암호인재 인력양성 1차 교육

정보컴퓨터공학과 권혁동

한성대학교 HANSUNG UNIVERSITY

CryptoCraft LAB
https://crypto.modoo.at

Contents

CryptoCraft LAB

암호기술의 역사

- Cryptography의 어원은 그리스어로 hidden writing을 의미
- American Heritage 정의
  - The art or process of writing in or deciphering secret code
- Webster 정의
  - The science or study the techniques of secret writing
- 일반적인 의미
  - **기밀성과 인증을 제공하는 통신 채널을 제공하는 방법을 연구하는 과학**

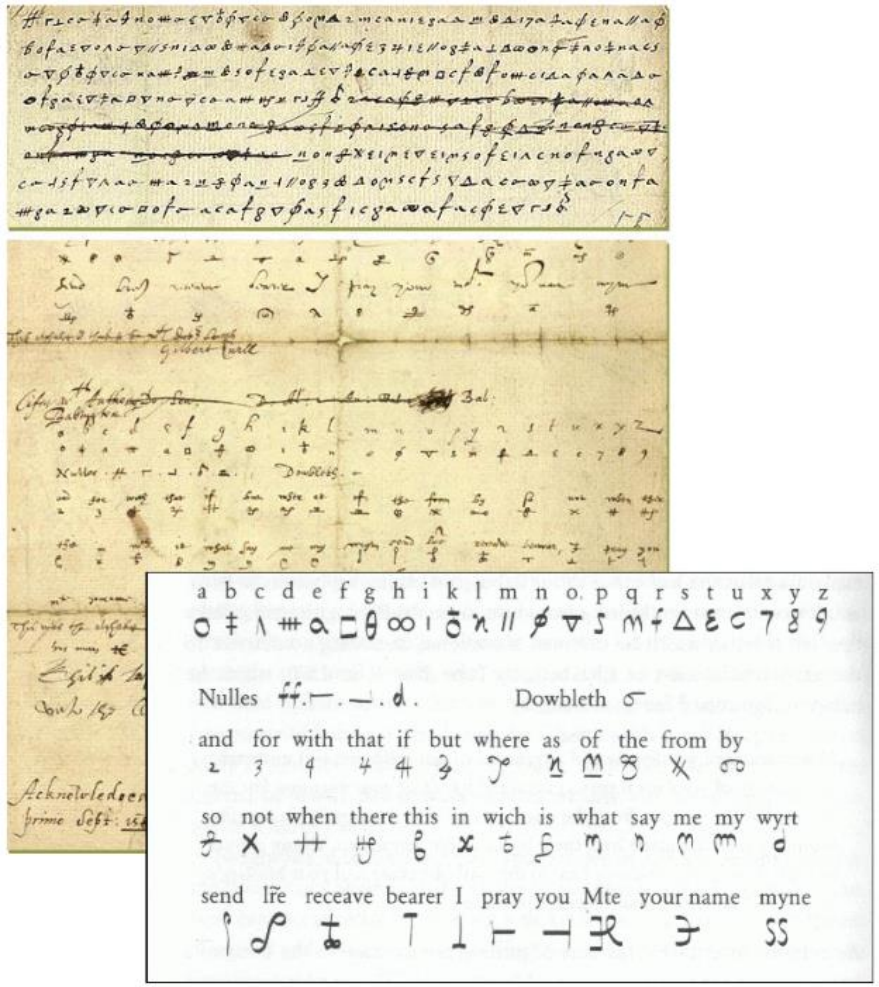
암호기술의 역사

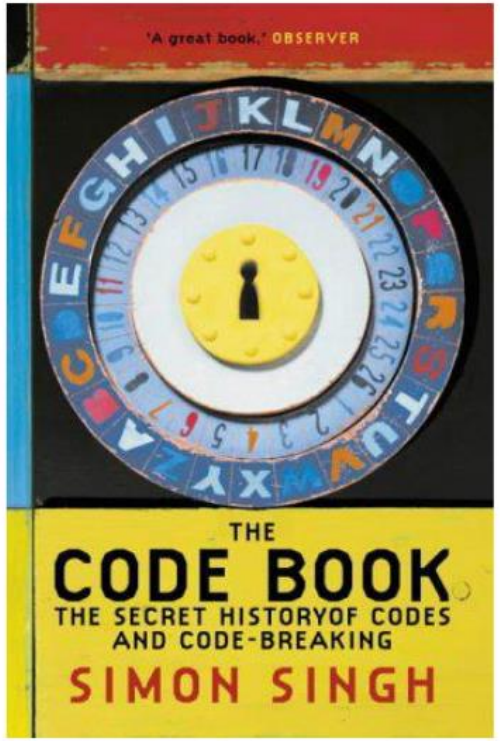
- Encryption(암호화)
  - Symmetric key encryption(비밀키 암호)
  - Asymmetric key encryption(공개키 암호)
- Authentication(인증)
  - Hash function(해시함수), Digital signature(디지털 서명), MAC(메시지 인증 코드)
- Key management(키 관리)
- Security protocols(보안 프로토콜)

암호기술의 역사

- 고전 암호: 암호방식 자체가 정보/키 역할
- 근대 암호: 기계장치에 의한 자동화
- 현대 암호: 컴퓨터를 이용한 정보처리, '키' 요소의 도입
  - Shannon의 정보이론 이후의 암호를 현대 암호로 분류

암호기술의 역사: 코드북


a b c d e f g h i k l m n o p q r s t u x y z
Nulles
Dowbleth
and for with that if but where as of the from by
so not when there this in wich is what say me my wyrt
send lre receave bearer I pray you Mte your name myne


'A great book.' OBSERVER
THE
CODE BOOK
THE SECRET HISTORYOF CODES AND CODE-BREAKING
SIMON SINGH

암호기술의 역사: Skytale

암호기술의 역사: General transposition

w	r	i	t	e
t	h	e	p	l
a	i	n	t	e
x	t	o	n	e
l	e	t	t	e

e	r	w	t	i
l	h	t	p	e
e	i	a	t	n
e	t	x	n	o
e	e	l	t	t

t	o	o	h	w
a	r	k	b	e
a	t	n	a	r
s	p	i	s	o
n	i	c	t	o

h	o	w	t	o
b	r	e	a	k
a	t	r	a	n
s	p	o	s	i
t	i	o	n	c

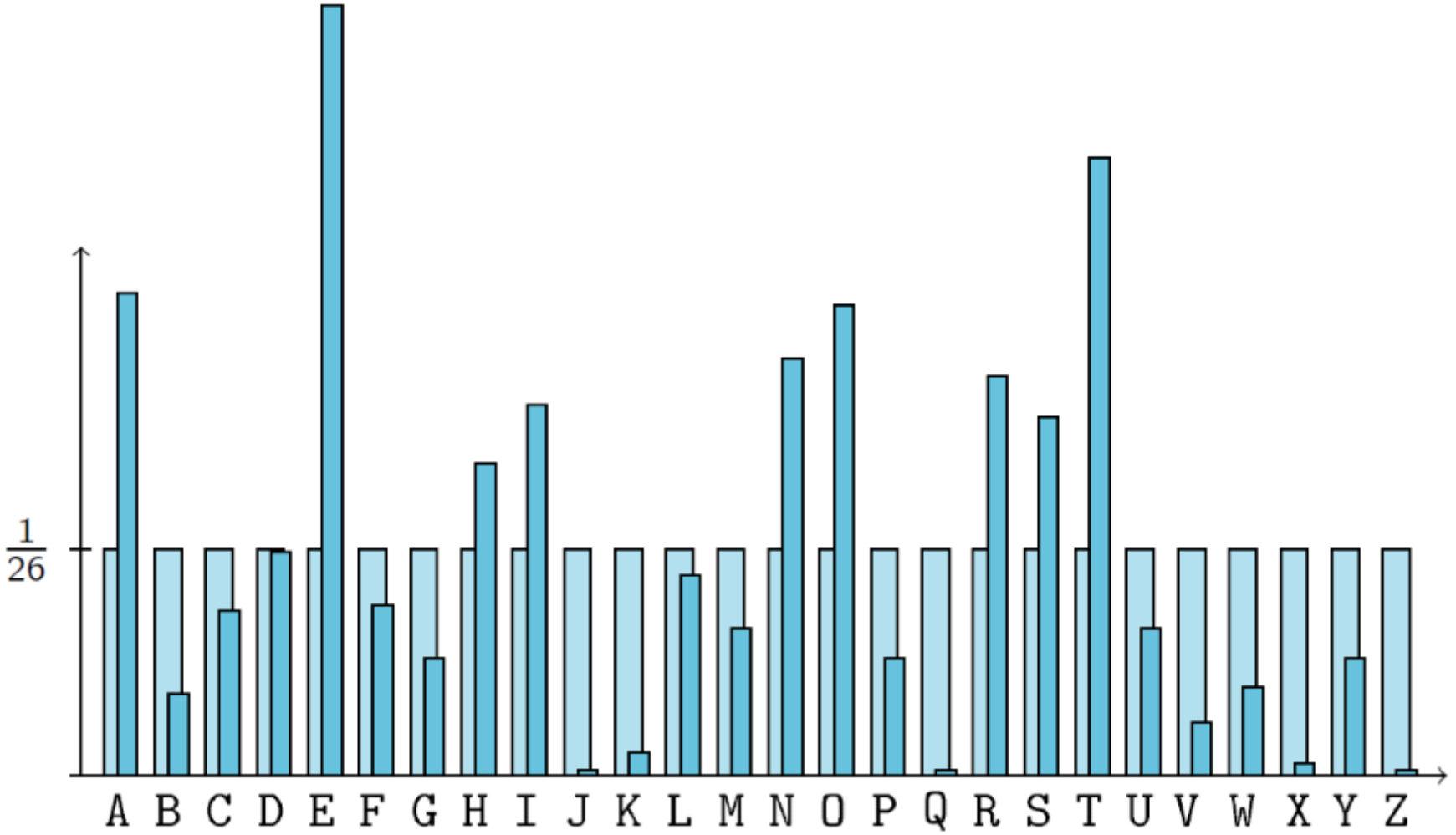
암호기술의 역사: Caesar Cipher

암호기술의 역사: Vigenere

```
makeastreamofkeylettersandusethemoneafteranother
keymakeastreamofkeylettersandusethemoneafteranot
weiqacxrwtdsfwsdvireikleevufhnzifvrqosxewtrftusk
```

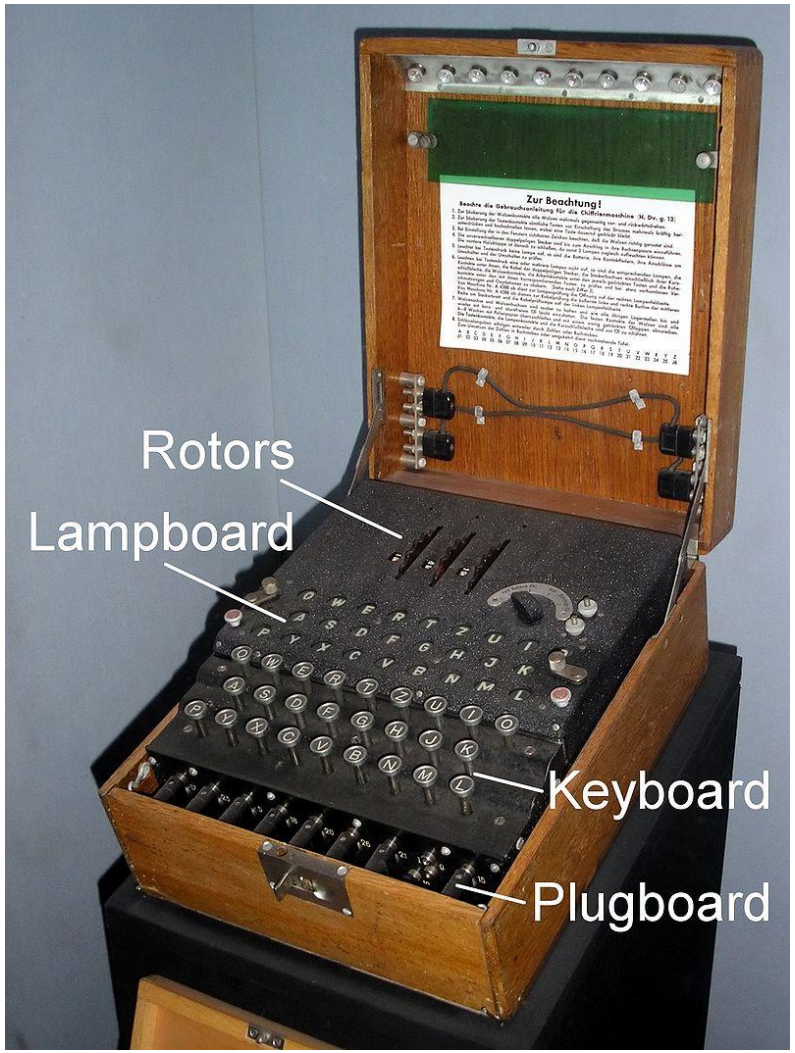
```
makeastreamofkeylettersandusethemoneafteranother
keykeykeykeykeykeykeykeykeykeykeykeykeykeykeykey
weioeqdvckqmpocipcdxcbwyxhscirrikyrckjrovyxsrrip
```

암호기술의 역사: Vigenere



암호기술의 역사: Enigma

- Vigenere 암호와 비슷한 원리
- 폴란드 수학자 Marian Rejewski가 최초로 해석
  - 1932
- Alan Turing이 독일군의 암호를 해석
  - 2차 대전 중

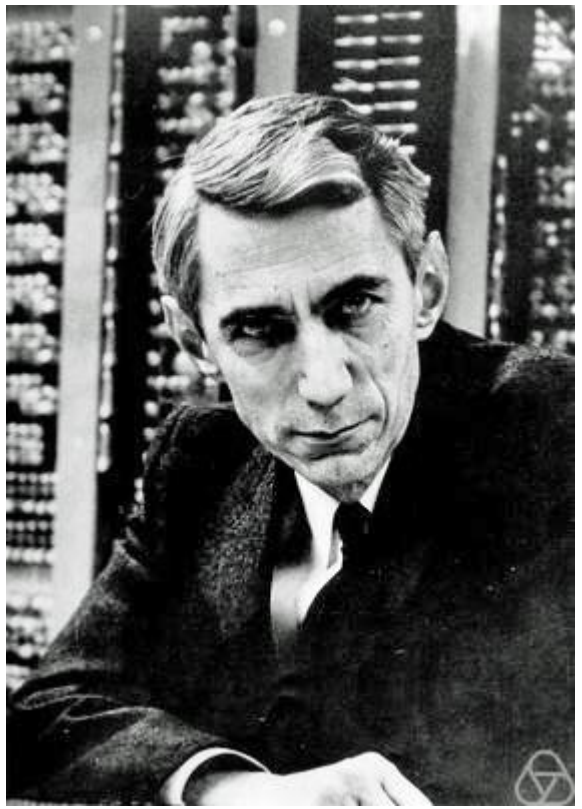


암호기술의 역사: Navajo code talkers

- 아메리카 대륙 원주민 나바호족으로 구성
- 암호통신병
- 2차 대전, 한국 전쟁에 참전
- **나바호족 언어가 복잡하고 유명하지 않음**
- 1968년 미국 정부가 존재를 인정
- 2000년 클린턴 행정부가 훈장 수여

암호기술의 역사: Shannon의 암호 이론

- 정보이론의 아버지, 암호학의 아버지
- Communication Theory of Secrecy System(1949)
  - 현대 암호와 증명 가능한 안전성의 개념을 정립
  - 정보이론을 확립
- 혼돈(Confusion)과 확산(Diffusion) 정의
- **블록암호의 설계 근간**



암호기술의 역사: Shannon의 암호 이론

- **완전 보안성 이론**

- $Pr_p(x|y) = Pr_p(x),\ \forall x \in P,\ y \in C$
  - 암호문 y가 주어질 때, 그에 대한 평문 x를 골라낼 확률
    = 무작위로 x를 선택할 확률

- $Pr_K(k) = \frac{1}{|k|},\ \forall k \in K,\ and\ \forall x \in P,\ y \in C,\ \nexists k \in K\ such\ that\ e_k(x) = y$
  - '키 공간 = 평문 공간 = 암호문 공간' 시스템이 완전 보안성을 가질 필요충분조건
  - 키는 무작위로 선택하고 서로 다른 키가 같은 평문을 같은 암호문으로 변환하지 않음

암호기술의 역사: Shannon의 암호 이론

- 완전보안성을 가지지 않은 암호 시스템의 경우,

  이를 깨뜨리는 방법이 일정 수준 이상의 노력이 필요하다 가정하면,

  이것을 어떻게 보장할 수 있는 것인가?

- **방법1: 모든 알려진 공격 방법에 대해 많은 자원 소모가 필요함을 입증**
  - 소비되는 자원, 계산에 드는 노력 등
- **방법2: 알려진 매우 어려운 문제로 환원(reduction)이 가능함을 입증**
- 1은 주로 비밀키, 2는 주로 공개키 암호에서 사용

암호기술의 역사: Shannon의 암호 이론

- 혼돈과 확산을 반복하면 암호를 안전하게 구성할 수 있음
- 혼돈: 암호문의 통계량은 평문에 영향을 받지만,

  공격자가 활용할 수 없을 정도로 복잡해야 함 -> 대치(substitution)
- 확산: 평문의 각 비트와 키의 각 비트는

  암호문의 많은 비트에 영향을 주어야 함 -> 변환(permutation)

암호기술의 역사: 현대 암호

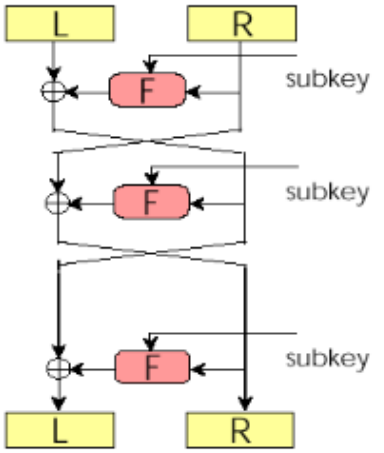
- 고대 암호는 암호화 방식(알고리즘)만 알면 복호화 가능
- 근대 암호는 초기 설정값을 알면 획득 가능
  - 에니그마의 경우, 최대 200만개, 컴퓨터로 전수조사 가능
- **현대 암호는 암호화 방식(알고리즘)과 초기 설정값(키)를 활용**
  - 에니그마와 유사

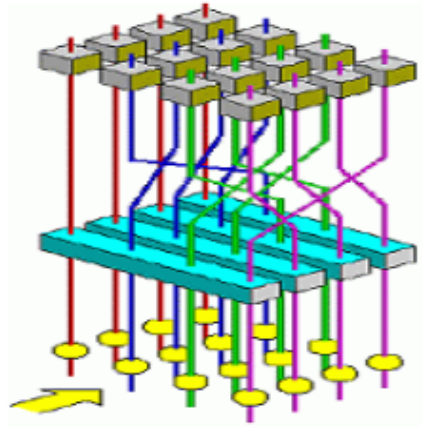
암호기술의 역사: 현대 암호

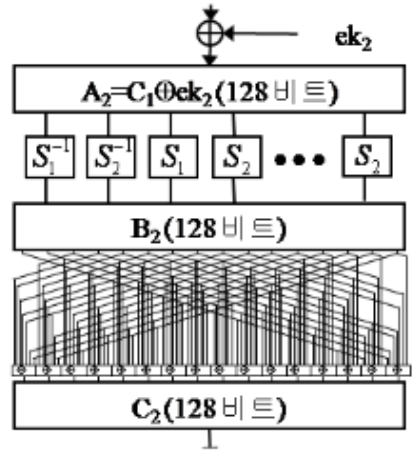
- 현대암호의 특징
  - 컴퓨터로 전수조사가 불가능할 정도로 큰 키 크기
  - 체계적인 키 관리 방식이 필요하여 공개키 암호의 등장
- 컴퓨터의 발전에 따라 키의 크기가 점점 커짐
  - DES(1977) -> 56비트
  - AES(2000) -> 128, 192, 256비트

암호기술의 역사: 현대 암호

- DES(Data Encryption Standard)
  - IBM의 설계를 NSA가 완성, 1977년 미국 표준
- AES(Advanced Encryption Standard)
  - DES 한계를 타파하기 위해 1998년부터 국제 암호공모사업 추진
  - 2000년 벨기에 연구팀의 Rigndael이 선정
- SEED
  - 국내 민간암호기술 활성화를 위해 국보연 주도로 개발, 2005년 ISO 표준
- ARIA(Academy, Research Institute, Agency)
  - 전자정부 안전성 강화를 위해 국보연 주도로 개발
  - 2004년 KS 표준, 2008년 행정기관 VoIP 규격으로 선정







정보보호 서비스

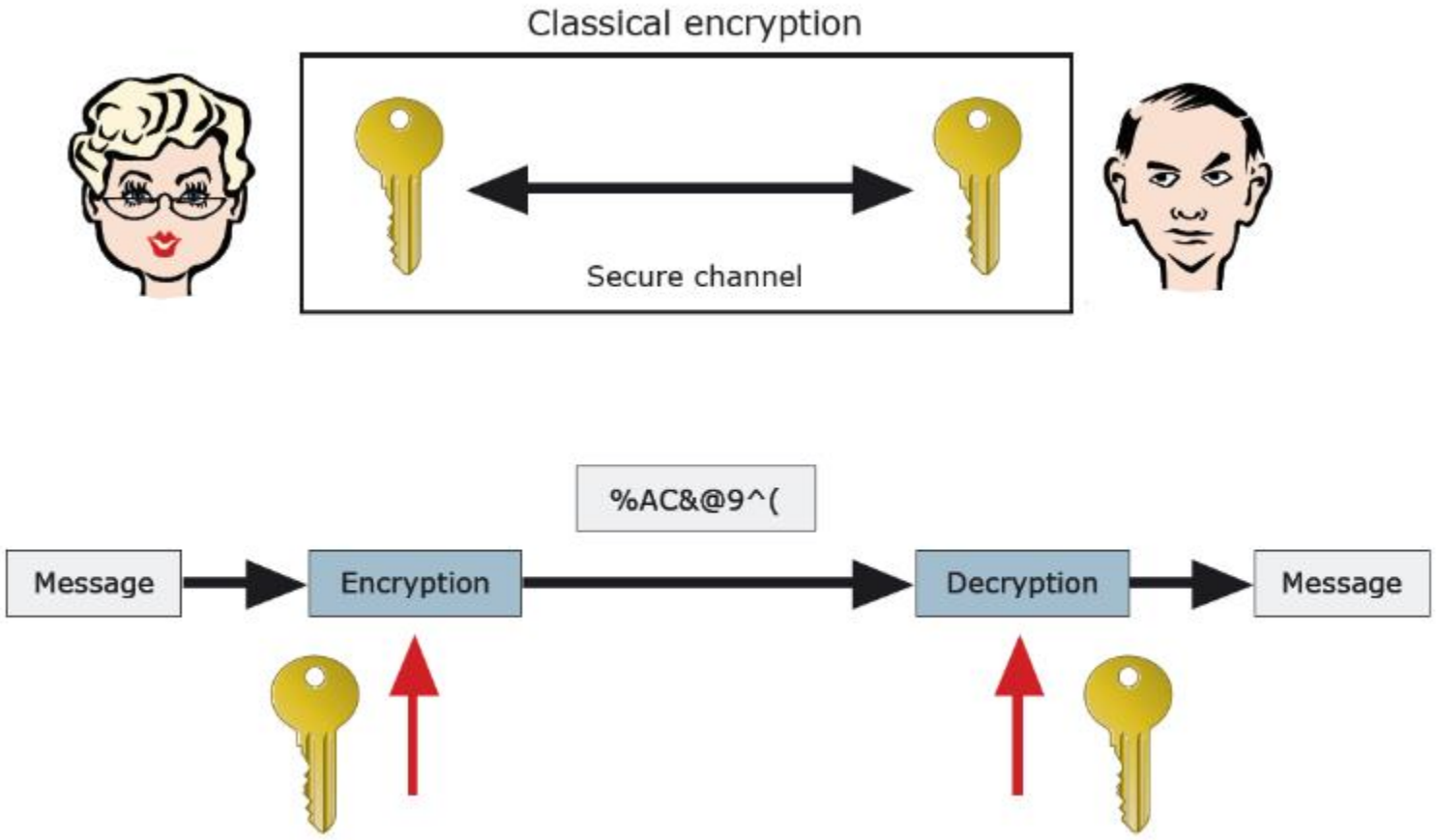
- **기밀성(Confidentiality)**
  - 정보가 의도하지 않게 **노출되지 않음**을 보장
- **무결성(Integrity)**
  - 공격자의 의도적인 공격에 **데이터가 위조 혹은 변조되지 않음**을 보장
- **인증(Authentication)**
  - 상대방의 **신원을 보증**할 수 있도록 함
- **부인방지(Non-repudiation)**
  - 송/수신자가 데이터를 보내거나 받은 **사실을 부인할 수 없도록** 함

정보보호 서비스

- 기밀성(Confidentiality)
  - 비밀키, 공개키 암호
- 무결성(Integrity)
  - 해시함수, MAC, 인증 암호화
- 인증(Authentication)
  - 패스워드, OTP, 토큰
- 부인방지(Non-repudiation)
  - 전자서명

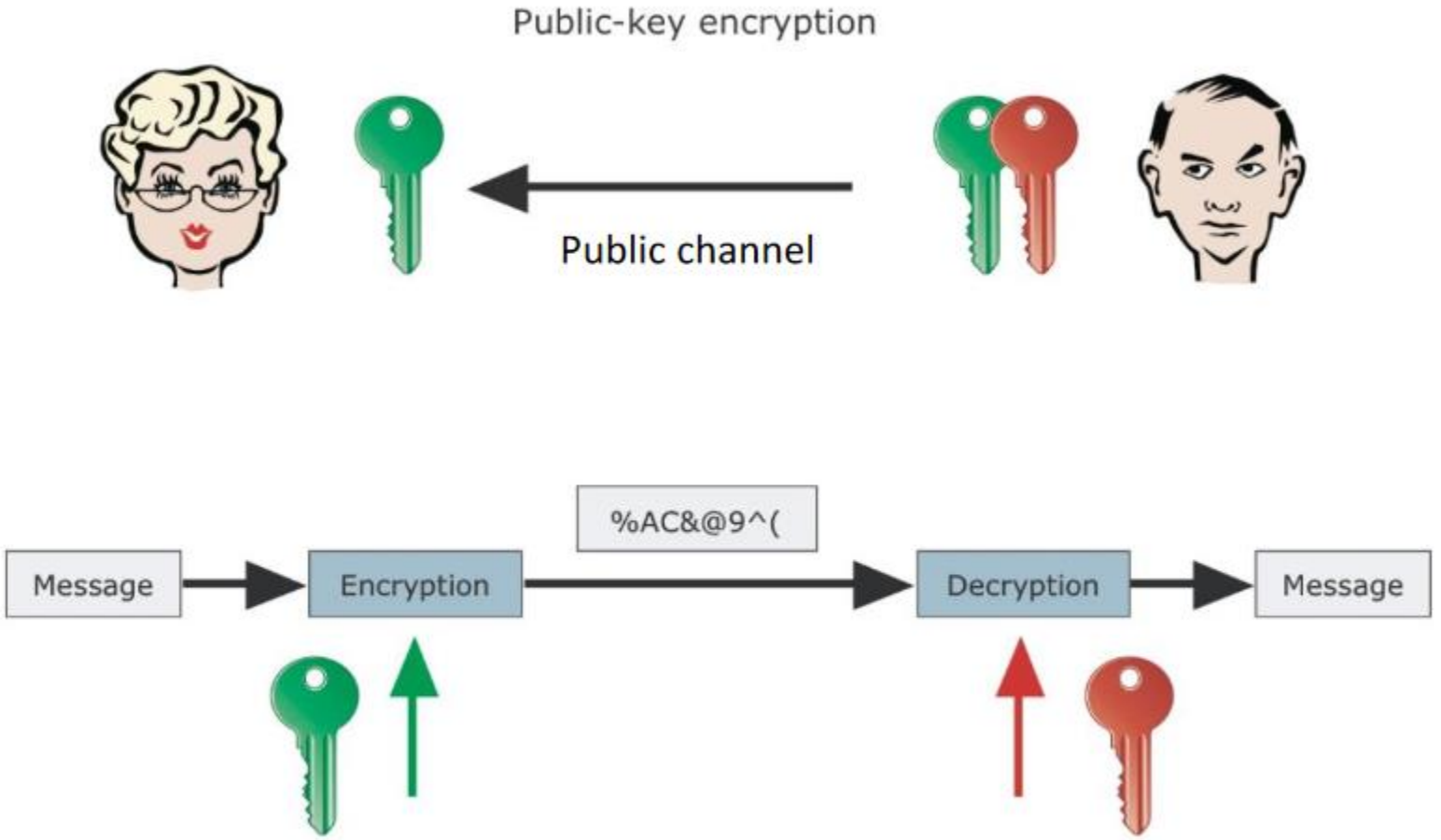
비밀키 암호와 공개키 암호

- 비밀키 암호



비밀키 암호와 공개키 암호

- 공개키 암호



비밀키 암호와 공개키 암호

	장점	단점
비밀키 암호	빠른 암호화	안전하지 않은 키 교환
공개키 암호	안전한 키 교환	느린 암호화
하이브리드 암호화 공개키 암호로 비밀키 암호화 비밀키 암호로 데이터 암호화	안전한 키 교환 빠른 암호화	?

비밀키 암호

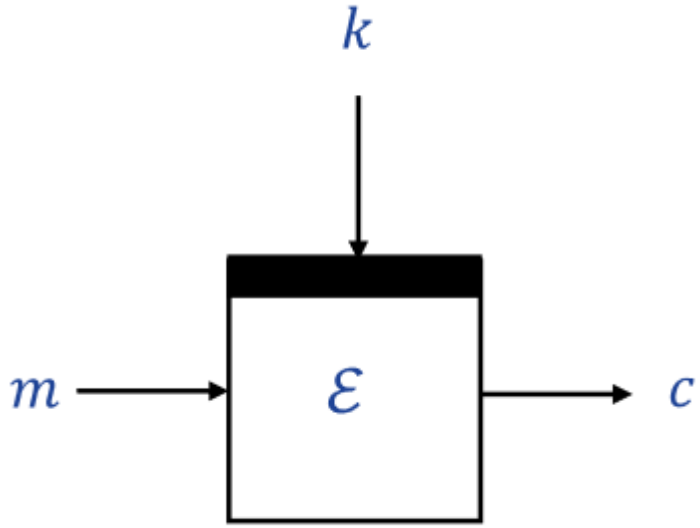
- Kerckhoffs' 원칙
  - 암호의 안전성은 알고리즘의 비밀성에 기반하지 않으며
    암호키의 비밀성에만 의존해야 함
  - 즉, 공격자는 키를 제외하고 모두 알 수 있다고 가정
- 공격자 시나리오
  - 암호문 단독 공격(Ciphertext only attack)
  - 알려진 평문 공격(Known plaintext attack)
  - 선택 평문/암호문 공격(Chosen plaintext/ciphertext attack)
  - **능동 선택 평문/암호문 공격(Adaptive chosen plaintext/ciphertext attack)**
    - **블랙박스 공격으로도 칭함**

비밀키 암호

- 블록암호
  - **일정 크기의 데이터**에 적용하는 알고리즘
  - 긴 길이의 암호화에는 블록암호를 여러 번 적용
    - **운용모드를 사용**
  - 내부 상태변수가 없거나 매우 적음
  - 많이 사용
- 스트림암호
  - 긴 난수열을 생성하여 평문과 비트단위로 XOR
  - 난수열 생성을 위해 큰 내부 상태변수 유지가 필요
  - 적게 사용

블록 암호

- $\forall k \in K, m \in P \; then \; d_k\big(e_k(m)\big) = m$
- $E: \{0,1\}^n \times \{0,1\}^k \rightarrow \{0,1\}^n, \;\; (\mathrm{m}, \mathrm{k}) \longmapsto c$
- $D: \{0,1\}^n \times \{0,1\}^k \rightarrow \{0,1\}^n, \;\; (\mathrm{c}, \mathrm{k}) \longmapsto m$
- 블록암호 기본 조건
  - 키 k가 있을 때, $E_k(m) = c$와 그 역인 $D_k(c) = m$의 계산이 쉬워야 함
  - 주어진 m과 c에 대해서, $E_k(m) = c$를 만족하는 k는 계산하기 어려워야 함
  - 고정된 m_0에 대해서 함수 $f(k) = \; e_k(m_0)$은 일방향 함수여야 함



블록 암호 분석

- 가정
  - 공격자는 대상 블록 암호의 **키를 제외한 모든 동작과정을 알고 있음**
  - 공격자는 대상 블록 암호에 비밀키 k를 사용한 **블랙박스 구현이 가능함**
- **목표**
  - 키 k를 찾기
  - 키 k에 $E_k(m) = c$를 만족하는 새로운 (m, c) 찾기
  - 대상 블록 암호가 랜덤 함수와 구별되는 특징을 찾아냄

블록 암호 분석

- Generic 공격

- **모든 블록암호에 대해서 성공 가능**

  - 전수조사 공격: 모든 가능한 키를 하나씩 대입

  - 테이블 공격: 모든 키 k에 대해서 $E_k(m_0)$저장

  - 코드북 공격: 키 k로 암호화 한 모든 평문/암호문 쌍을 수집

블록 암호 분석

- Short-cut 공격
- 암호 알고리즘의 설계에 따라 성공 여부가 다름
- **Generic 공격보다 효율적이여야 성공으로 판단**
  - Differential cryptanalysis, Linear cryptanalysis
  - Higher-order, Truncated, Impossible differential attack
  - Boomerang/Rectangle attack
  - Integral attack, Interpolation attack
  - …