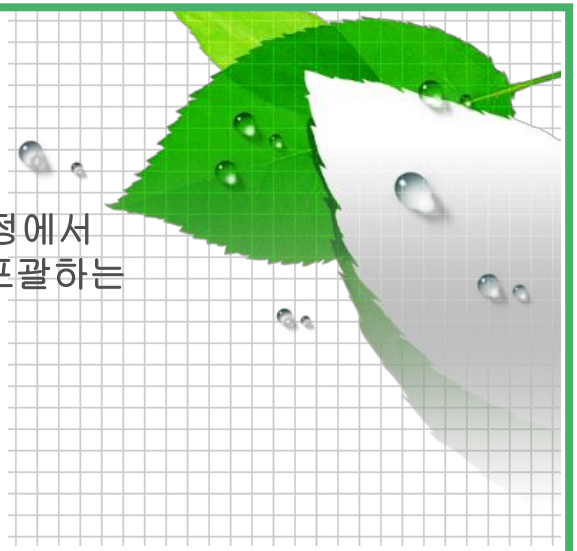

정보 보안

정보보안 개요



- 정의
  - 유형, 무형의 정보 생성과 가공, 유통, 배포, 그리고 사용하는 과정에서 발생하는 여러 부작용에 대처하기 위한 모든 정보 보호 활동을 포괄하는 광의의 개념
- 문제 발생 장소에 따른 구분
  - 컴퓨터 보안
  - 네트워크 보안
- 네트워크 상에서의 정상적인 정보 전송

그림 12-1 정보의 정상적인 전송

정보 보안 위협의 예(1)

전송차단

- 사용자 **A**가 사용자 **B**에게 정보를 전송할 때 사용자 **C**가 **B**와 연결할 수 없도록 하는 데이터 전송 차단**(interruption)**

그림 12-2 정보 전송 차단(방해)

가로채기

- 사용자 **A**가 사용자 **B**가 정보를 주고 받고 있는 사이에 사용자 **C**가 도청하는 경우

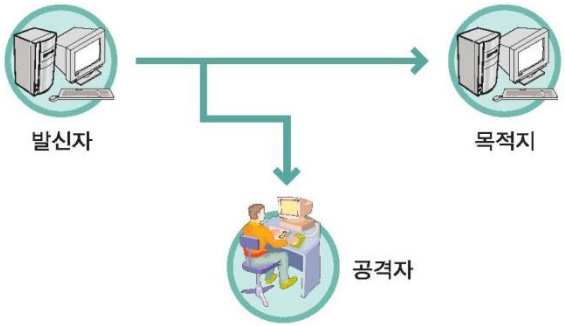


그림 12-3 정보 가로채기

정보 보안 위협의 예(2)

변조

- 사용자 A가 사용자 B에게 전송할 정보를 사용자 C가 중간에 가로채서 정보의 일부 또는 전부를 변경하여 잘못된 정보를 B에게 전송하는 경우

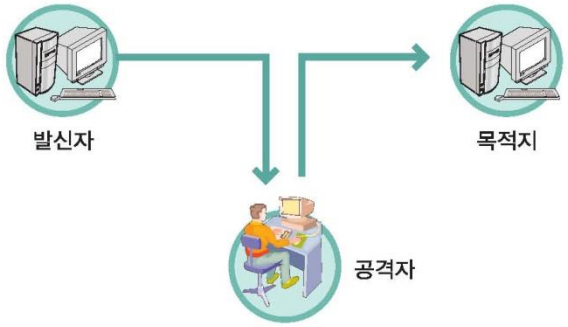


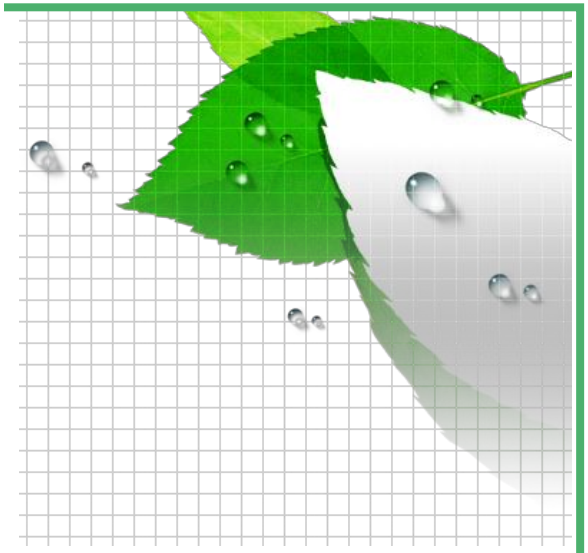
그림 12-4 정보 변조

위조

- 사용자 A도 모르게 사용자 C가 사용자 B에게 A가 정보를 전송한 것처럼 위조(fabrication)한 후 B에게 전송하는 경우

그림 12-5 정보 위조

정보보안 목표

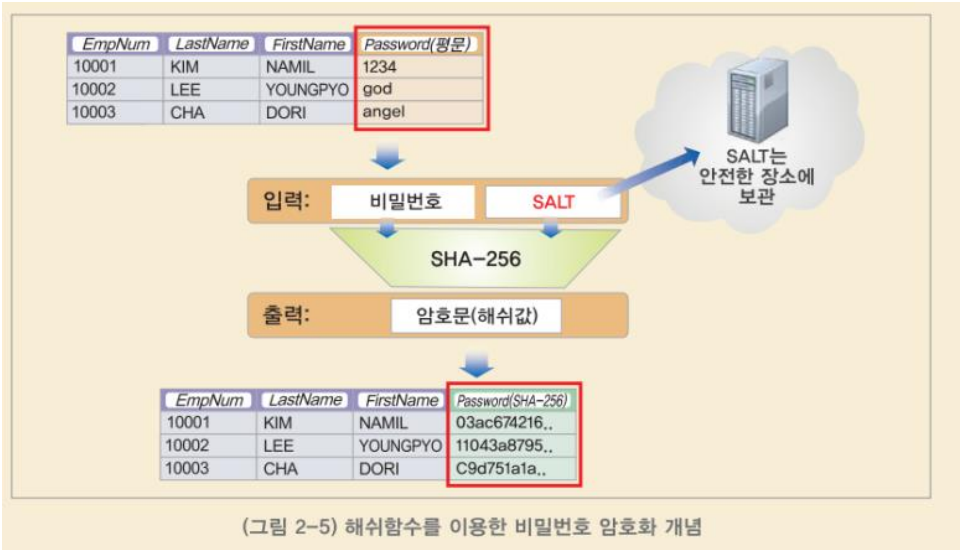


- 기본적인 목표
  - 내부 또는 외부의 침입자에 의해 행해지는
    - 파괴
    - 변조
    - 유출
  - 등과 같은 정보 범죄로부터 중요한 정보를 보호
- 정보보안 3요소
  - 기밀성(Confidentiality; 비밀성)
    - 정보의 비밀을 유지
  - 무결성 (Integrity)
    - 비인가된 변경으로부터 정보를 보호
  - 가용성 (Availability)
    - 필요할 때 언제든지 사용할 수 있음

기밀성

- 정보의 소유자가 원하는 대로 정보의 기밀이 유지되어야 함
- 오직 인가된(사람/프로세스/시스템)만이 알 필요성에 근거하여 시스템에 접근할 수 있음. 대표적인 예로는 로그인 통제
- 적용 기술 : 단방향암호화, 해쉬함수

그림 12-6 비밀성



(그림 2-5) 해쉬함수를 이용한 비밀번호 암호화 개념

무결성 정확하다 완전하다

- 정보는 고의적인, 비인가된, 우연한 변경으로부터 보호되어야 함
- 정보의 정확성, 완전성을 보장되어야 한다는 원
- 적용기술 : 암호기술, 전자서명, 바이러스 백신

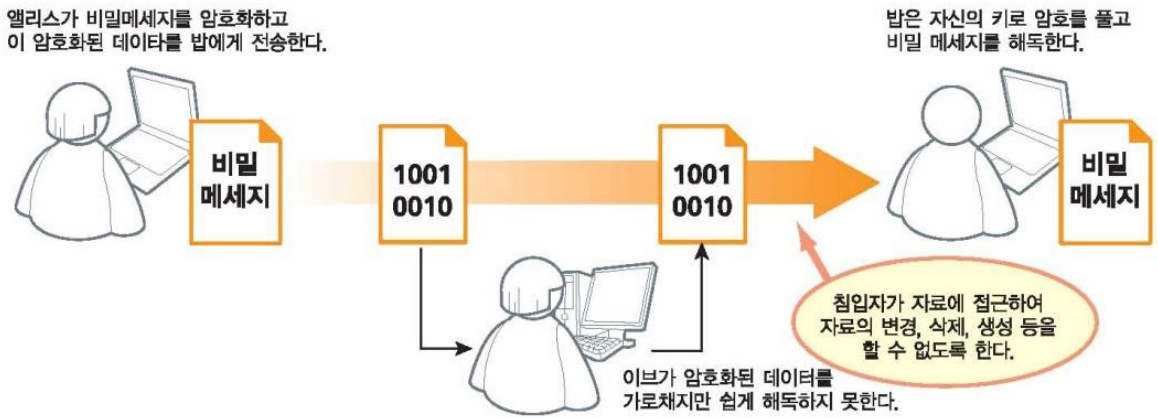


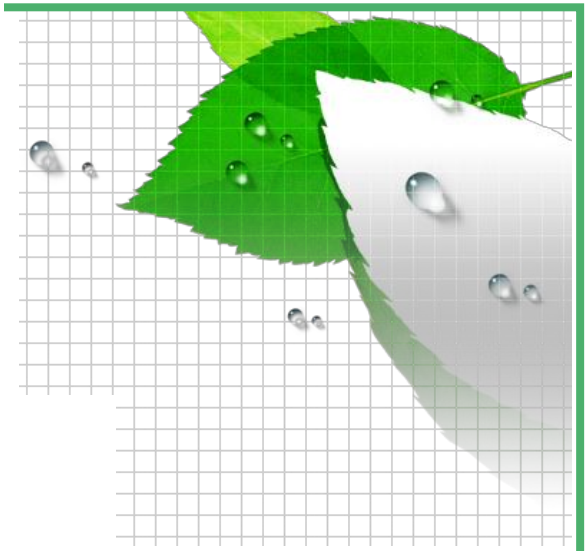
그림 12-7 무결성

가용성

- 정보는 사용자가 필요로 하는 시점에 접근이 가능해야 한다는 원칙
- 정보 시스템은 적절한 방법으로 작동되어야 하며, 정당한 방법으로 권한이 주어진 사용자에게 정보 서비스를 거부하여서는 안됨
- 가용성을 위협하는 공격
  - **Dos** (Denial Of Service)
    - **서비스 거부 공격**
    - 공격자가 호스트의 H/W 또는 S/W 등을 무력하게 만들어 호스트에서 적법한 사용자의 서비스 요구를 거부하도록 만드는 공격
    - 컴퓨터시스템이 처리할 수 없을 정도로 엄청난 분량의 패킷을 동시에 범람시킴으로써 네트워크의 성능을 저하시키거나 시스템을 마비시키는 방식
    - 1:1 공격
  - **Ddos**(Distributed Denial of Service)
    - 여러대의 컴퓨터를 이용하여 한대의 공격대상 시스템에 대한 DoS 공격
- 적용기술 : 백업, 결함허용 시스템 등

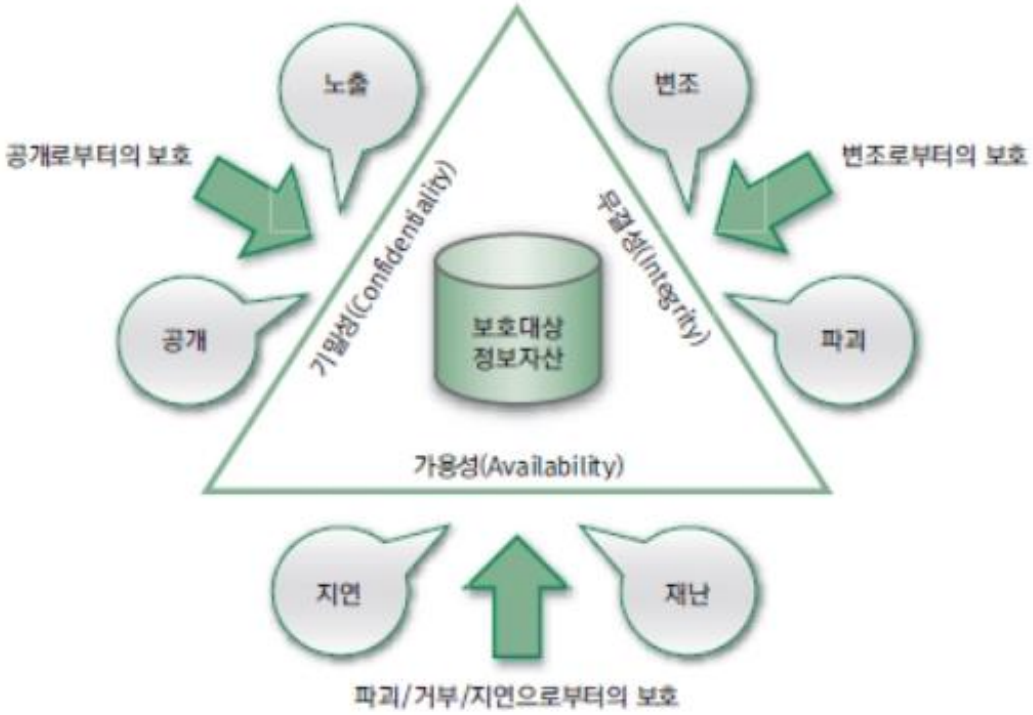
•결함감지하고 결함 진단을 통하여 결함으로 인한 타 모듈에 오류 파급 차단

정보보안 서비스(1)



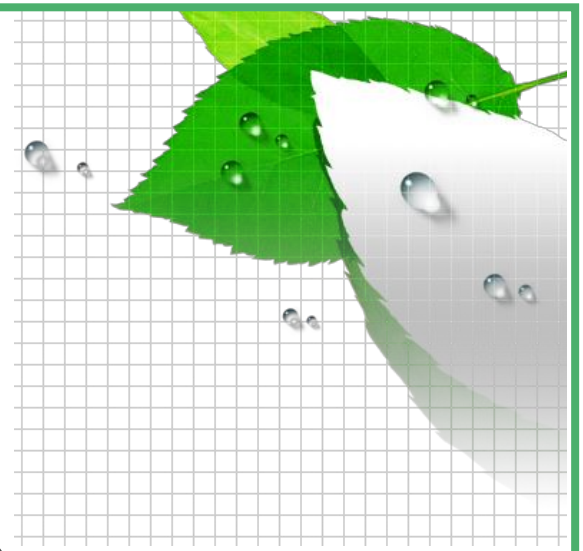
❖ 정보보호

- 비밀성, 무결성, 가용성 유지



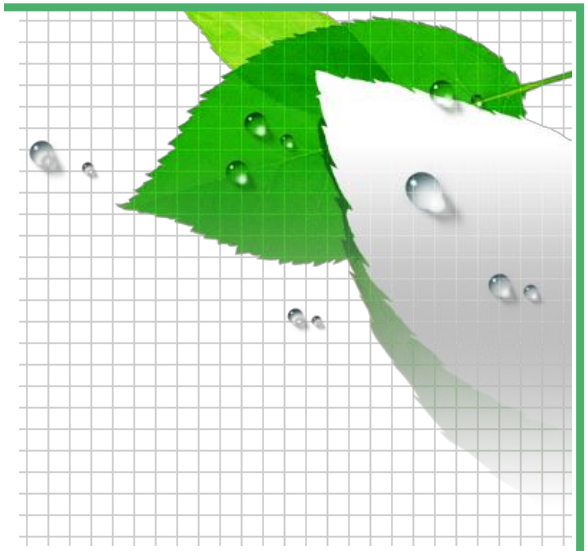
정보보안 서비스(2)

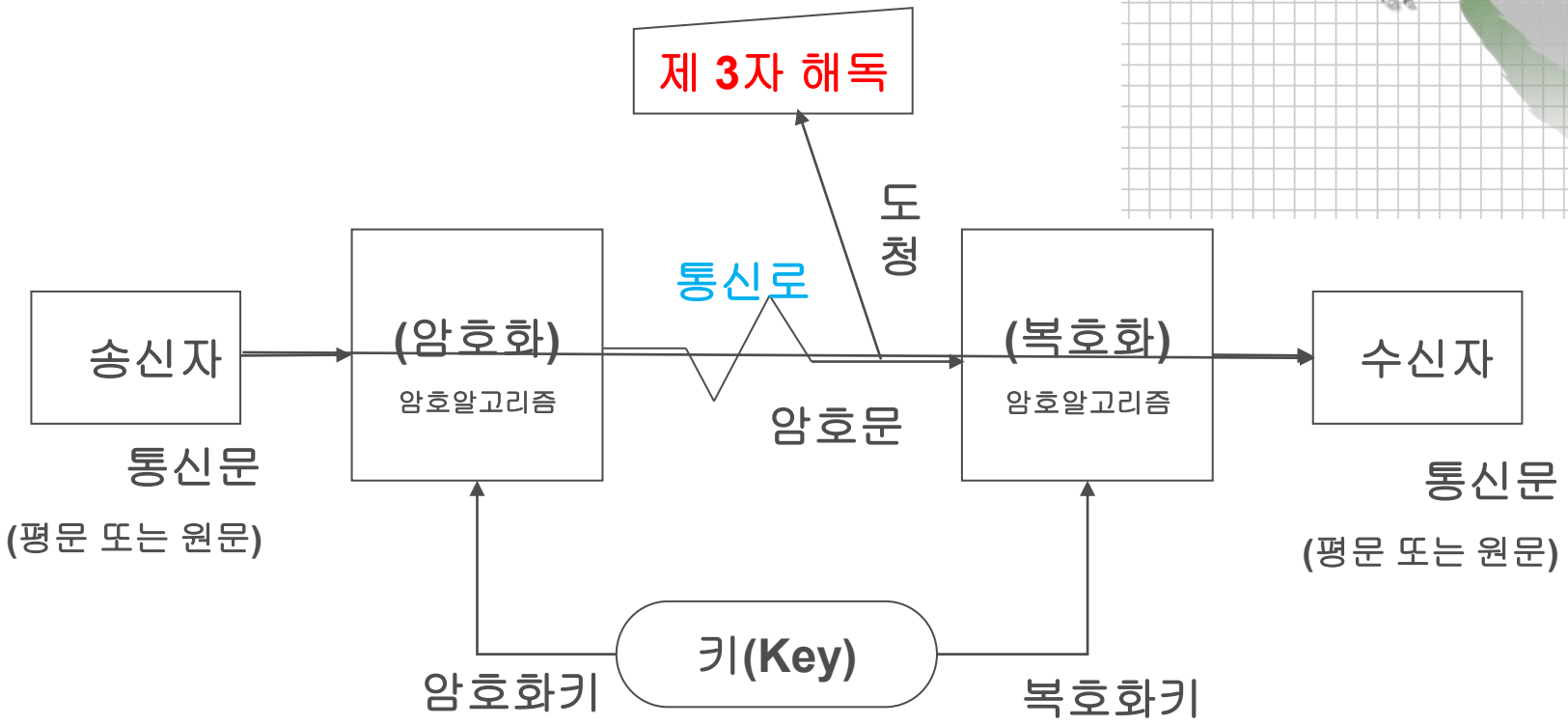
- 부인방지
  - 송신자와 수신자 두 사람 각각 전송하지 않았다고 주장하거나, 수신하지 않았다고 주장하는 것을 막는 방법
- 접근제어
  - 네트워크상에서 호스트 시스템이나 통신 링크에 연결된 응용 프로그램으로의 접근을 제한하거나 조절하는 능력
- 인증
  - 사용자 본인임을 확인



암호학

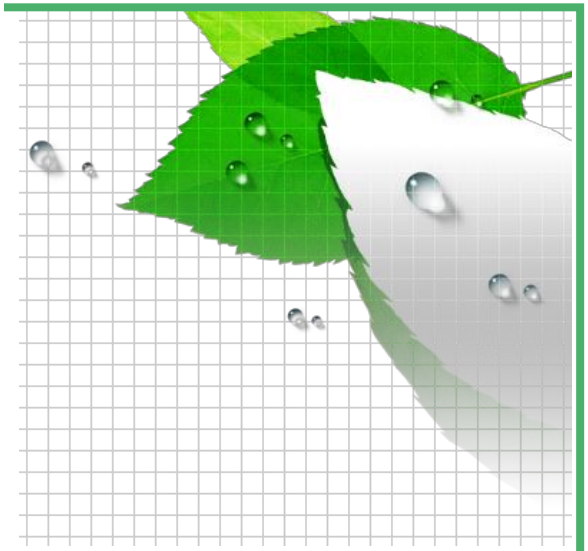
비밀 통신 절차




제 3자 해독
도청
통신로
송신자
(암호화)
암호알고리즘
암호문
(복호화)
암호알고리즘
수신자
통신문
(평문 또는 원문)
통신문
(평문 또는 원문)
키(Key)
암호화키
복호화키

참고영상

❖ 암호학의 역사



암호의 역사

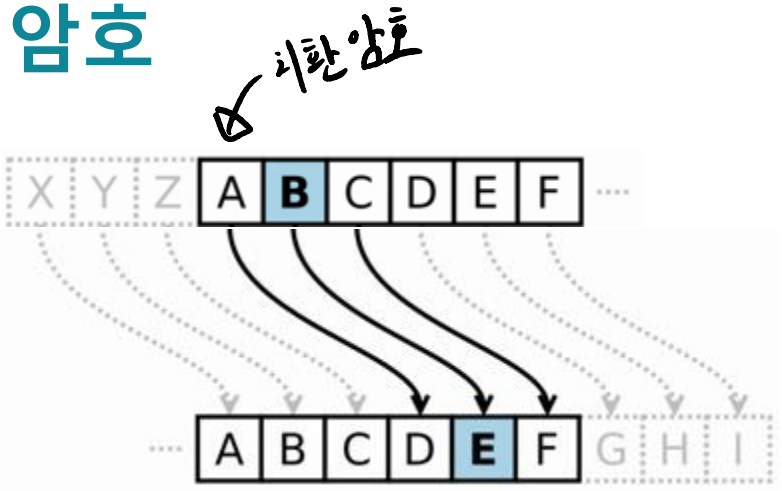
❖ 라이산더장군(스파르타)의 스키테일

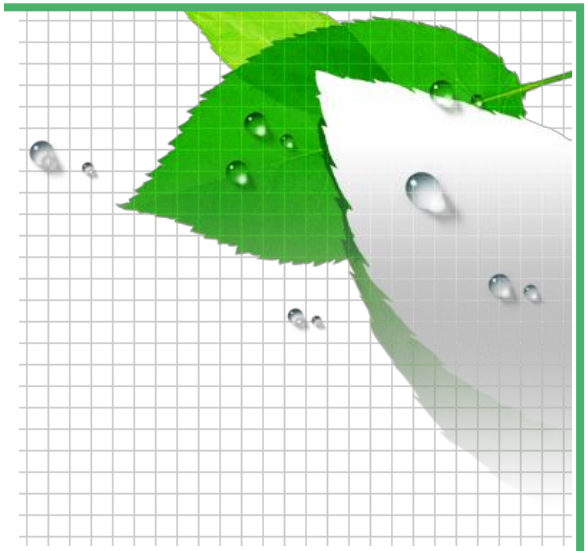
Key = 통나무의 두께

스파르타 군대의 '스키테일'에 적은 "HELP ME I AM UNDER ATTACK"은 양피지 리본을 풀면 "HENTEIDTLAEAPMRCMUAK"라는 전치암호가 된다.

암호의 역사

❖ 시저의 암호

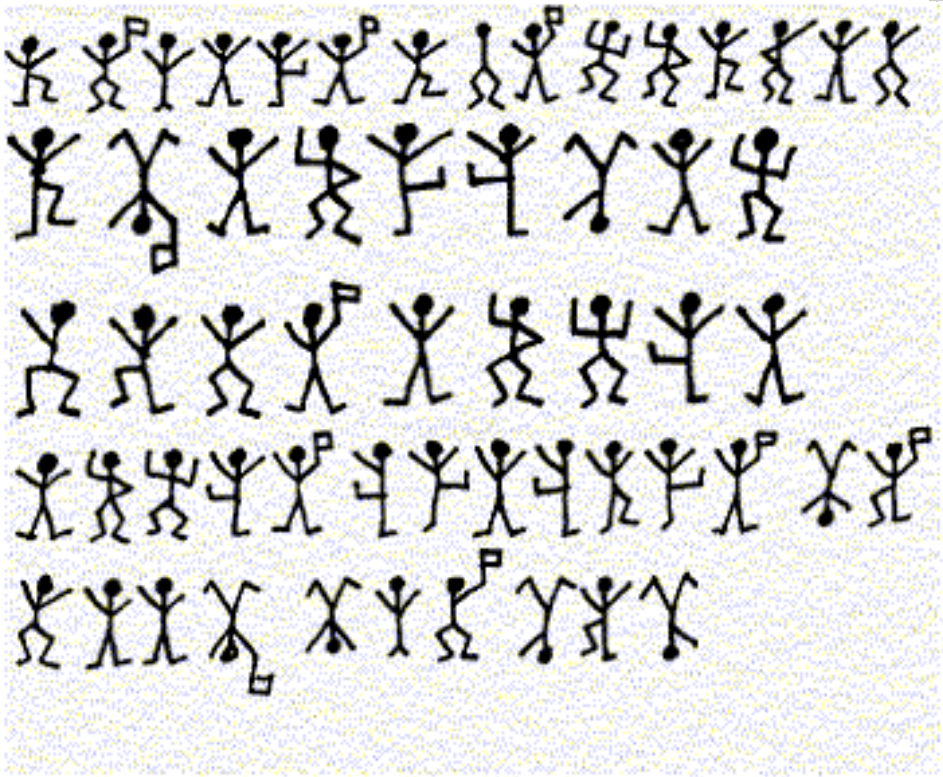




Key = 알파벳의 이동거리

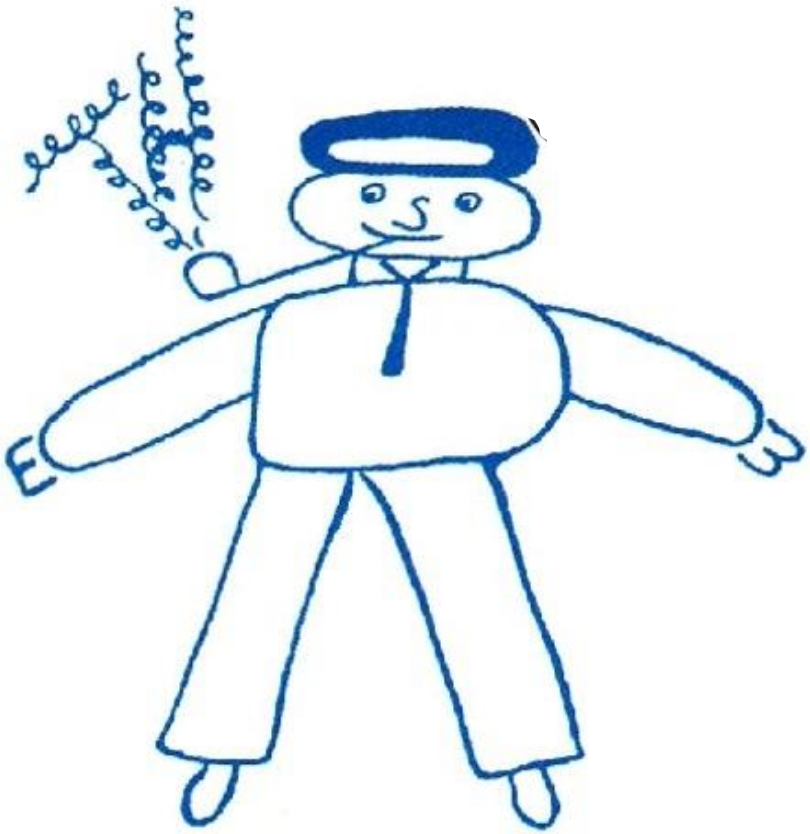
소설 속의 암호화

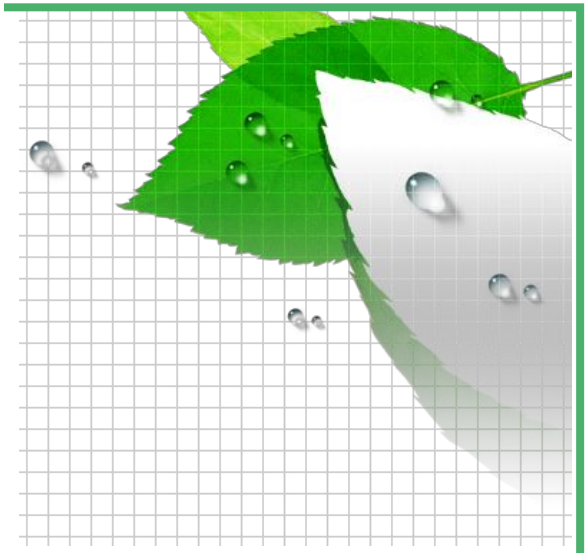
❖ 셜록홈즈의 춤추는 인형



1차세계대전

❖ 프랑스 스파이의 비밀편지

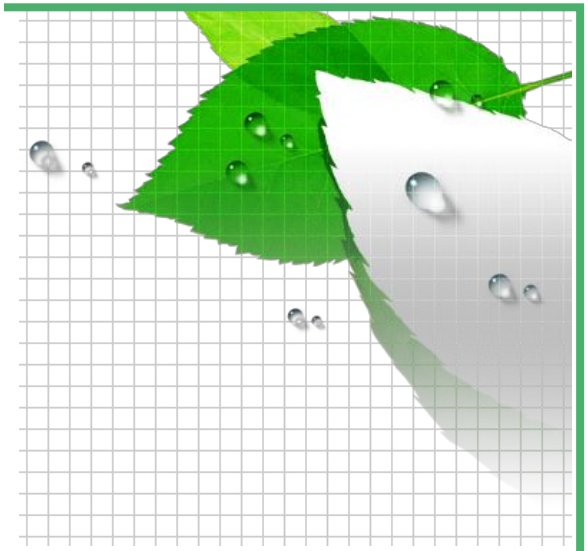




1. 9일 leper
2. 모자 쓰고 넥타이맨 해군이 접선자
3. 8일 Ypres
4. 담배를 통해 화학무기 공격

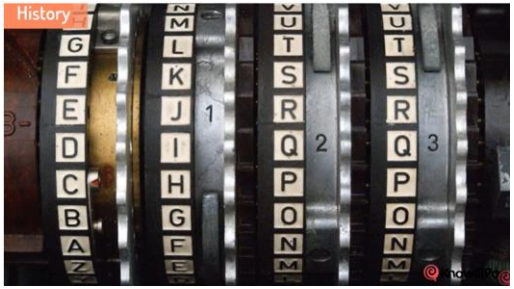
참고영상

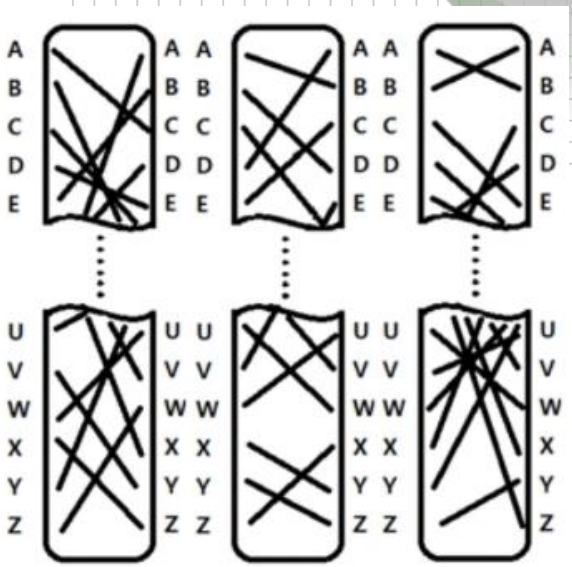
- 기계식 암호화의 대표
  - 애니그마



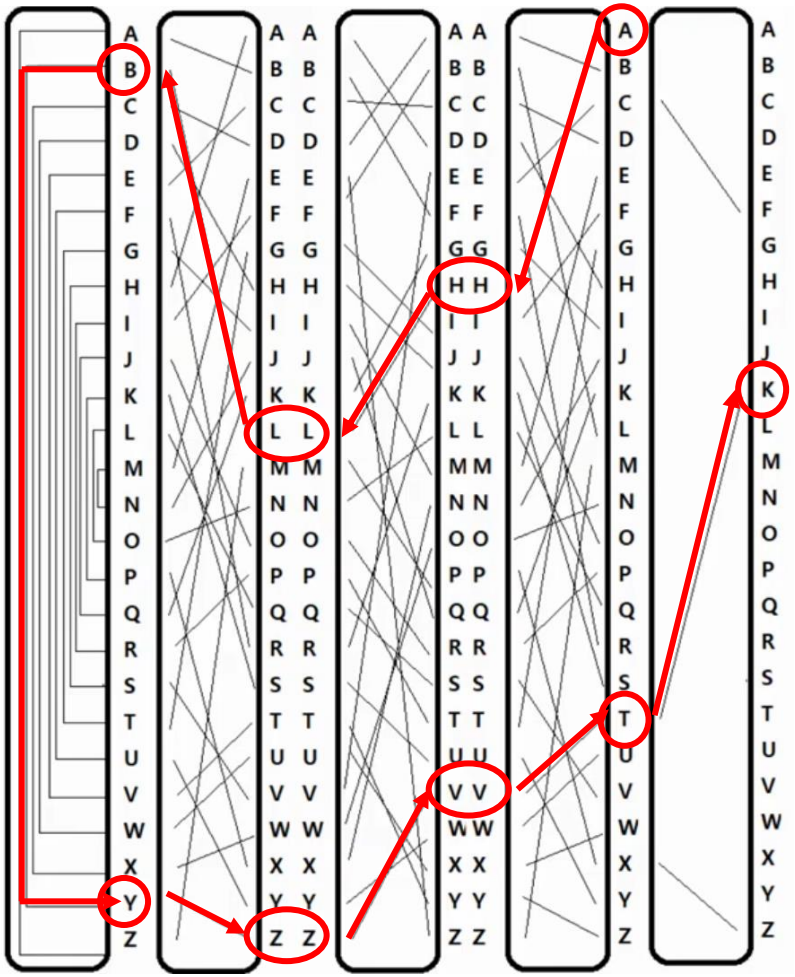
2차세계대전

- 기계식암호
  - 독일의 Enigma

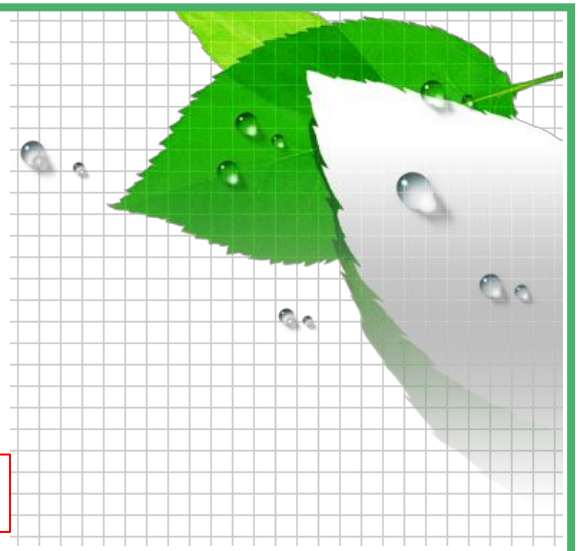




Enigma의 원리



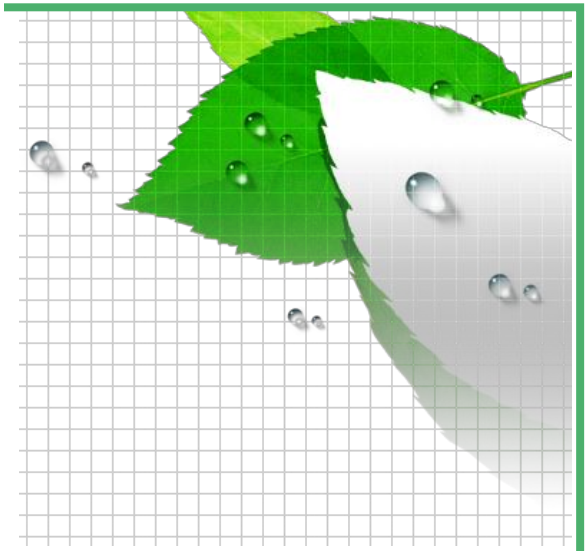
반사판 회전판



A→K

- 영국의 수학자 앨런튜링에 의해 해독됨
  - 콜로서스
  - 컴퓨터의 효시

참고 영상출처



- 유튜브
  - KnowlliPop 놀리팝
  - **https://www.youtube.com/watch?v=7Lh0aT_15b8**