제1장 암호학

한국IT 정보보안학부

1.1 정보화 사회와 암호학

❖ 사회의 변천

- 수렵 사회
  - 총을 비롯한 온갖 연장을 가지고 새나 짐승을 포획하는 일.
  - 고대의 인류에게는 수렵(사냥)이 먹고 살기 위한 절대적인 생활수단
- 농경 사회
  - 가축이나 인력이 사회를 움직이는 주요동력
- 산업 사회
  - 석유와 석탄, 천연가스 같은 지하자원이 세상을 움직이는 주요 동력
- 정보화 사회
  - 주요원동력

  -> 정보 (Information),

  -> 정보기술 (Information Technology),

  -> IT 인프라구조 (IT Infrastructure)

1.1 정보화 사회와 암호학

❖ 정보화 사회

- 정보통신망 보급
- 정보시스템 사용 일반화
- 정보의 분산화
- 정보의 대용량화

1.1 정보화 사회와 암호학

❖ 정보화 사회

- 컴퓨터와 정보통신 기술의 결합

- 정보
  - 축적 (storage)
  - 처리 (processing)
  - 전송 (transmission)

- 정보시스템의 역기능
  - 정보의 무단절취, 수정, 파괴
  - 정보통신망의 부정 접속
  - 바이러스 확산 등

- 정보보호
  - 기밀성 (confidentiality)
  - 무결성 (integrity)
  - 가용성 (availability)

1.1 정보화 사회와 암호학

❖ 정보보호 취약성

- 물리적 취약성
- 자연적 취약성 : 화재, 홍수, 지진, 번개
- 환경적 취약성 : 먼지, 습도, 온도
- 하드웨어 취약성
- 소프트웨어 취약성
- 매체 취약성
- 전자파 취약성
- 통신 취약성 : 무단 접속, 침입
- 인적 취약성

1.1 정보화 사회와 암호학

❖ 정보보호 위협

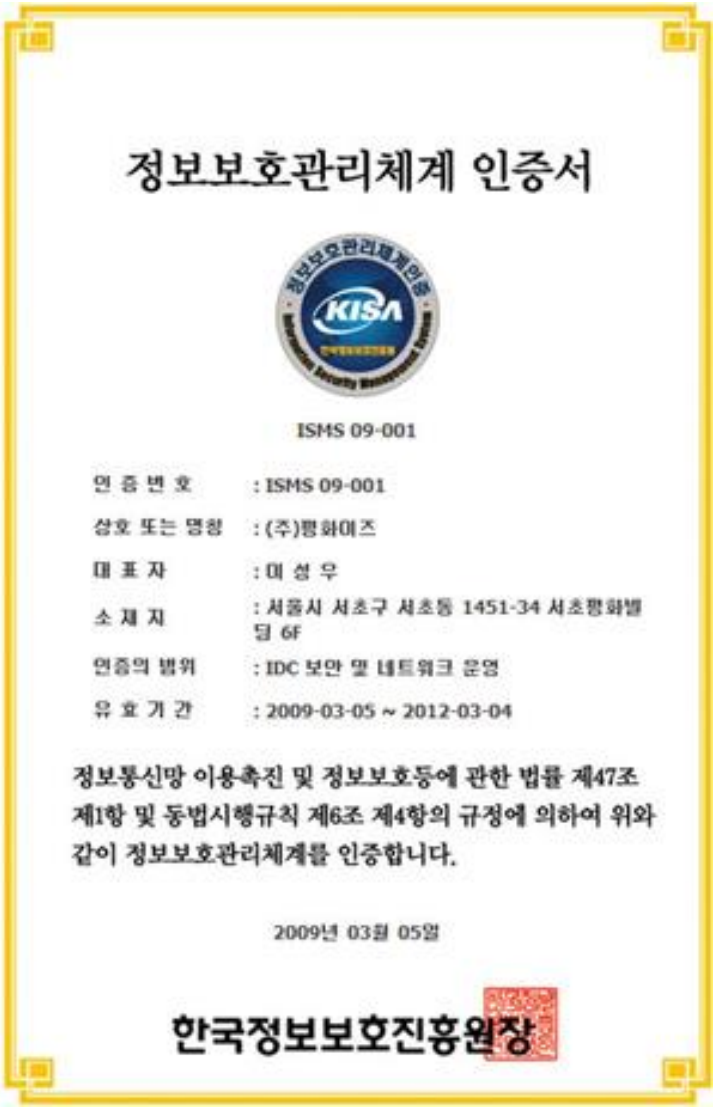
- 자연에 의한 위협
- 비의도적 위협 : 실수, 태만
- 의도적 위협 : 해커, 사이버테러, 도청

1.1 정보화 사회와 암호학

❖ 정보보호 체계

- 정보보호 관리
  - 전략정책, 위험분석, 보안계획, 보안구현, 인식교육, 보안감사
- 정보보호 산업
  - 정보보호 제품, 정보보호 서비스
- 정보보호 기술
  - 보안 제품기술 ,시스템 보안기술
  - 응용서비스 기술
    - 전자우편, 인터넷 보안, 전자상거래 보안
  - 보안 기반기술
- 정보보호 기반
  - 암호 키 센터, 사고대응 체제, 인증 / 인정
  - 법률 / 규제, 표준화, 홍보

정보보호관리체계(ISMS)인증



정보보호관리체계 인증서

ISMS 09-001

인 증 번 호	: ISMS 09-001
상호 또는 명칭	: (주)평화이즈
대 표 자	: 이 성 우
소 재 지	: 서울시 서초구 서초동 1451-34 서초평화빌딩 6F
인증의 범위	: IDC 보안 및 네트워크 운영
유 효 기 간	: 2009-03-05 ~ 2012-03-04

정보통신망 이용촉진 및 정보보호등에 관한 법률 제47조 제1항 및 동법시행규칙 제6조 제4항의 규정에 의하여 위와 같이 정보보호관리체계를 인증합니다.

2009년 03월 05일

한국정보보호진흥원장

정보보호관리체계인증 Information Security Management System KISA 한국인터넷진흥원 Korea Internet & Security Agency

http://isms.kisa.or.kr/kor/main.jsp

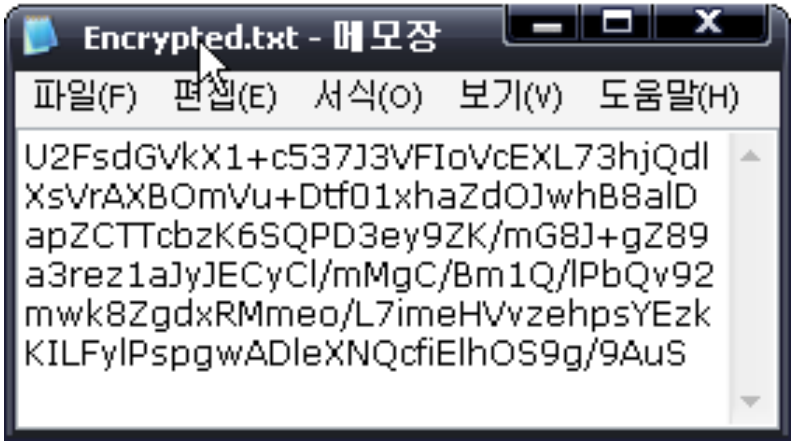
암호화

❖ 정보자산의 암호화

- 가장 경제적이면서도 정보 시스템이 요구하는 보안 수준에 따라 효과적으로 보안 대책을 제공할 수 있는 방법

  - [기사] 금융사 직원, 고객정보 암호화 필수

- 정보 보안 전문가는 정보 자산을 효과적으로 보호하기 위한 정보 암호 메커니즘, 암호 알고리즘 등의 지식을 이해하고 실무에 적용할 수 있어야 한다.



1.1 정보화 사회와 암호학

❖ 암호

- 암호의 사용 목적
  - 비밀통신 (비밀성)
  - 인증 (사용자 인증, 메시지 인증)
  - 접근제어 (가용성)

- 암호학의 학문화
  - 통신
    - 통신방식
    - 통신이론

1.1 정보화 사회와 암호학

❖ 암호화의 목적

- 기밀성(secrecy)
  - 수동적인 공격으로부터 데이터를 보호
  - 즉, 인증된 사람만 자료 열람
- 무결성(integrity)
  - 수신된 메시지가 불법적으로 재생된 것인지 확인
  - 전송과정에서 변조 또는 재구성 되지 않았음을 증명
- 인증(authentication)
  - 정보나 사용자의 정체(실제신원)를 확인
- 부인방지(non-repudiation)
  - 송신자와 수신자간의 전송 메시지에 대한 분쟁을 방지

1.1 정보화 사회와 암호학

암호학이 사용되어지는 분야

- 컴퓨터,네트워크시스템의 데이터 Protection
- 전자상거래
- 온라인(인터넷) Banking
- 전자서명
- 이동전화
- 전자지갑

1.1 정보화 사회와 암호학

용어정의

- 암호학 (Cryptology)
  - Cryptology=(cryptos=hidden)+(logos=theory)
  - 기밀, 자료 무결성, 사용자 인증, 자료출처 인증 등과 같은 정보보안에 관련된 수학적 기술의 연구
- 암호 기술 (Cryptography)
- 암호분석 기술 (Cryptanalysis)
- 암호 (Cipher)
  - 자료의 기밀성을 보장하기 위하여 안전성이 입증된 수학적 논리에 의하여 변환하는 과정
  - 평문을 인가되지 않은 자가 이해하기 어려운 형태로 수학적 논리에 의하여 변형하기 위한 원리, 수단, 방법

1.2 암호의 역사

- 라이산더 암호 (그리스 BC. 400)
- 시저 암호 (로마 BC. 100~44)
- ENIGMA 암호
- ADFGVX 암호
- 무라사끼 암호 (97식)
- DES (1974)
- 공개키 암호 방식 (Diffie-Hellman, 1976)
- RSA (1978)
- AES(2000)
- SEED
- ARIA

1.2 암호의 역사

❖ 암호의 사용

- 고대, 근대
  - 외교
  - 전쟁

- 현대
  - 외교문서
  - 고문서 해독
  - 상업용

1.2 암호의 역사

❖ 암호

- 고대 암호
  - 전치 암호(transposition cipher)
  - 환자 암호(substitution cipher))
- 근대 암호
  - 적 암호(product cipher) : 환자 암호 + 전치 암호
  - 암호기 사용
- 현대암호
  - 현대 대수학

1.2 암호의 역사

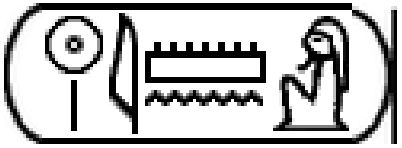
❖ 고대 암호 : 환자 암호, 전치 암호

- 고대 이집트 문자
- Atbash (아트배쉬 암호)
- Steganography (스테가노그라피)
- Scytale (스카이테일)
- Polybius square (폴리비우스 사각형)
- Caesar (시저 암호)

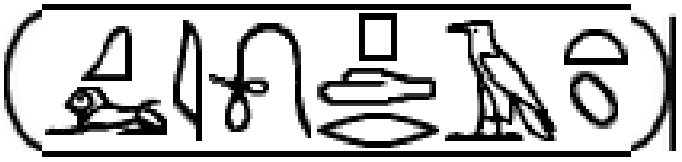
1.2 암호의 역사

❖ 고대 이집트 문자

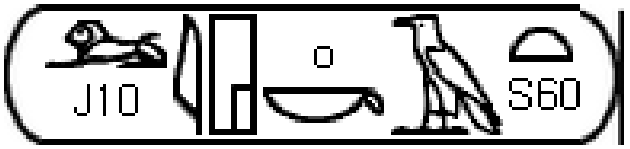
- 고대 이집트 왕조 시대에 사용한 상형 문자
- 환자 암호 방식, 생소한 그림기호를 사용함
- 암호화 된 가장 오래된 문서로 평가됨



jmn-rꜥ, "Amon-Ra ";



qljwꜥpdrꜥ.t, "Cleopatra ";



ljwkꜥ.t, "Lioka."

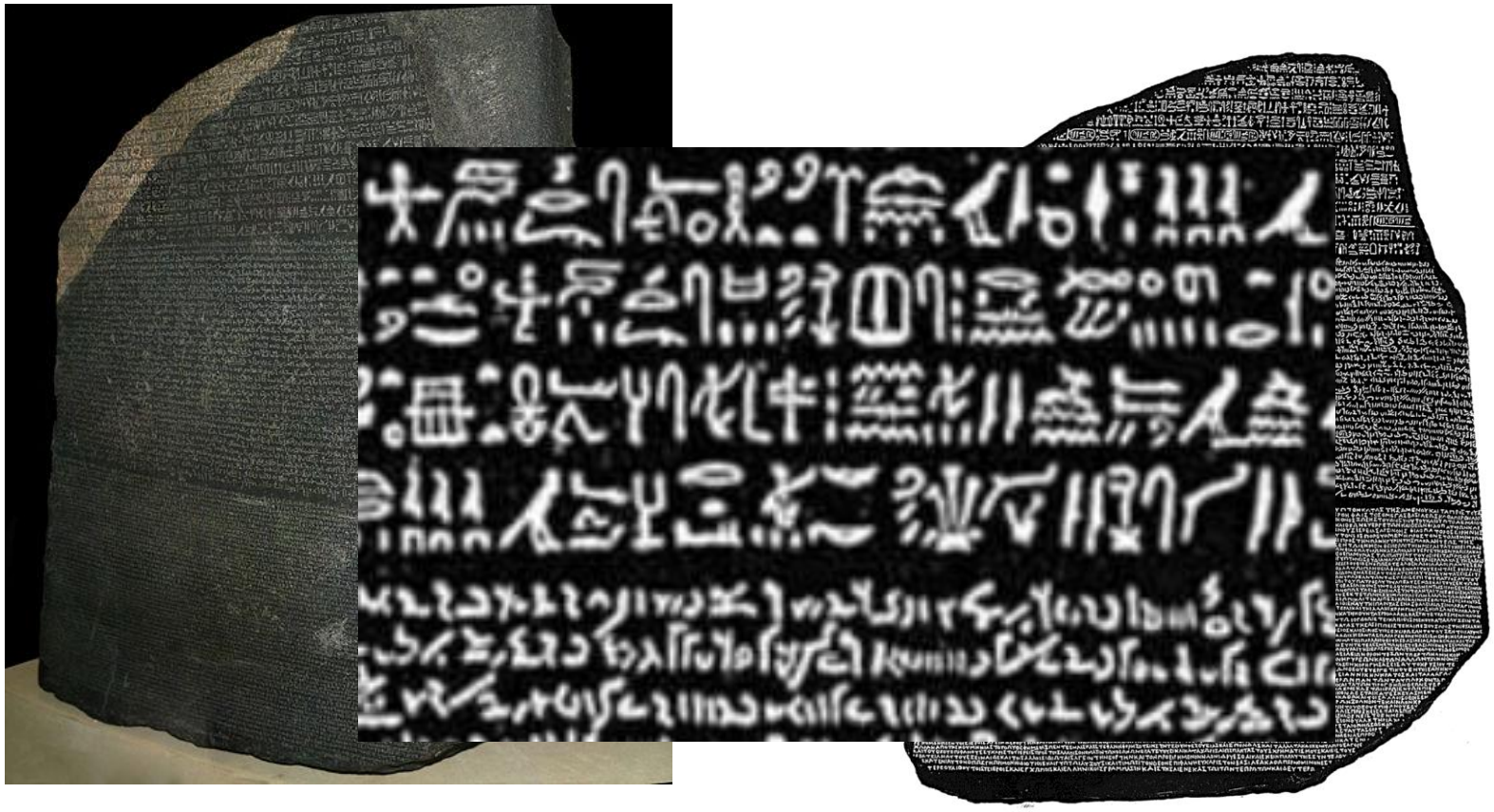
1.2 암호의 역사

- 사자의 서(死者의 書, Book of the Dead)

1.2 암호의 역사

❖ Rosetta Stone : 로제타 석

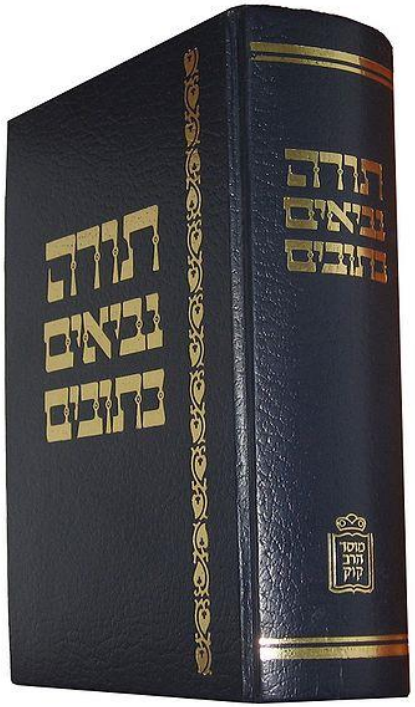
- 로제타 석으로 인해 이집트 상형문자를 해석할 수 있었다고 함
- 고대 이집트 문명의 비밀을 밝히는 데 큰 공을 세운 중요한 유물

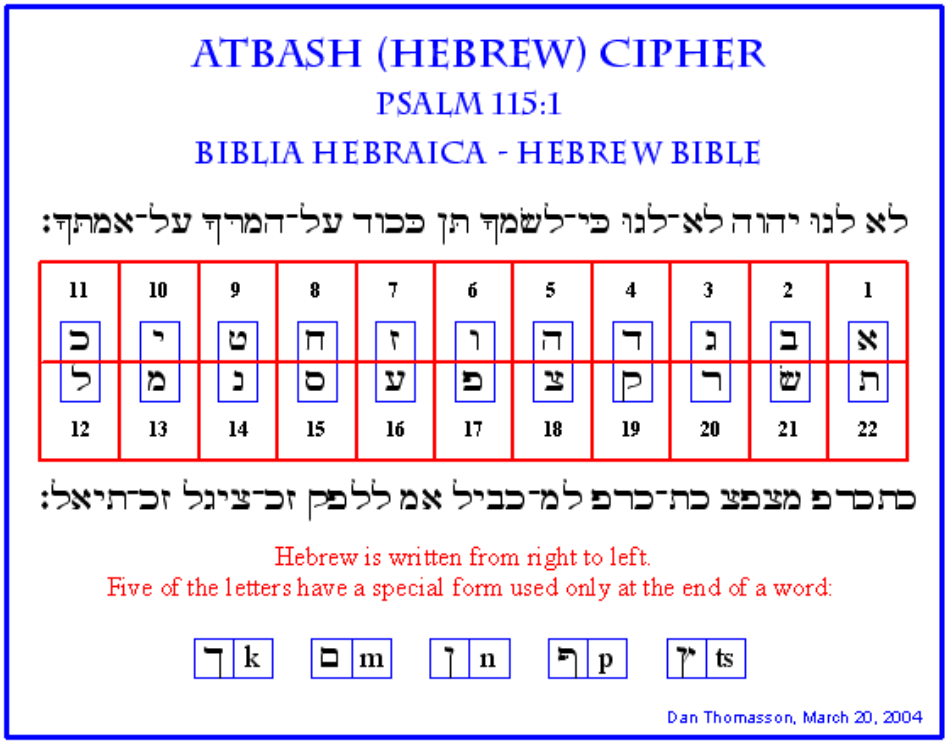


1.2 암호의 역사

❖ Atbash Cipher (아트배쉬 암호)

- Hebrew 알파벳을 위한 단순 환자 암호
- Hebrew Bible(성서)를 기술할 때 사용
- 글자의 순서를 완전히 거꾸로 하여 기록





1.2 암호의 역사

❖ Atbash Cipher (아트배쉬 암호)

- Good to see it → Tllw gl hvv rg 로 암호화

The Atbash cipher for the modern Hebrew alphabet would be:

```
Plain:  אבגדהוזחטיכלמנסעפצקרשת
Cipher: תשרקצפעסנמלכיטחזוהדגבא
```

An Atbash cipher for the Roman alphabet would be as follows:

```
Plain:  abcdefghijklmnopqrstuvwxyz
Cipher: ZYXWVUTSRQPONMLKJIHGFEDCBA
```

An easier, simpler and faster way of doing this is:

```
First 13 letters: A|B|C|D|E|F|G|H|I|J|K|L|M
Last 13 Letters:  Z|Y|X|W|V|U|T|S|R|Q|P|O|N
```

1.2 암호의 역사

❖ Steganography (스테가노그라피)

- 비밀(암호) 메시지
- 메시지 암호라기 보다는, 다른 사람이 인식하지 못하도록 통신문(내용)을 감추는 기법

  - 예) 각 픽셀의 마지막 두 bit를 변형함으로써 나무로 부터 고양이 이미지 만들어 냄

1.2 암호의 역사

❖ Scytale, 스카이테일

- 가장 오래된 암호 방식으로 기원전 400년경 고대 희랍인들이 사용한 전치 암호기술
- 최초의 군사적 암호로 스파르타 군대에서 사용함, 지도자와 부하 간의 송수신 통신 내용 보호가 목적

1.2 암호의 역사

❖ Polybius square (폴리비우스 사각형)

- 그리스인 폴리비우스(Polybius)는 그리스 알파벳을 숫자로 변환시키는 암호를 개발
- 한 알파벳 문자에 대해서 대응하는 숫자들이 적힌 표(checker board)를 가지고 알파벳을 수로 변환, 환자 암호기술

- 예) I am a student

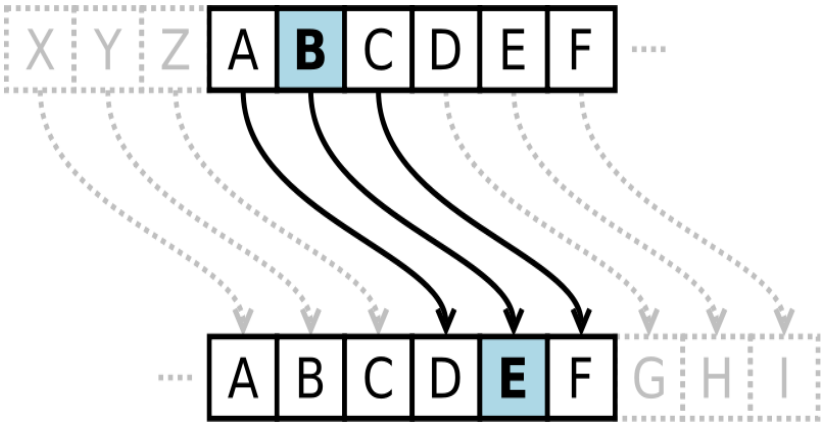
24 11 32 11 43 44 45 14 15 33 44

Greek alphabet			
Αα	Alpha	Νν	Nu
Ββ	Beta	Ξξ	Xi
Γγ	Gamma	Οο	Omicron
Δδ	Delta	Ππ	Pi
Εε	Epsilon	Ρρ	Rho
Ζζ	Zeta	Σσς	Sigma
Ηη	Eta	Ττ	Tau
Θθ	Theta	Υυ	Upsilon
Ιι	Iota	Φφ	Phi
Κκ	Kappa	Χχ	Chi
Λλ	Lambda	Ψψ	Psi
Μμ	Mu	Ωω	Omega

1.2 암호의 역사

❖ Caesar cipher (시저 암호)

- 환자 암호기술
- 케사르 암호 방식, 시프트 암호 방식이라고도 함
  - Caesar cipher, shift cipher
  - 각 평문의 문자를 3자리(n자리) 뒤의 문자로 치환



1.2 암호의 역사

❖ 근대 암호 : 적 암호, 암호 기계

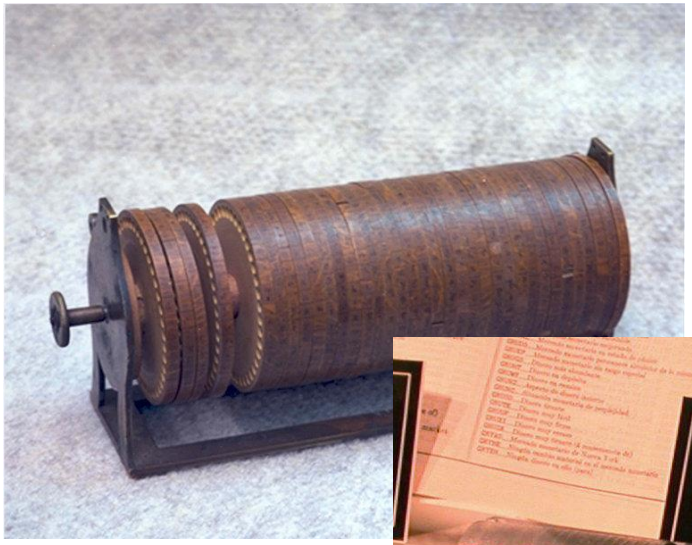
- 17세기 근대 수학의 발전과 더불어 고급 암호가 발전하기 시작
- 본격적인 근대 수학을 도입한 과학적인 근대 암호는 20세기에 비로소 발전하기 시작

- Jefferson disk
- Enigma
- Colossus computer
- Hill's cipher machine
- Hagelin M-209 Cipher Machine

1.2 암호의 역사

❖ 제퍼슨 디스크 (Jefferson disk)

- 시스템은 26개의 바퀴를 사용해서, 서로 다른 문자의 알파벳을 다른 것으로 치환시키는 것



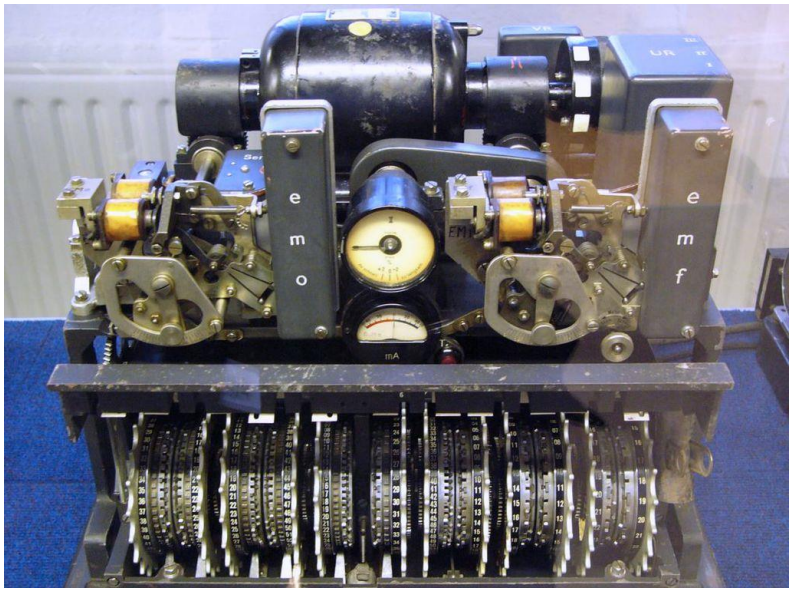
1.2 암호의 역사

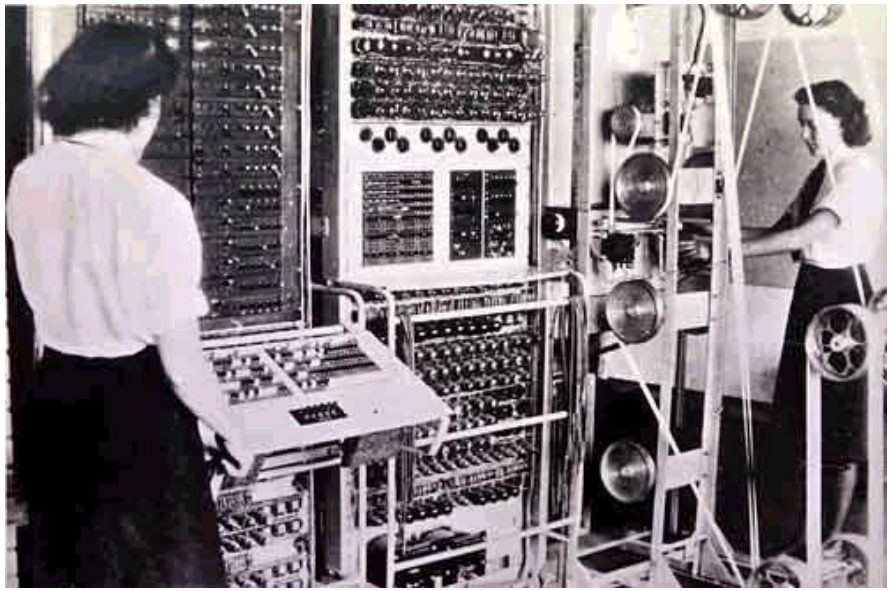
❖ Enigma

- 1918년 독일 개발
- 평문을 자판으로 입력하면 각 회전자에 의하여 암호문으로 변환됨

1.2 암호의 역사

- **Colossus computer (Mark II)**
  - 1943년부터 1945년 사이에 영국의 암호 해독가들이 로렌츠 암호 해독을 위해 개발한 컴퓨터

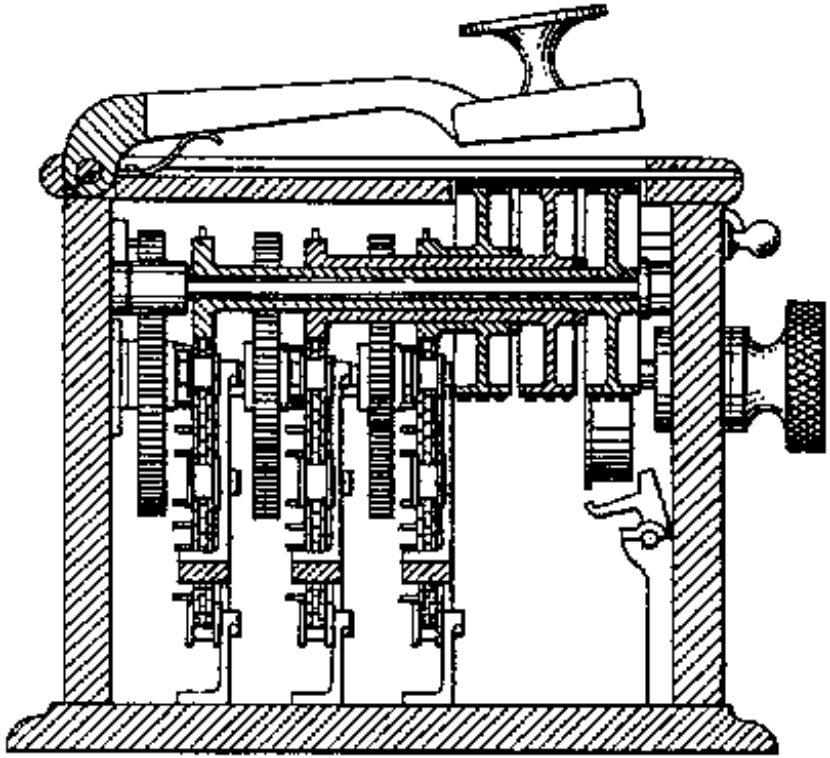




1.2 암호의 역사

❖ Hill cipher machine

- 1929년 Lester S.Hill
- Hill 암호, 다형 환자 암호
- 두 문자 이상을 묶어 이들을 다른 문자나 숫자로 변환

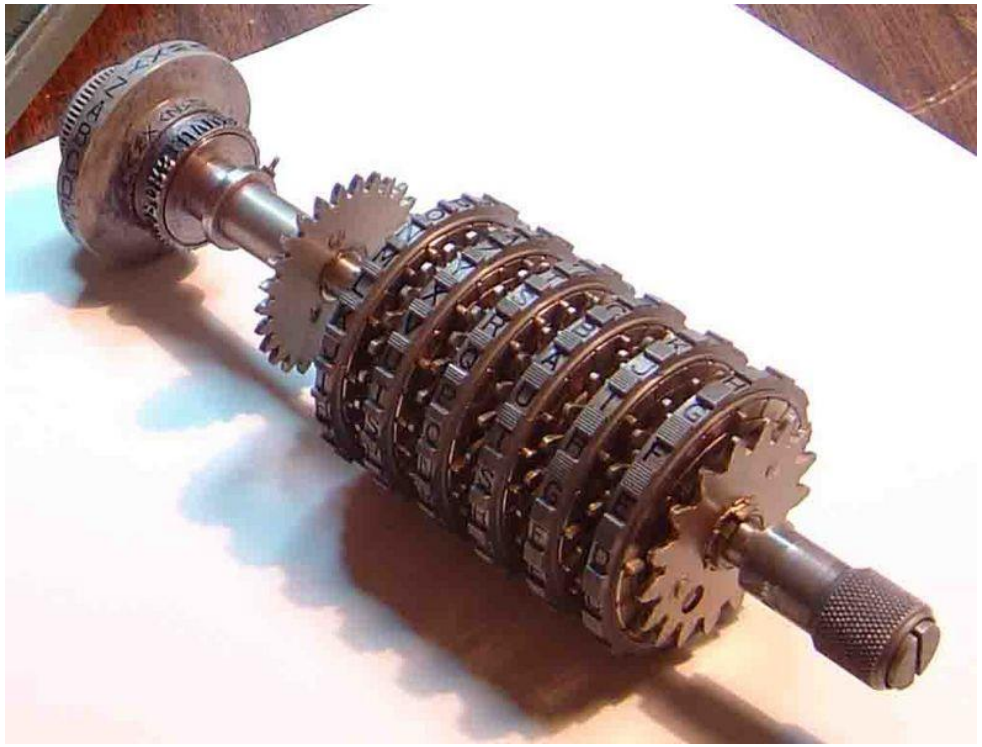


1.2 암호의 역사

❖ Hagelin M-209 Cipher Machine

- 해글린 암호 기계
- 한국전쟁에서 미군이 사용

HAGELIN M-209 CIPHER MACHINE (GVG / PD)



1.2 암호의 역사

❖ 암호

1.2.3현대암호

- 공개키 암호방식제안 (1976)
- RSA(1978)
- DES(1977)　　SEED
- AES(2000)　　ARIA

1960년대	컴퓨터와 통신 시스템의 발달로 디지털 형태 자료의 보호 및 보안 서비스 제공 필요성 증가
1970년대	IBM의 Horst Feistel이 개발을 시작해서 1977년에 미국 표준 암호화 알고리즘으로 채택된 비밀키 암호법 DES 탄생
1976년	Diffie와 Hellman, Paper – New Directions in Cryptography(Link), 공개키 암호법 제안
1978년	Rivest, Shmir, Adleman이 최초의 공개키 암호화 알고리즘 RSA 연구 (2002년 튜링상 수상)
1985	Taher Elgamal, 공개키 암호화 알고리즘인 ElGamal 암호 개발

1.3 암호 방식

❖ 암호의 분류

- 관용 암호 방식(conventional cryptography)
  - 공통키 암호 방식
  - 대칭 암호 방식
- 공개키 암호 방식(public-key cryptography)
  - 비대칭 암호 방식
  - Two key 암호 방식

1.3 암호 방식

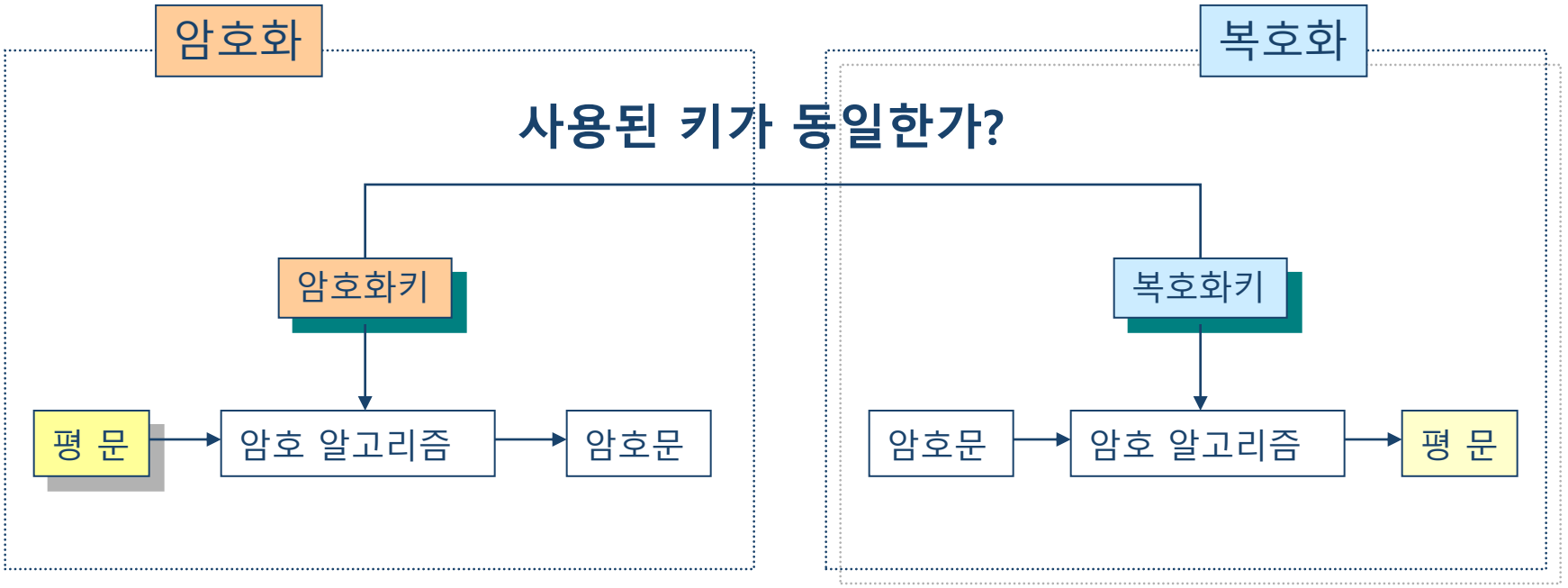
❖ 현대암호

[관용암호방식]

[공개키암호방식]

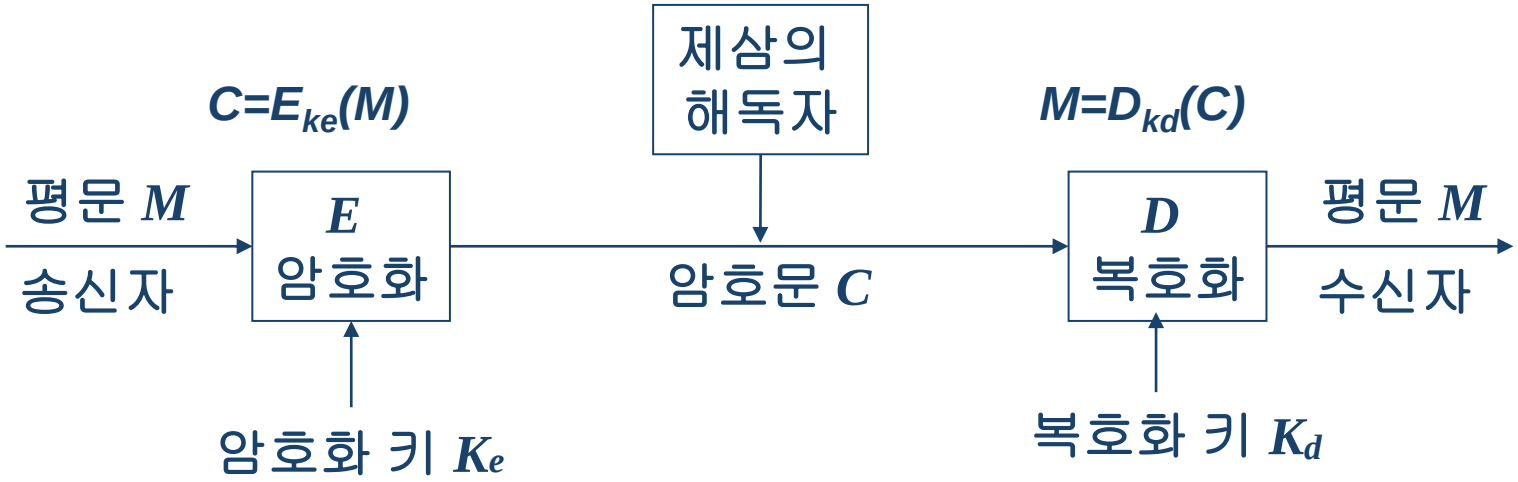
YES! 사용된 키가 동일하다.

NO! 사용된 키가 동일하지 않다.



1.3 암호 방식

❖ 암호 방식



- M : 평문
- C : 암호문
- E : 암호화 알고리즘
- D : 복호화 알고리즘

- $E_{ke}(M) = C$
- $D_{kd}(C) = M$
- $D_{kd}(E_{ke}(M)) = M$
- $D_{kd}E_{ke} = 1$

연습문제

1. 정보화사회에서의 암호학의 필요성에 대하여 설명하라.
2. Cryptography와 steganography의 차이점에 대하여 설명하라.
3. 관용 암호방식과 공개키 암호방식의 근본적인 차이점에 대하여 생각해 보고, 각각의 장단점을 설명하라.
4. 시프트(환자)암호를 사용했다고 가정할 때 다음 암호문을 해독하라.

   암호문 : PRGHUQ FUBSWRORJB

5. 키를 분배하는 방법에 있어서 관용암호방식과 공개키 암호방식이 어떻게 다른지 설명하라.