못한다. 우선 문자의 출현빈도를 계산해서 그 출현빈도가 일반 평문에서의 출현빈도와 같다면 그 암호문은 전치암호를 통해 암호화된 암호문임을 알 수 있다.

다. 혼합암호(Product Cipher)

암호화 및 복호화 과정을 보다 빠르고 실수없이 수행하기 위한 암호장비에 대한 필요성이 증가됨에 따라서 세계 제 2 차대전을 기점으로 많은 암호와 장비가 등장하기에 이르렀다. 암호화 장비로서는 폴리알파벳 환자암호를 적용키 위해 개발된 Jefferson Cylinder와 Wheatstone disk가 있으며 ENIGMA와 같은 Rotor 머신이 있다. 또 인쇄가능한 암호장비로서는 Boris Hagelin의 M-209머신과 수신자가 복호할 때 평문을 인쇄해주는 Siemens와 Halste의 T-52머신 등이 있다.

또한 근대에 들어와서는 메모리와 시프트 레지스터를 이용한 현대적 암호장비들이 등장하였으며 특히 IBM의 Lucifer 암호로 대표되는 환자와 전치기법을 함께 적용시킨 혼합 변환기법이 제안됨으로써 현대 암호연구에 크게 기여하였다.

혼합암호의 대표적인 기법으로는 IBM의 Lucifer암호와 이를 기반으로 개발된 DES를 들 수 있다.

IBM의 Lucifer 암호는 1970년 IBM의 Feister에 의해 개발된 것으로 환자와 전치기법을 조합시킨

것이다. 이것은 후에 대표적 관용암호계인 DES에 직접적인 영향을 미쳤다.

한편, DES는 현재까지 가장 널리 실용화되어 있는 암호기법중 하나로서, 여기에서는 이 기법을 중점으로 살펴본다. 과거의 데이터 통신은 사설 네트워크와 전용선을 사용하여 하나의 조직안에서만 이루어져 왔기 때문에 암호화 표준의 필요성이 없었다. 따라서 각 조직마다 서로 다른 암호장비를 가지고 있었고 다른 프로토콜을 사용하였다. 그러나 통신기술의 발달로 모든 네트워크나 컴퓨터가 연결됨에 따라 서로 직접적인 통신을 위해 프로토콜과 암호의 표준이 필요하게 되었다.

이에 1977년 미국 표준국인 NBS에서는 미국 정부의 표준 암호방식으로서 IBM이 제안한 알고리즘을 DES라는 이름으로 발표하였다. 이는 64비트의 데이터블럭을 56비트의 키를 이용하여 순열, 환자, 모듈러 2 등의 기본 알고리즘을 조합함으로써 암호화와 복호화를 수행하는 것으로 그 절차를 그림 3에 보였다.

그림에서 보듯이 IP는 입력된 64비트의 평문 블럭에 전치를 행하여 입력데이터와 키를 직렬로 로드되게 함으로써 알고리즘이 좀더 쉽게 단일 칩에

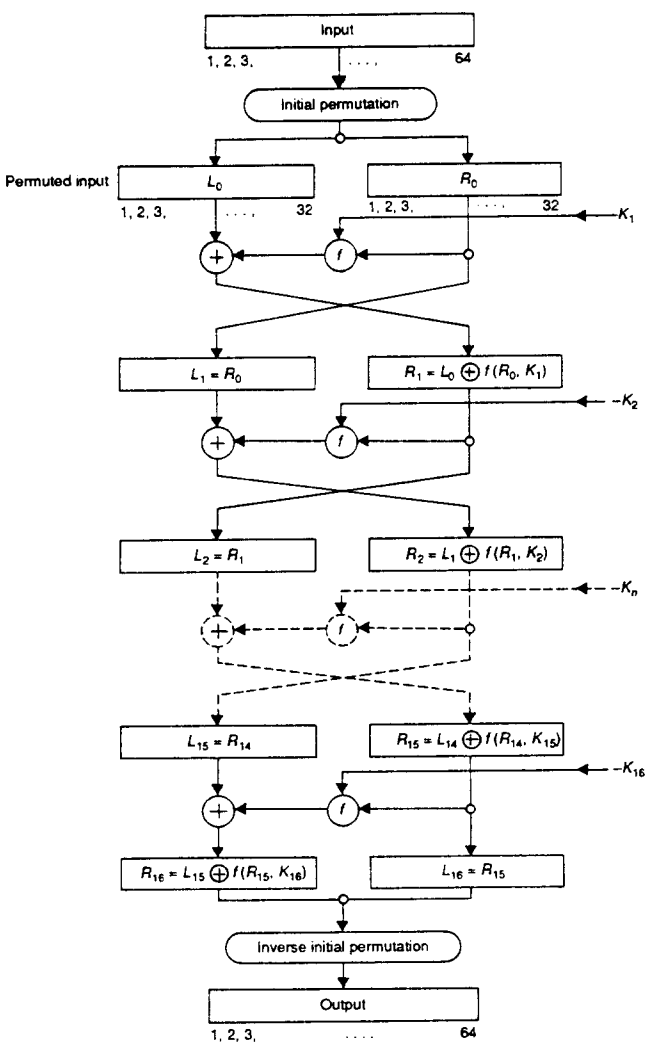


그림 3. DES 알고리즘의 개요

구현되게 하고, L_0와 R_0는 64비트의 평문을 32비트씩 양분한 것이고, 함수 f는 DES에서 가장 중요한 부분인 비트확장과정, mod 2 연산과정, 대체과정 및 전치과정으로 구분되었다.

외부에서 공급되는 키는 64비트로 구성되었으며, 그중 56비트는 알고리즘에 사용되고 나머지 8비트는 패리티비트로 사용한다. 56비트는 매 단계마다 간단한 시프트와 비트선택을 행하여 48비트씩 다르게 함으로써 암호강도를 향상시킨다. 그림 4는 DES 암호화에 사용되는 키 일람표 계산을 나타낸 것이다.

한편, DES는 구현시에, 보다 암호화 강도를 높이기 위해 4가지 운용모드를 채용하고 있다. DES의 기본 알고리즘을 평문의 매 64비트 블럭마다 동일키로서 그대로 적용하는 ECB(Electronic Codebook)모드와, 암호문 블럭을 피드백하여 다음 평문블럭과 모듈러연산을 취한 다음 기본 알고리즘을 수행하는 CBC(Cipher Block Chaining), 또한 CBC를 스트림모드로 변환한 CFB(Cipher Feedback)모드, 그리고 CFB와 달리 키를 피드백하여 스트림암호를 수행하는 OFB(Output Feedback)가 그것이다.

DES 알고리즘은 암호해독자에 의해 이미 그 알고리즘 자체가 분석되어 미국의 NBS의 후신인 NIST에서는 이를 표준 권고안에서 제외시키고 있으나, 그 실용성 때문에 최근까지 널리 사용되고 있다.

라. 지수암호

1976년 Diffie와 Hellman이 "New Direction in Cryptography"라는 초청논문에서 기존 관용암호계의 키분배 문제를 해결하고 디지탈 서명이 가능한

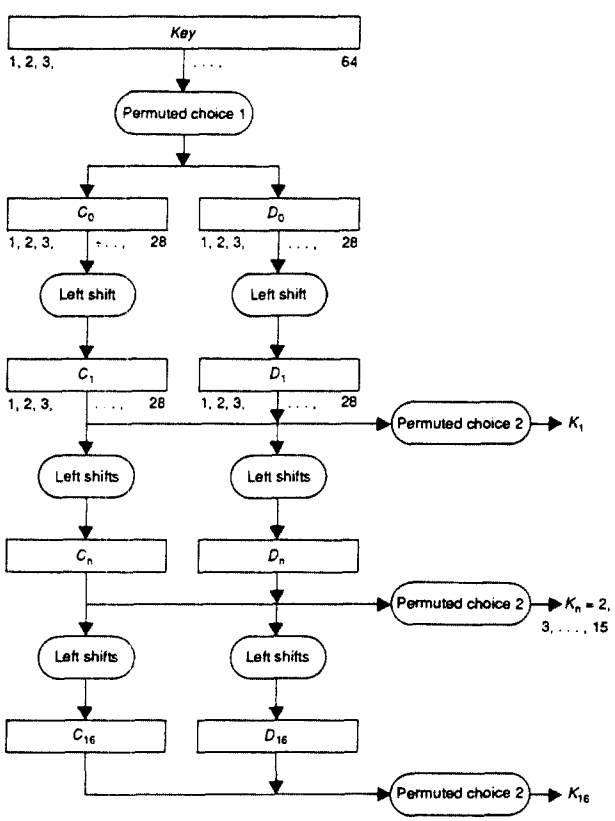


그림 4. DES에 사용되는 키 일람표 계산

새로운 암호방식인 공개키 암호방식을 제안한 이래, 이에 대한 연구가 활발히 이루어져 왔다.

그 가운데 1978년에 발표된 유한체상에서의 지수연산에 의한 암호기법인 Pohlig Hellman 방식과 Rivest, Shamir, Adleman이 발표한 RSA 방식에 대해 알아본다.

1) Pohlig Hellman방식

대부분의 공개키 암호방식에서와 마찬가지로, 이 방식은 먼저 큰 소수 p로 부터 $\phi(p)=p-1$인 오일러 함수와 p와 가장 가까운 소수인 d를 구하고, 다시 number theory에서 소개되는 페르마정리와 유클리드알고리즘을 이용하여 $e=inv(d, \phi(p))$를 구한 다음, 이 p, d, e를 이용해 다음 함수로 암호화를 수행한다.

암호화 : $C=M^e \bmod p$

복호화 : $M=C^d \bmod p$

이 방식의 암호강도는 유한체 GF(p)상에서의 이산대수연산의 난도(complexity)에 의존한다.

2) RSA 방식

두개의 큰 소수인 p, q에 대하여 그 곱인 $n=p*q$를 구하는 것은 간단하지만 이 n을 소인수분해하여 p, q를 구하는 것은 매우 어려운 계산을 요한다.

RSA는 바로 이러한 소인수분해의 난도를 이용한 암호방식으로, 디지탈서명이 가능하고 계산적 안전도가 높으며 키관리가 용이하다는 장점이 있다.

이 기법의 기본 알고리즘은 다음과 같다.

*. 매우 큰 소수 p, q 발생

*. p, q로부터 $n=p*q$와 $\phi(n)=(p-1)(q-1)$을 구한다.

*. $(d, \phi(n))$의 최대공약수가 1인 d를 선정

*. $d*e\equiv 1 \pmod{\phi(n)}$을 만족하는 e를 구한다.

*. 여기서 공개키는 e, 비밀키는 d가 된다.

*. 암호화 과정 : $C=M^e \pmod n$

복호화 과정 : $M=C^d \pmod n$

마. Knapsack 암호계

공개키 암호방식의 또 다른 흐름에는 NP-complete Knapsack 문제에 기반한 Trapdoor Knapsack 암호방식이 있다. 대표적인 것으로는 Mercle과 Hellman이 1978년에 제안한 MH Knapsack 방식과 이를 응용한 Graham-Shamir Knapsack과 Shamir Signature-only Knapsack이 있다. 여기서는 MH 방식에 대해 알아본다.

1) MH-Knapsack

A를 n개의 정수로 구성된 공개백터, M을 n개의 2진 디지트로 구성된 평문벡터라 할 때, 암호문 $C=A*M=\Sigma a_i*m_i$가 된다. 여기서 Knapsack 문제란 A와 C가 주어졌을 때 이로부터 M을 구하는 것을 말하며, 만일 A가 100개 이상의 큰 정수를 사용한다면 이 Knapsack문제는 계산상으로 풀기 어려운 NP(Nondeterministic Polynomial)문제가 된다.

따라서, Trapdoor Knapsack 암호방식이란 적절한 A를 선택함으로써, 비밀 trapdoor를 모르면 M을 구할 수 없게 한 암호방식으로서 그 기본 알고리즘은 다음과 같다.

*. 큰 비밀 정수 r과 t를 선택

*. 이 정수들로 부터 $s*t\equiv 1 \pmod r$인 비밀정수 s를 계산

*. $a_i' > a_1'+a_2'+\cdots+a_{i-1}'$인 superincreasing order에 의한 비밀벡터 A'를 생성

*. A'를 공개벡터 A로 변환 : $a_i \equiv a_i'*t \pmod r$

*. 암호화 : $C\equiv A*M\equiv \Sigma a_i'*m_i*t \pmod r$
(여기서 m_i란 평문 요소를 가르킨다)
복호화 : $C'\equiv C*s \pmod r$, $M\equiv C'*t \pmod r$

4. 암호계의 구현기술

암호계를 실제 시스템상에서 구현코자 할 때에는 신뢰성(reliability), 유용성(usability), 안전성(security) 등을 위해 암호알고리즘 뿐만 아니라 하드웨어적 구현, 패키징, 테스팅, 유지보수 등도 함께 고려되어야 한다. 또한 키 분배문제를 비롯하여

에러정정과 같은 다른 기능과의 통합도 암호계의 구현에 있어서 큰 비중을 차지하고 있다.

또한 정보통신망의 보급확대와 함께, 네트워크상에 있어서의 정보보호를 위한 관심이 크게 고조되고 있다. 따라서 최근에는 네트워크상에서의 데이터 안전성을 구현하기 위한 연구도 활발히 이루어지고 있다.

여기에서는 앞에서 설명한 여러 암호알고리즘을 이용, 실제 시스템상에서 구현하는 운용모드방식인 블럭암호와 스트림암호에 대해 살펴보고, 네트워크상에서의 적절한 암호계의 적용위치 및 키 분배 문제를 비롯한 암호화 프로토콜에 대해서 설명한다.

가. 스트림암호와 블럭암호

스트림암호는 평문의 각 심볼을 바로 암호문의 한 심볼로 바꾸는 암호이다. 즉 메시지 M을 연속된 문자나 비트단위로 나누어 각 메시지 요소 m_i를 키열 $K=k_1k_2\cdots$의 각 키요소로 각각 암호화하는 방식으로서 키열이 Rotor나 Hagelin머신과 같이 어떤 주기를 갖고 반복되는 방식을 주기적(periodic) 스트림암호, Vernam이나 Running Key 암호와 같이 키가 One-Time Pad인 방식을 비주기(nonperiodic) 스트림암호라 한다.

또한, 스트림암호는 키열과 평문열의 관계에 따라 동기식(synchronous)과 자기동기식(self-synchronous)으로 나눌 수 있다.

동기식 스트림암호는 키열이 평문열과는 독립적으로 생성되는 것으로서 이것은 암호문의 문자가 전송중에 손실될 때 송수신자가 다시 키발생기를 재동기시킨 후에 비밀통신을 해야 함을 의미한다. 대표적인 기법으로는 Linear Feedback Shift Register, DES의 OFB모드, Vernam 암호 등이 있다.

자기동기식 스트림암호는 각 키 문자가 앞의 n개 암호문자로부터 생성되는 방식으로서 전송중에 암호문자가 손실되거나 변경되더라도 그 이후 n개 문자에 대해서만 에러가 전파된 다음에 다시 올바른 암호문을 받을 수 있는 자기 스스로 재동기 기능을 갖는 암호방식이다. 여기에는 자동키 암호(autokey cipher)와 DES의 CFB모드 등이 있다.

스트림암호의 장점은 첫번째로 변환속도가 빠르다는 것이다. 각 심볼들은 평문의 다른 심볼에 영향을 받지 않고 즉시 암호화되므로 암호알고리즘 자체의 수행속도에 대한 영향만을 받는다. 또한 에러의 전파가 적다. 각 심볼단위로 암호화되므로 암호화과정에서 발생한 에러는 한 심볼에만 영향을 미치게 된다.

반면 스트림암호의 단점으로는 첫째 적은 확산효과를 갖는 점을 들 수 있다. 각 심볼은 독립적으로 암호화되기 때문에 각 심볼이 갖고 있는 정보는 암호문중 하나의 심볼에 모두 포함된다. 따라서 암호해독자는 각각의 심볼에 대해서 공격을 할 수 있게 된다. 두번째로 능동적인 공격에 대처하기가 어렵다. 즉 어떤 심볼의 삽입이나 변경에 대처하기가 어렵게 된다.

한편 블럭암호는 스트림암호와는 달리 평문 심볼의 집단을 하나의 블럭으로 보고 이 블럭을 기본단위로서 암호화하는 방법이다. 블럭암호(block cipher)는 메시지 M을 연속적으로 나누어 같은 키 K로 암호화하는 방식으로서 DES, RSA, Knapsack 등의 현대적 암호방법 등이 블럭암호의 대표적 방법이다.

블럭암호의 장점은 첫째로 평문의 정보가 암호문의 여러 심볼에 분산되므로 확산효과가 우수하다는 것이다. 두번째로 블럭의 길이가 정해져 있기 때문에 심볼의 삽입이나 제거가 불가능하다. 만약 공격자가 하나의 심볼을 삽입했다고 하면 수신자는 길이가 다른 블럭을 얻게 되어 이상이 생겼음을 알게 된다. 반면에 블럭단위로 암호화가 이루어지므로 평문이 완전히 하나의 블럭을 구성한 다음에 비로소 암호화가 이루어지므로 암호과정이 블럭의 크기에 따라 지연된다. 실시간을 요구하는 응용에서는 이것이 가장 큰 단점이다. 또한 암호화과정에 있어서 에러는 여러 변환에 영향을 미치므로 에러의 전파가 크다는 단점도 있다.

나. 암호의 적용위치

데이터가 채널을 통해 전송될 때 근원지와 목적지

노드사이에 여러 중간노드를 거치게 되는데, 이 때 암호화의 적용위치에 따라 중간 노드마다 암호화와 복화를 행하는 링크암호(link by link encryption)와, 근원지와 목적지 노드에서만 암호화와 복호화는 단말간 암호(end-to-end encryption)로 나눌 수 있다.

1) 링크암호

이 암호는 그림 5에서 보듯이 각 중간노드에서 암호화와 복호화가 수행되는 것으로, 각 노드사이의 링크에서 데이터가 암호화된다. 이러한 접근방식은 각 링크내의 데이터가 헤더를 포함하여 모두 암호화되어 있으므로 공격자에 의한 트래픽분석을 막을 수는 있으나, 각 중간 노드마다 암호장비를 설치해야 할 뿐만 아니라 노드내에서는 데이터가 평문의 상태로 있게 되므로 이를 보호하기 위한 별도의 노드보호 경비가 요구되는 등 많은 단점이 있다.

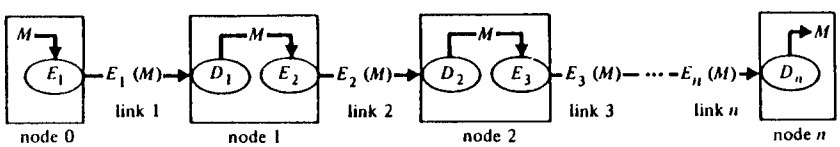


그림 5. 링크암호의 구성

2) 단말간 암호

이 암호는 그림 6에서와 같이 근원지와 목적지 노드에서만 암호를 적용시킨 것으로, 헤더를 제외한 데이터(PDU : Protocol Data Unit) 만을 보호한다. 링크암호와는 달리 이 방식은 메시지가 어디로 전송되는지, 또 얼마나 많은 양의 데이터가 어느 시간대에 주로 전송되는지와 같은 트래픽 분석을 완전히 막을 수는 없지만, 트랜스포트계층 등에서 적절한 조치를 취함으로써 어느 정도 이를 제어할 수 있으며, 또 각 노드에 대한 보호와 노드내의 암호화장비가 불필요하므로 상당히 경제적이며, 주로 패킷교환망이나 패킷방송망 등에 많이 채용되고 있다.

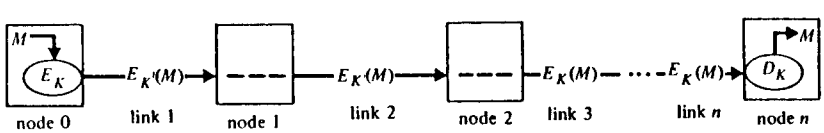


그림 6. 단말간 암호

다. 암호화 프로트콜

정보보호의 가장 큰 과제로는 정보의 안전성(secrecy)과 정보와 사용자에 대한 신뢰성(authenticity)을 들 수 있다. 따라서 2자 이상간의 안전한 통신을 수행하기 위해서는 암호화 알고리즘을 이용, 이들 secrecy와 authenticity를 해결해야 한다.

이와 같이 2자 이상간에 있어서 정보의 secrecy와 정보와 사용자에 대한 authenticity를 만족하는 안전한 통신절차를 암호화 프로토콜이라 한다.

1978년 Rivest, Shamir, Adleman에 의해 사용자 인증이 가능한 공개키 암호방식인 RSA 암호화 알고리즘이 발표된 이래, 더욱 활기를 띠게 된 암호화 프로토콜에 관한 연구는 크게 다음 6가지 분야로 나눌 수 있다.

* digital signature
* random selection(poker protocol)
* voting
* transfer without knowledge(oblivious transfer)
* contract signing
* delivery with assurance of receipt

이들 각 프로토콜에 있어서 암호화 알고리즘과 암호화 테크닉이 정보의 secrecy, privacy, authenticity 등과 같은 암호화 요구사항을 만족시키기 위해 적용되고 있다.

특히, 2자 이상간의 정보통신에 있어서 통신 상대방의 정당성을 확인하기 위한 디지탈 서명(Digital Signature)은 암호화 프로토콜의 대표적 예로서 DES와 같은 관용키 암호계나 RSA 방식으로 대표되는 공개키 암호계를 그 프로토콜의 구현 메카니즘으로 채용한 구체적인 디지탈 서명 방식들이 다수 제안되어 있다.

또한 임의 정보를 서로 신뢰할 수 없는 2자 이상간에 공정하게 분배하기 위한 「Mental Poker」 프로토콜도 그 응용 중 하나인 키분배 프로토콜을 중심으로 심도있게 연구되고 있다.

최근 정보화 사회의 진전에 따라 컴퓨터 통신망을 통한 정보교환의 형태와 종류가 날로 다양해지고 복잡해가는 것과 발맞추어, 정보통신에 있어서 송수신자 부인봉쇄라든가 수신확인 등의 정보보호에 대한 요구도 늘어나고 있는 실정이다. 이에 따라 이러한 정보보호에 대한 요구를 만족시키기 위한 "Voting", "Oblivious transfer", "Contract signing", "Certified Mail" 등의 암호화 프로토콜에 대한 연구도 최근들어 활발히 진행되고 있다.

한편 이들 암호화 프로토콜들을 기존 구축되어 있는 네트워크로 이식하기 위한 연구도 일부 진행중이다. 특히 실용화기를 맞고 있는 개방형통신망(OSI)에 있어서 정보보호를 위한 프로토콜 설계 연구로는 미국 NSA에 의해서 개발된 네트워크와 트랜스포트 계층에서의 시큐리티 프로토콜인 SP3와 SP4를 비롯하여 응용계층에서의 여러 시큐리티 프로토콜이 제안된 바 있다. 이외에도 응용계층내의 한 부계층으로서 시큐리티 서비스를 제공하기 위한 시큐리티 모델 연구도 진행중에 있다.

라. 키의 관리

암호통신시스템을 운용하는데 있어서 송수신자간의 키배송문제는 매우 중요한 과제로서, 특히 네트워크가 대규모화되고 또 장애나 신규가입자에 의한 빈번한 변동이 수반되고 있는 정보화사회에 있어서 키의 분배 및 관리는 커다란 문제로 부각되고 있다. 일례로 종래 관용암호계에서는 네트워크에 가입되어 있는 n명의 이용자 모두각 각 일대일로 다른 가입자와의 공유 비밀키를 가져야 하므로 총 $n(n-1)/2$개의 비밀키쌍이 유지되어야만 하였다.

따라서 정보화사회를 대비하여 대규모 네트워크에서의 키분배 및 관리에 대한 연구가 활발히 진행되어 왔다.

먼저, 관용암호계에서의 키관리를 해결하기 위한 하나의 제안으로서 IBM이 SNA에 적용시키고 있는 키배송센터(KDC : Key Distribution Center)를 들 수 있다. 이는 각 가입자가 키를 소유하지 않고 KDC가 모든 키를 저장하고 있다가 가입자의 요구가 있을 때에 키를 분배하는 방식이다.

그러나 KDC에 의한 관리기법도 키배송을 위한 과중한 통신 오버헤드가 걸리는 등 관용암호계가 갖는 문제를 완전히 해결하기는 어려웠으므로, 관용암호계의 $n(n-1)/2$개의 키쌍을 n개로 줄여보자는 제안이 바로 공개키 암호계이다. 이 방식은 전화번호부와 같은 공개키화일에 각 가입자의 공개키를 등록해 두고 서로 통신하는 암호방식으로, 각 가입자는 독자적인 비밀키를 갖으므로 이를 사용하여 디지탈 서명을 할 수 있어 통신상대의 합법성여부를 확인할 수 있다는 특징이 있다.

하지만 공개키 방식에 의한 공개키화일도 네트워크가 크게 확장될 수록 이의 관리가 상당한 문

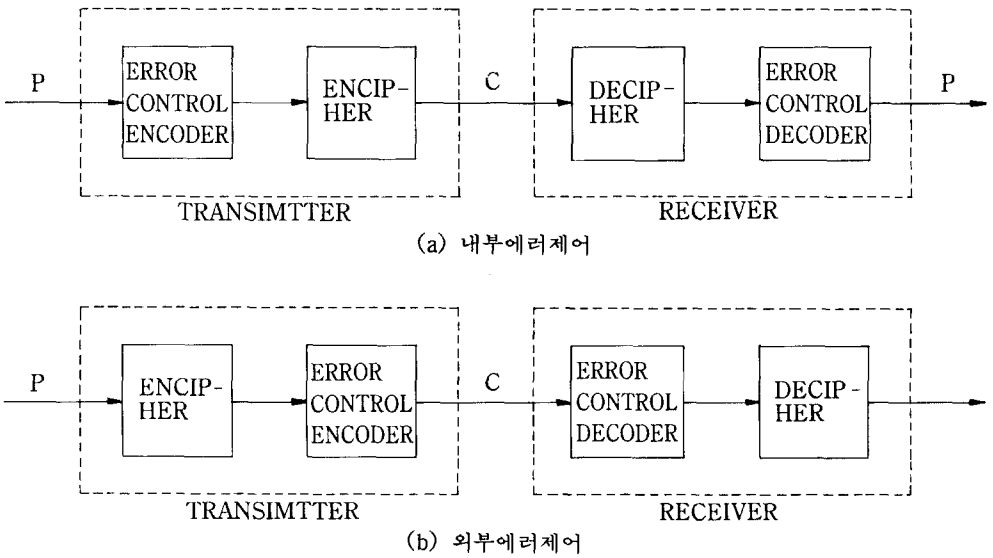


그림 7. 암호와 에러제어코딩과의 관계

제를 일으키게 되므로, 이 공개키화일을 없애자는 방향에서의 키관리방식이 연구되고 있다.

그 큰 흐름중 하나가 Kohnfelder가 제안한 공개키증명서(PKC : Public Key Certificate)방식으로서, 이는 각 가입자가 자신의 공개키를 갖고 있다가 암호통신을 할 때에 자신의 ID와 공개키로 디지탈 서명을 하여 자신의 공개키를 보증할 수 있는 보증서를 함께 보내자는 키분배방식이다.

또한 공개키화일을 없애자는 방향에서의 암호연구에 커다란 영향을 미친 것은 Shamir의 ID 자체를 공개키로서 사용하자는 방식으로서, 이 ID에 기반한 키분배방식은 Shamir이래 전세계적으로 연구가 활발히 진행되고 있으며, 네트워크상에서의 구현예도 나와 있다.

한편, 또다른 키관리방식에 대한 연구로는 Blom이 제안한 KPS(Key Predistribution System)가 있다. 이는 먼저 네트워크관리센터가 각 가입자에게 IC카드 등의 형태로 미리 각자의 비밀알고리즘을 배포하고, 각 가입자가 비밀통신을 하고자 할 때에는 이 알고리즘에 상대의 ID를 입력하면 상대와의 공통 비밀키가 생성되는 것으로, 다른 방식과는 달리 키분배를 위한 사전통신이 전혀 필요없다는 장점이 있다.

마. 에러제어

암호계를 네트워크상에 구현코자 할 때, 통신로상에서 발생하는 에러를 제어하기 위한 채널코딩과 함께 자주 사용되는데, 이때 암호와 에러제어코딩 중 어떤 것을 먼저 수행하는가에 따라 그 결과가 달라진다.

먼저 그림 7(a)에서와 같이 에러제어코딩을 내부에서 수행하면 블럭암호의 경우 자동인증(automatic authentication)이 가능케 되는 장점이 있다. 또 블럭암호와 self-synchronous 스트림암호는 복호시에 에러가 확산되는 성질이 있으므로 그림 13(a)에서와 같이 암호알고리즘에 앞서 에러검출코딩을 하는 것이 바람직하다. 반면 synchronous 스트림 암호는 에러확산 성질이 없으므로 고정된 선형에러제어코드를 사용하게 되면 공격자가 쉽게 이

에러제어비트까지도 계산된 비트로 조작할 수 있으므로, 비선형 및 keyed 에러검출코드를 사용하여야 한다.

한편 에러정정코드는 그림 7(b)에서와 같이 외부에 적용시키는 것이 바람직하다. 왜냐하면 내부에 적용시킬 경우, 보호시의 에러확산때문에 정정해야 할 에러코드가 너무 많아지기 때문이다.

한편 최근에는 에러제어알고리즘을 암호알고리즘과 통합하여 데이터의 안전성과 신뢰성을 동시에 제공하는 에러제어 및 암호의 결합알고리즘도 활발히 연구되고 있다.

5. 암호학의 향후 전개방향

미래 정보화사회에 있어서 컴퓨터 네트워크는 점차 확장되어갈 것이며, 유통되는 정보량 또한 엄청나게 증가하리라는 것은 이미 널리 주지되어 있는 바와 같다. 따라서 이러한 환경하에서 정보의 프라이버시와 인증은 지금까지보다 더 훨씬 중요한 과제로서 부각되고 있다는 사실은 의심할 여지가 없다. "정보화 사회와 시큐리티" 이는 불가분의 관계로서 함께 연구개발되어가야 할 것이다.

따라서 정보를 보호한다는 측면에서의 암호연구는 앞으로 보다 다채롭게 진행되어 다가오는 정보화사회에 있어서 보다 안전하며 보다 실용성있는 시큐리티기술이 종합적으로 강구되어야 할 것이다.

먼저, 암호학의 배경을 이루고 있는 유한체상에서의 연산, 특히 커다란 정수의 소인수분해 및 이산대수학 그리고 고속 소수판정법 등에 관한 연구가 암호강도와 속도개선을 위해 꾸준히 진행되고 있으며, 대규모 네트워크 지향의 암호방식과 영지식 증명에 의한 인증, 그리고 효율적 네트워크 응용을 위한 키분배 등의 암호화 프로토콜에 대한 연구도 향후 더욱 발전시켜 나가야 할 분야이다.

또한 리스크(risk) 관리나 시스템감사를 지원하는 이론과 기술을 비롯하여 컴퓨터바이러스에 대처하기 위한 컴퓨터면역학 등, 또 다른 방향에서의 연구도 보다 광범위한 종합적 시큐리티대책을 위한 중요한 과제이다.

참 고 문 헌

1. D. W. Davies, W. L. Price, "Security for Computer Network," John Wiley & Sons, 1984.

2. W. Diffie, M. E. Hellman, "Privacy and Authentication : An Introduction to Cryptography," Proc. IEEE, Vol. 67, No. 3, Mar. 1979.

3. W. Diffie, M. E. Hellman, "New Direction in Cryptography," IEEE Trans. Inform. Theory, Vol. IT-22, Nov. 1976.

4. Pohlig, S., M. E. Hellman, "An Improved Algorithm for Computing Logarithms over GF(P) and its Cryptographic Significance," IEEE Trans. on Info. Theo. Vol. IT-24(1), Jan. 1978.

5. R. L. Rivest, A. Shamir, L. Adleman, "A method for obtaining digital signatures and public key cryptosystems," Comm. ACM, Vol. 21 No. 2, Feb. 1978.

6. Denning, Dorothy, "Cryptography and data security," Addison Wesley Pub., 1982.

7. N. J. A. Sloane, "Error-Correcting Codes and Cryptography," The Mathmatical Gardner, Boston, 1981.

8. 정진욱, 우치수, "실시간 통신환경에 있어서 압축코딩과 암호코딩의 결합," 한국정보과학회 논문지, Vom. 17, No. 6, 11월 1990.

9. 정진욱, "압축과 암호코딩의 결합에 관한 연구," 서울대학교 박사학위논문, 1991. 2

10. C. P. Pfleeger, Security in Computing, Prentice Hall, 1989, pp. 3-73.

11. R. Berger, S. Kannan and R. Peralta, "A Framework for Study of Cryptographic Protocols," Advances in Cryptology — Proceedings of Crypto85, pp. 87-103.

□ 著者紹介

정 진 욱(正會員)

成均館大學校 電氣工學科 卒業(學士)
成均館大學校 大學院 電子工學科(碩士)
서울大學校 大學院 計算統計學科(博士)
韓國科學技術研究所 研究員/韓國科學技術院 시스템공학센터 데이타통신研究室長.
Racal Milgo Co. 研究員(미국 Florida 所在)
現在 成均館大學校 情報工學科 副教授