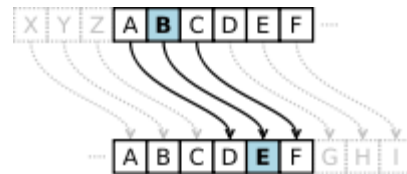


# 암호학

**암호학**(暗號學, 영어: cryptography, cryptology)은 정보를 보호하기 위한 언어학적 및 수학적 방법론을 다루는 학문으로 수학을 중심으로 컴퓨터, 통신 등 여러 학문 분야에서 공동으로 연구, 개발되고 있다. 초기의 암호는 메시지 보안에 초점이 맞추어져 군사 또는 외교적 목적으로 사용되었지만, 현재는 메시지 보안이외에도 인증, 서명 등을 암호의 범주에 포함시켜 우리의 일상에서 떼 놓을 수 없는 중요한 분야가 되었다. 현금지급기의 사용, 컴퓨터의 비밀번호, 전자상거래 등은 모두 현대적 의미의 암호에 의해 안정성을 보장받고 있다.



현대 암호학은 암호 시스템, 암호 분석, 인증 및 전자서명 등을 주요 분야로 포함한다.

## 용어 설명

암호학을 이용하여 보호해야 할 메시지를 **평문**(平文, plaintext)이라고 하며, 평문을 암호학적 방법으로 변환한 것을 **암호문**(暗號文, ciphertext)이라고 한다. 이때 평문을 암호문으로 변환하는 과정을 **암호화**(暗號化, encryption)라고 하며, 암호문을 다시 평문으로 변환하는 과정을 **복호화**(復號化, decryption)라고 한다.

암호학적 서비스가 제공하고자 하는 목표에는 다음과 같은 것이 있다.

- 기밀성** (機密性, Confidentiality): 부적절한 노출 방지. 허가받은 사용자가 아니면 내용에 접근할 수 없어야 함.
- 무결성** (無缺性, Integrity): 부적절한 변경 방지. 허가받은 사용자가 아니면 내용을 변경할 수 없어야 함.
- 가용성** (可用性, Availability): 부적절한 서비스 거부 방지.
- 부인봉쇄** (否認封鎖, Non-repudiation): 메시지를 전달하거나 전달받은 사람이 메시지를 전달하거나 전달받았다는 사실을 부인할 수 없어야 함.

## 암호학의 역사

암호학의 기원은 수천년 전부터 이뤄, 최근 수십 년까지의 기간을 일컫는다.역사상 기록으로 남은 가장 오래된 암호는 율리우스 카이사르가 사용한 대입암호이다. 고대 그리스에서 사용되던 스키테일 암호체계도 있다. 이 시기의 암호화 기법을 고전 암호학 이라 부르는데, 고전 암호학의 암호학 기법은 대체로 큰 차이가 없었다. 이런 고전 암호화 기법은 20세기 초에 이뤄서야 변화가 생겼는데, 이의 예로는 에니그마(독일어:Enigma 뜻:수수께끼)가 사용한 회전륜 가밀법이 대표적이다. 이후 전자요소와 계산기(컴퓨터)는 큰 발전을 이뤘으며, 이때 사용된 암호화 기법은 전통적인 사서통신에 쓰일 수 없게 되었다. 암호학의 발전은 암호분석학과 함께 발전했다. 즉 암호 편집과 가밀법에 대한 해독법을 말한다. 주로 가밀된 신호의 빈율을 분석하여 해석했는데, 이런 방법을 응용하여 해석된 암호문은때때로 역사를 바꾸기도 했다. 예를 들어, 치머만 전보를 해석한 것은 미국이 1차 세계대전에 참전하게 되는 계기가 되었고, 연합국

이 나치의 암호문을 해석한 것은 2차세계대전의 기간을 2년정도 단축시켜 주기도 하였다. 20세기부터 70년대 이전에 암호학의 대부분은 정부의 안전범주에 속했지만, 공개표준키 체제의 탄생과 공개키 가밀 법의 발명은 암호학을 대중영역에 접하게 하였다.

## 대칭키 암호 시스템

---

암호문을 생성(암호화)할 때 사용하는 키와 암호문으로부터 평문을 복원(복호화)할 때 사용하는 키가 동일한 암호 시스템이다. 암호 시스템의 안전성은 키의 길이, 키의 안전한 관리에 상대적으로 의존성이 높다. 암호문의 작성자와 이의 수신자가 동일한 키를 비밀리에 관리해야 하므로 폐쇄적인 특성을 갖는 사용자 그룹에 적합한 암호 시스템이다. 냉전시절 워싱턴과 모스크바 사이의 핫라인(hot line)에 적용되었던 OTP(one time pad)는 대칭키 암호 시스템의 예이다.

### 암호화 및 복호화

엘리스(Alice)가 밥(Bob)에게 암호문을 보내고 복호화하는 가장 기본적인 과정을 기술한다. 엘리스와 밥은 같은 키를 공유하고 있어야 한다. 엘리스는 공유한 키로 암호화를 하며, 밥은 같은 키로 이를 복호화한다. 보통 복호화 과정은 암호화 과정의 역과정이다. 암호화와 복호화에 사용된 키가 같지 않더라도 한 키로부터 다른 키를 쉽게 얻을 수 있는 경우에는 대칭키 암호 시스템의 범주에 넣는다.

### 대칭키 암호 시스템의 문제점

대칭키 암호 시스템은 알고리즘이 상대적으로 단순한 장점이 있지만 키 관리에 어려움이 많다. 시스템에 가입한 사용자들 사이에 매 두 사용자 마다 하나의 서로 다른 키를 공유해야 하기 때문에  $n$  명이 가입한 시스템에는  $nC_2 = n(n-1)/2$  개의 키가 필요하다. 또 각 사용자는  $n-1$  개의 키를 관리해야 하는 부담이 있다. 이는 매우 큰 단점으로 키 관리가 상대적으로 용이한 공개키 암호 시스템의 출현의 계기가 되었다.

### 대칭키 암호 시스템의 종류

대칭키 암호 시스템의 안전성은 키의 길이와 매우 관련이 크다. 일반적으로 키의 길이가 길수록 안전성은 높다. 그러나 키의 길이를 무한정 길게 하면 그에 따르는 관리의 어려움이 커진다.

- DES
- Advanced Encryption Standard(AES)
- ARIA
- Twofish
- SEED

## 공개키 암호 시스템

---

대칭키 암호 시스템의 가장 큰 약점은 키관리의 어려움에 있다. 한 사용자가 관리해야 할 키의 수가 너무 많아지기 때문이다. 이러한 약점을 보완하기 위해 나타난 암호 시스템이 공개키 암호 시스템이다. 공개키 암호 시스템에서 각 사용자는 두 개의 키를 부여 받는다. 그 하나는 공개되고(공개키, public key), 다른 하나는 사용자에게 의해 비밀리에 관리 되어야 한다.(비밀키, private key) 공개키 암호 시스템에서 각 사용자는 자신의 비밀키만 관리하면 되므로 키 관리의 어려움을 줄일 수 있다. 공개키 암호 시스템에서는 각 사용자의 공개키를 관리하는 공개키 관리 시스템(공개키 디렉터리)이 필요하며 각 사용자는 이 시스템에 자유롭게 접근하여 다른 사용자의 공개키를 열람할 수 있어야 한다.

공개키 암호 시스템은 두 키의 수학적 특성에 기반하기 때문에, 메시지를 암호화 및 복호화하는 과정에 여러 단계의 산술 연산이 들어간다. 따라서 대칭키 암호 시스템에 비하여 속도가 매우 느리다는 단점을 지니고 있다.

## 암호화 및 복호화

엘리스(Alice)가 밥(Bob)에게 암호문을 보내고 복호화하는 가장 기본적인 과정을 기술한다. 두 사용자에게는 각각 공개키와 비밀키가 부여되었고, 이들의 공개키는 공개키 디렉터리에 저장되어 있다. 엘리스는 공개키 디렉터리에서 밥의 공개키를 찾아 이를 이용하여 문서를 암호화하여 밥에게 보낸다. 밥은 수신한 비밀 문서를 자신만이 알고 있는 자신의 비밀키로 복호화하여 엘리스가 보낸 문서의 내용을 알 수 있다. 공개키 만으로는 복호화가 불가능하기 때문에, 엘리스 역시 암호화 하고 나서 복원할 수 없다는 특징이 있다.

공개키 암호 시스템에서 암호화-복호화 시스템은 두 키가 짝으로 동작하기 때문에, 비밀키로 암호화 하고 공개키로 복호화 할 수도 있다. 이 방법을 이용하면 해당 공개키에 맞는 비밀키 보유자를 확인 할 수 있으며, 전자서명에서는 이런 성질을 이용한다.

이와 같이 공개키 암호 시스템에서는 암호화할 때 사용되는 키와 복호화할 때 사용되는 키가 다르기 때문에 비대칭 암호 시스템이라고 부르기도 한다.

## 공개키와 비밀키의 관계

공개키 암호 시스템에서 각 사용자에게 부여되는 공개키와 비밀키에는 수학적 연관이 있기 때문에 암호화와 복호화가 가능하다. 이 둘은 마치 두 조각으로 나뉜 유리 조각과 같다. 한쪽은 공개되어 있고 그에 맞는 다른 한쪽은 감추어져 있는 것이다. 그러나 이들은 본래의 모습을 감추고 있다. 한쪽이 그대로 공개 된다면 숨겨진 다른 한쪽의 모습도 알려질 수 있기 때문이다. 원래의 모습을 감추고 또 원래의 모습으로 되돌리는 과정에서 수학이 중요한 역할을 한다.

## 공개키 암호 시스템의 종류

다음은 잘 알려진 공개키 암호 시스템의 예이다. 이들은 각각이 갖는 알고리즘과 키 생성상의 특성을 갖는다. 이것은 처리 속도, 구현의 편의성과 연관이 되어 응용되는 분야를 결정하게 된다.


- RSA
- ElGamal
- 타원 곡선 암호
- 배낭 암호

## 전자서명

---

- RSA

## 양자암호

 이 부분의 본문은 양자암호입니다.

### 양자암호

일반적으로 공개키 암호 시스템의 안정성은 한 방향으로의 접근은 쉽지만 그 역방향으로의 해결은 매우 어려운 수학 문제에 근거하고 있다. 예를 들어 RSA의 안전성은 알려진 매우 큰 두 소수의 곱은 쉽게 구할 수 있지만, 두 소수를 모르는 채 곱해진 결과가 어떤 소수들의 곱인지를 알아내는 것은 현실적으로 불가능하다는데 안전성의 근거를 두고 있는 것이다.

그런데 만약 안정성의 기반이 되는 어려운 수학의 문제가 해결된다면 그 문제에 안전성의 기반을 둔 암호 시스템은 더 이상 사용이 불가능하게 될 것이다.

그렇다면 가장 안전한 암호 시스템은 무엇인가? 가장 단순한 알고리즘을 사용하는 one time password(OTP)가 그 가운데 하나이다. 그러나 OTP는 대칭키 암호 시스템으로 키생성, 키분배 등 일련의 키관리의 어려움이 있는 암호 시스템이다.

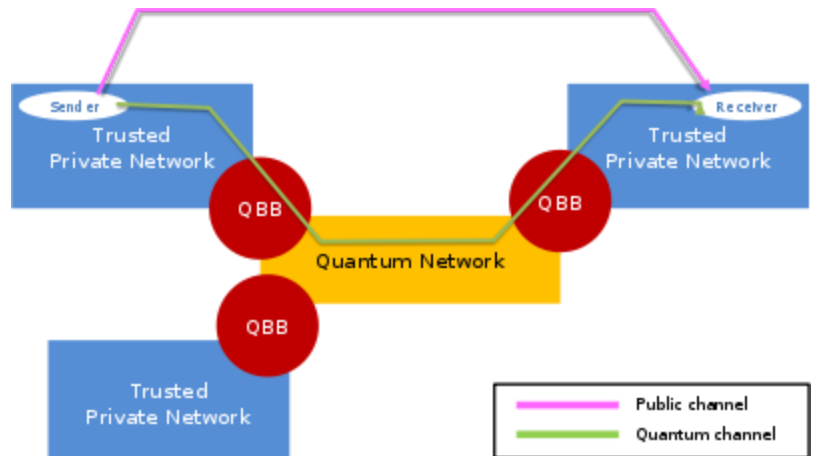
양자암호(quantum cryptography)는 OTP와 같은 안전한 암호 시스템이 갖는 키분배의 문제점을 해결할 수 있는 훌륭한 도구이다. 이런 이유 때문에 양자암호는 양자키분배(quantum key distribution)으로 이해되고 있다.

### 양자암호의 안전성

양자암호의 안전성은 불확정성원리(Uncertainty principle)에 근거하고 있다. 양자암호에서 키분배를 위한 통신으로 양자채널(quantum channel)과 인터넷이나 전화와 같은 통신수단(classical channel)을 동시에 사용한다. 일반적인 통신 수단을 이용한 정보의 교환은 노출 되어도 문제가 없다. 그러나 양자채널을 이용한 정보의 교환은 보안이 필요하다. 그런데 키 분배 또는 공유 과정에서 불법적인 사용자가 양자채널을 통과하는 정보를 측정하게 되면 불확정성원리에 따라 키분배 시스템의 정확도에 문제가 생겨 이를 합법적인 사용자가 감지할 수 있게 된다는 것이다. 하지만 중간자 공격(en:Man-in-the-middle attack)에 대해 취약하다는 단점이 있으며, QND(en:Quantum Nondemolition measurement)를 응용한 FPB Attack에 대해서도 취약하다는 것이 증명되었다.<sup>[1]</sup> 하지만 위의 두 경우 물리적 수단이나 고가의 장비가 동원되어야 한다는 전제조건이 있어 사실상 불가능하다.

### 키분배 프로토콜

1984년 Charles H. Bennett와 Gilles Brassard에 의해 완성된 키분배 프로토콜 BB84가 대표적이다. BB84에서는 광자 편광(photon polarization)의 상태를 수직, 수평 그리고 두 대각선으로 나누어 표현하여 디지털 신호를 나타내는 방법으로 키분배에 활용하고 있다. 하지만 광자 편광의 경우 노이즈에 취약하



양자암호에 기반해 만든 양자암호 네트워크 SECOQC의 네트워크 구조

다는 약점이 있어 이론에 대한 이해를 돕기 위한 용도로만 사용되고 있으며 실제 구현시, 위상차(phase)의 상태를  $0, \frac{1}{2}\pi, \pi, \frac{3}{2}\pi$ 로 나눈 다음 Mach-Zehnder interferometer (en:Mach-Zehnder interferometer)를 이용하여 구현한다.

## 양자암호의 종류

- BB84
- E91

## 같이 보기

---

- 암호학자
- 암호화
- 암호학의 개요(en:Outline of cryptography)
- 플레이페어 사이퍼(en:Playfair cipher)
- 스테가노그래피
- 크립트

## 각주

---

1. Franco N. C. Wong; Jeffrey H. Shapiro (2006년 5월 21일). “Attacking quantum key distribution with single-photon two-qubit quantum logic”. 《Lasers and Electro-Optics and 2006 Quantum Electronics and Laser Science Conference. CLEO/QELS 2006.》 .

---

원본 주소 "<https://ko.wikipedia.org/w/index.php?title=암호학&oldid=33529014>"