알기 쉬운

정보보호개론 3판

흥미로운 암호 기술의 세계

INFORMATION SECURITY and CRYPTOGRAPHY

INFINITYBOOKS
인피니티북스

INFORMATION SECURITY and CRYPTOGRAPHY

CHAPTER 2 암호의 세계

Section 01
암호

1.1 암호에서 사용하는 이름

1.2 송신자/수신자/도청자

1.3 암호화와 복호화

1.4 암호의 기밀성

1.5 해독

1.1 암호에서 사용하는 이름

앨리스와 밥 _Alice and Bob

일반적으로 앨리스는 메시지를 전송하고 밥이 수신하는 모델에 사용된다. 이 이름은 나중에 등장하게 될 비대칭 암호 시스템인 RSA를 만든 사람 중의 하나인 Ron Rivest가 1978년에 처음으로 사용하였다.

이브 _Eve

영어로 도청자(eavesdropper)는 소극적인 공격자를 의미한다. 이브는 앨리스와 밥 사이에 이루어지는 통신을 도청하기는 하지만 통신 중인 메시지를 수정하지는 못한다. 나중에 다루게 될 양자 암호에서 이브는 통신 환경을 나타내기도 한다.

맬로리 _Mallory

영어로 악의를 가진(malicious) 공격자를 의미한다. 이브와는 다르게 맬로리는 메시지를 수정하고, 자신의 메시지로 대체하여 이전의 메시지를 재전송할 수 있는 능력 등을 가지고 있다. 이브의 공격을 막는 것보다 맬로리의 공격을 막는 것이 훨씬 더 어렵다. 종종 Marvin이나 Mallet이라는 이름이 사용되기도 한다.

1.1 암호에서 사용하는 이름

트렌트 _Trent

영어로 신뢰할 수 있는 중재자(trusted arbitrator)이며, 중립적인 위치에 있는 제3자이다. 사용되는 프로토콜에 따라 그 역할이 달라진다.

빅터 _Victor

영어명은 verifier이며 Pat이나 Peggy라는 이름을 사용하기도 한다. 의도된 거래나 통신이 실제로 발생했다는 것을 검증할 때 등장한다.

그림 2-1 • 이 책에 나오는 주요 등장 인물

1.2 송신자 · 수신자 · 도청자

그림 2-2 • 앨리스가 밥에게 메일 보내기(송신자/수신자)

1.2 송신자 · 수신자 · 도청자

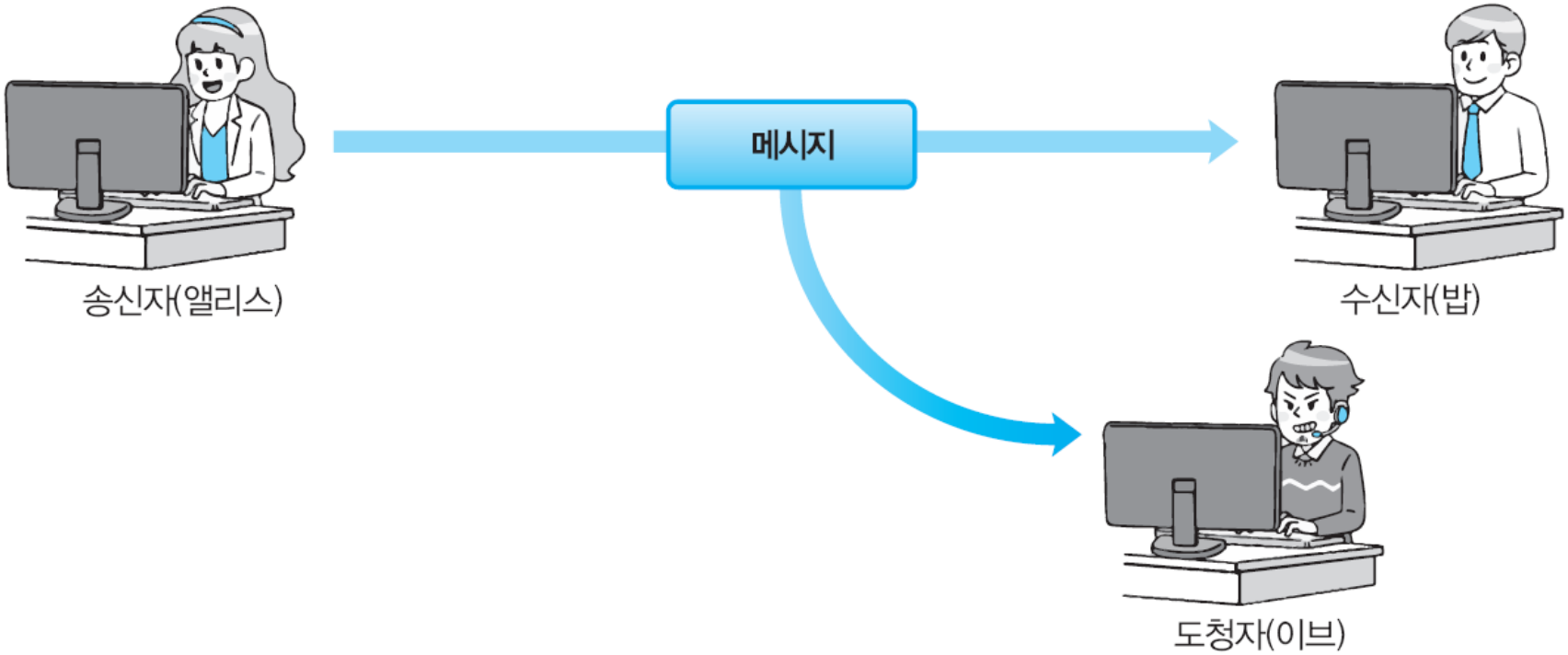


그림 2-3 • 이브의 메일 도청(도청자)

1.2 송신자 · 수신자 · 도청자

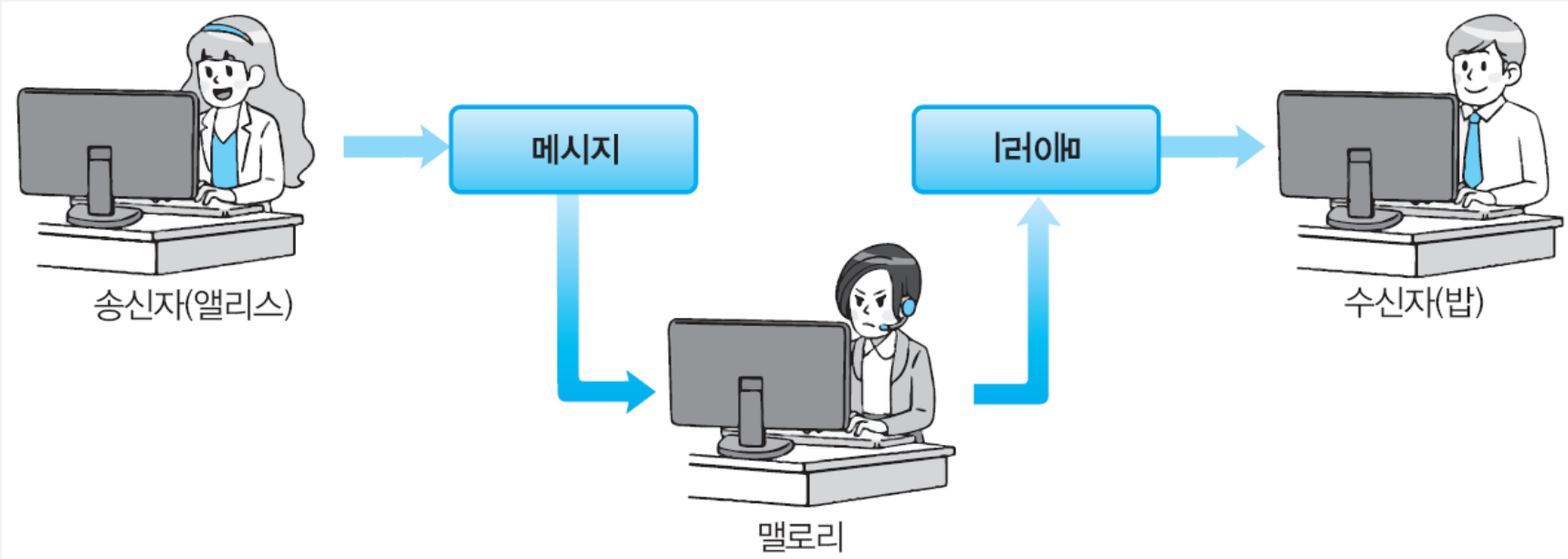


그림 2-4 • 맬로리의 메일 수정

1.3 암호화와 복호화

- 평문(plaintext)
  - 암호화하기 전의 메시지
- 암호문(ciphertext)
  - 암호화한 후의 메시지
- 암호기술
  - 중간에서 도청자가 암호문을 가로채어 갖게 된다고 하더라고 특정 비밀값을 모른다면 암호문을 평문으로 복호화 할 수 없도록 하는 기술

암호화 과정

칼럼 **복호와 복호화**

암호문을 평문으로 변환하는 과정을 「복호화한다」라기 보다 「복호한다」라고 하는 편이 더 적절해 보인다. 하지만 평문을 암호문으로 변환하는 과정을 「암호한다」라고는 하지 않는다. 결국 암호와 복호라는 용어는 비대칭성이 있다. 이 책에서는 「암호화」와 「복호화」글자의 대칭성을 고려해서 「복호화」라는 표현으로 통일하기로 한다.

그림 2-5 • 암호화 과정

복호화 과정

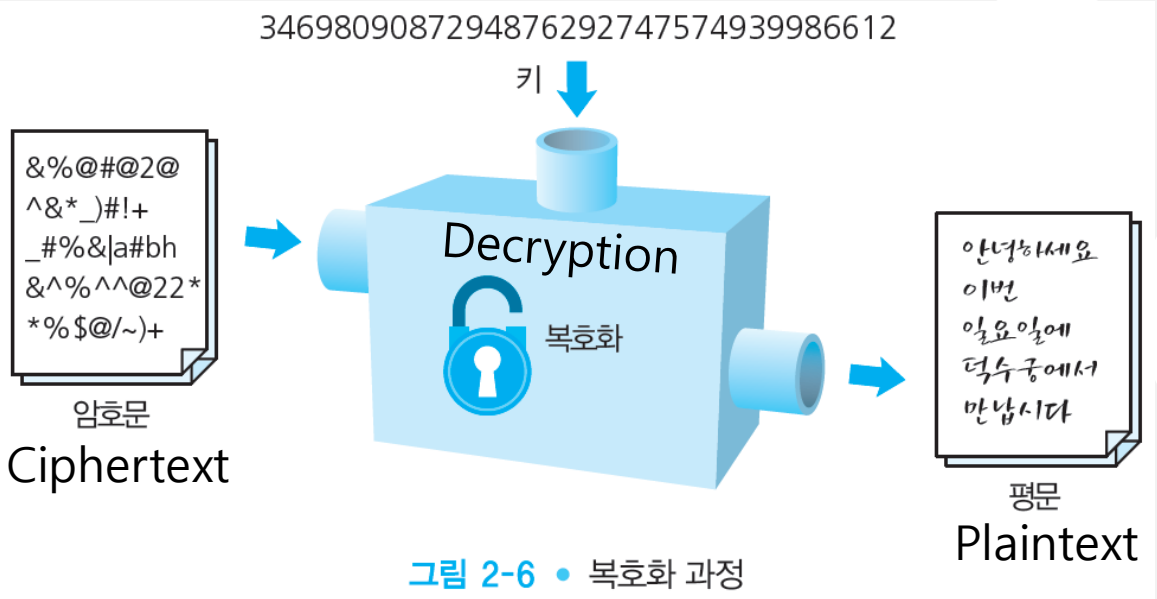


그림 2-6 • 복호화 과정

암호문

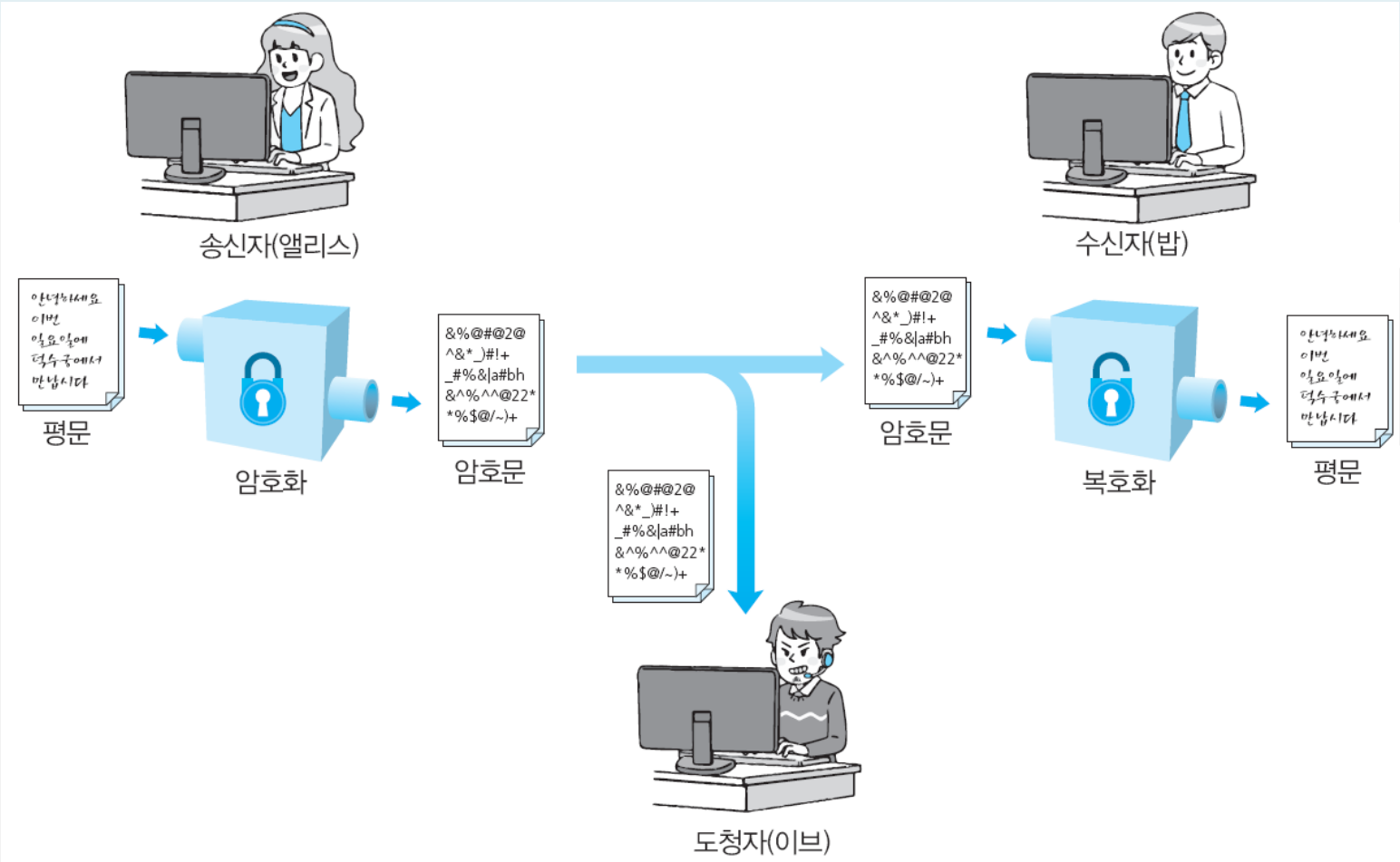


그림 2-7 • 도청자가 보는 것은 암호문뿐이다

1.4 암호의 기밀성

- 메일의 기밀성 (confidentiality, 또는 비밀성)
  - 앨리스와 밥은 암호(cryptography) 기술을 사용해서 메일의 내용을 비밀로 유지

1.5 해독

- 복호화
  - 정당한 수신자가 암호문을 평문으로 바꾸는 것
- 암호 해독(cryptanalysis)
  - 수신자 이외의 사람이 암호문으로부터 평문을 복원하려고 시도하는 것
- 암호 해독자(cryptanalyst)
  - 암호 해독을 하는 사람
    - 나쁜 의도를 가진 자
    - 암호 연구자

Quiz 1 일기의 암호

- 앨리스는 매일 워드 프로세서로 일기를 쓴다. 누군가가 읽지 못하게 하기 위해 디스크에 저장할 때는 매번 암호화를 하고 있다. 일기를 다시 읽고 싶을 때는 그때마다 복호화를 하고 있다.

  이 경우 송신자와 수신자는 각각 누구인가?

Section 02
암호화와 복호화의 기호 표현

2.1 암호 시스템의 요소

2.2 암호 시스템의 기호 표현

2.1 암호 시스템의 요소

- 평문(plaintext)
- 암호문(ciphertext)
- 암호 알고리즘(encryption algorithm)
- 복호 알고리즘(decryption algorithm)
- 키(key)

2.2 암호 시스템의 기호 표현

- $C = E_K(P)$:
  - 평문 P를 키 K로 암호화하여(E) 암호문 C를 얻음
- $P = D_K(C)$:
  - 암호문 C를 키 K로 복호화하여(D) 평문 P를 얻음

- 다른 표현
  - $C = E_K(P) = E(K, P)$
  - $P = D_K(C) = D(K, C)$

암호화와 복호화

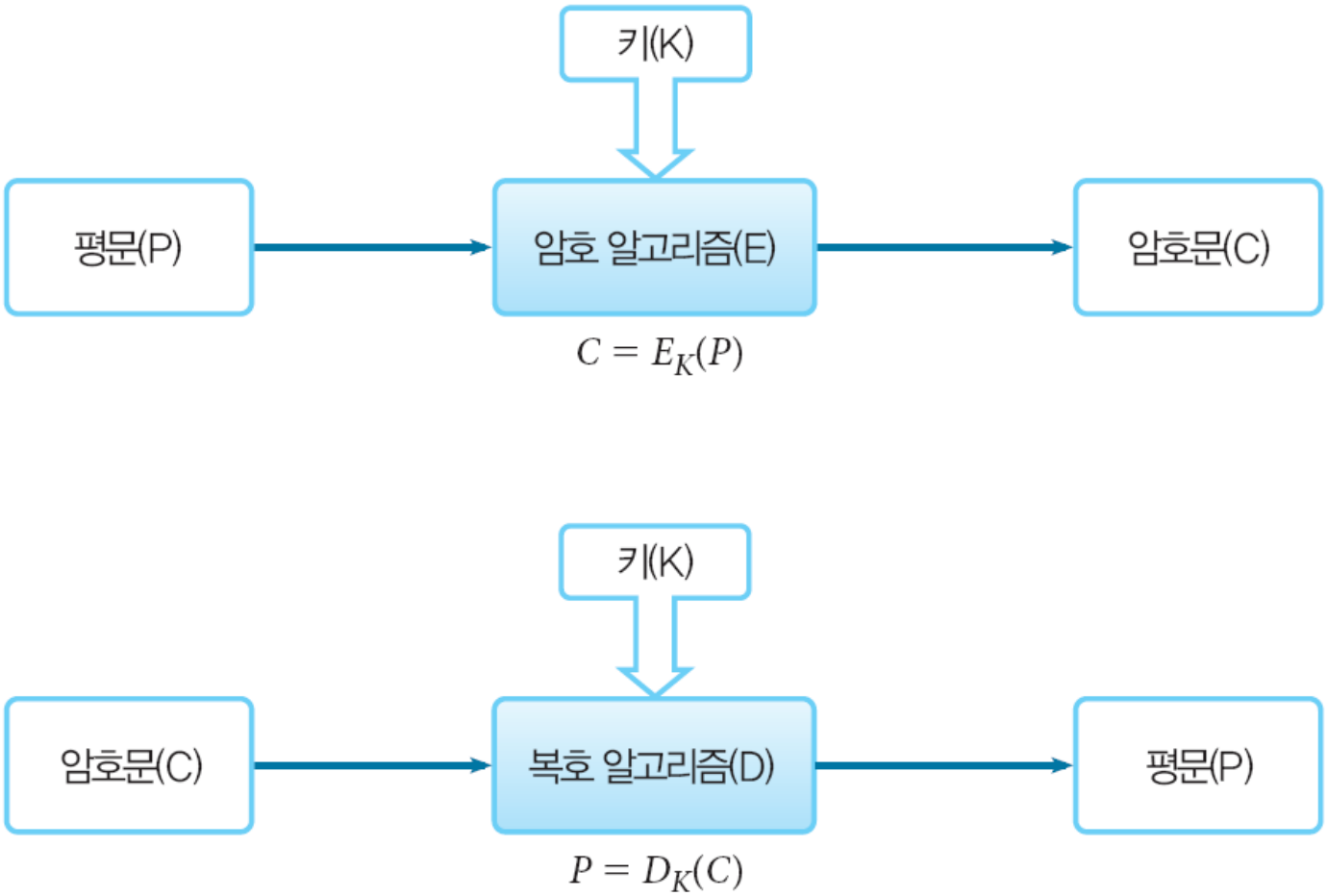


그림 2-8 • 암호화와 복호화

Section 03
대칭 암호와 공개 키 암호

3.1 암호 알고리즘

3.2 키

3.3 대칭 암호와 비대칭 암호

3.4 하이브리드 암호 시스템

3.1 암호 알고리즘

- 암호화 알고리즘
  - 평문을 암호문으로 만드는 절차
- 복호화 알고리즘
  - 암호문을 평문으로 만드는 절차
- 암호 알고리즘
  - 암호화와 복호화 알고리즘을 합한 알고리즘

3.2 키

- 암호 알고리즘의 키는 다음과 같은 매우 긴 숫자

  203554728568477650354673080689430768

- 2진화된 숫자로 변경하여 사용
- 암호 키의 안전
- 금고의 키가 금고 안의 귀중품을 지켜주는 것과 같음

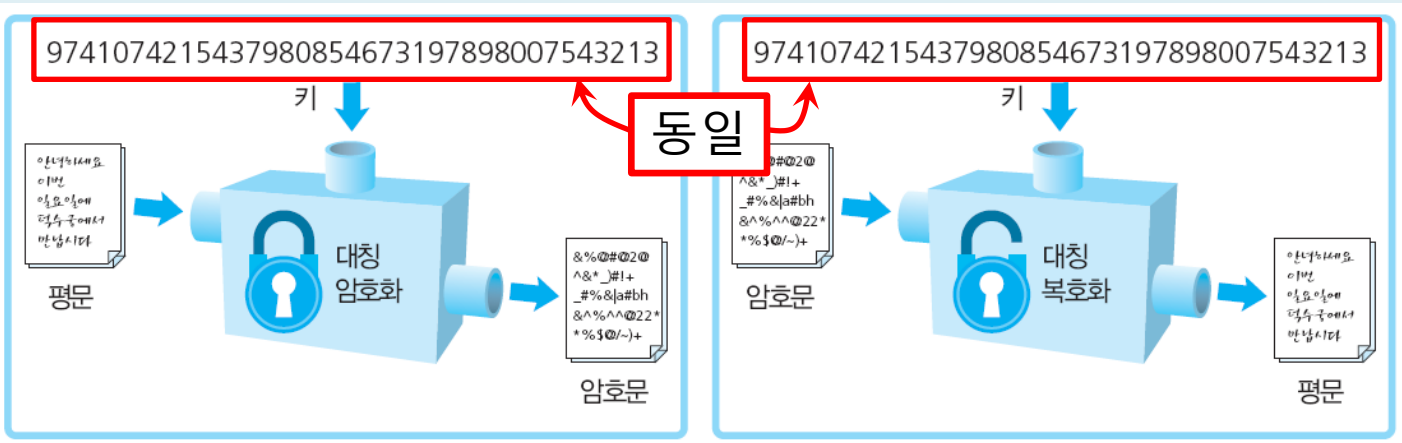
3.3 대칭 암호와 비대칭 암호

- **대칭 암호(symmetric cryptography)**
  - 암호화를 할 때 사용하는 키와 복호화 할 때 사용하는 키가 동일한 암호알고리즘
- **비대칭 암호(asymmetric cryptography)**
  - 암호화를 할 때 사용하는 키와 복호화를 할 때 사용하는 키가 서로 다른 암호알고리즘

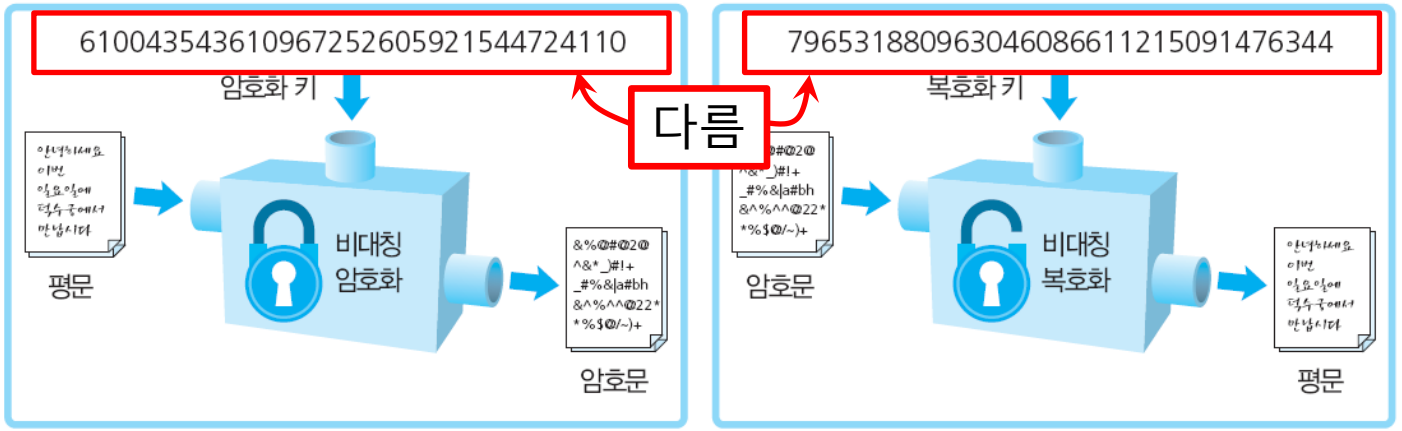
비대칭 암호

- 비대칭 암호 요소
  - 송신자: 한 쌍의 키
  - 수신자: 한 쌍의 키
    - 이 한 쌍의 키: (공개키, 개인키)
      - 이 두 개의 키는 수학적으로 밀접한 연관
- 공개키 암호(public-key cryptography)
  - 공개키는 공개를 하므로 이 암호 알고리즘을 공개키 암호라 함
  - 비대칭 암호 보다 공개키 암호라는 용어를 자주 사용
  - 1970년에 발명되었으며 현재 공개키 암호를 많이 사용

대칭암호와 비대칭 암호



(a) **대칭 암호:** 암호화와 복호화에 동일한 키를 사용



(b) **비대칭 암호:** 암호화와 복호화에 서로 다른 키를 사용

그림 2-9 • 대칭 암호와 비대칭 암호

3.4 하이브리드 암호 시스템

- 하이브리드 암호 시스템
  (hybrid cryptosystem)
  - 대칭 암호와 공개 키 암호를 조합한 암호방식
  - 대칭 암호와 공개키 암호의 장점을 조합

Section 04
그 밖의 암호 기술

4.1 일방향 해시 함수

4.2 메시지 인증 코드

4.3 디지털 서명

4.4 의사난수 생성기

4.1 일방향 해시 함수(I)

- 해시값이란 일방향 해시함수(one-way hash function)를 사용하여 계산한 값
- 문서의 기밀성이 아니라 무결성(integrity) 점검
- 기밀성 : 정보가 유출되지 않았음을 확인
- 무결성 : 정보가 변경되지 않았음을 확인

4.1 일방향 해시 함수(II)

- 정보나 소프트웨어를 공개적으로 제공할 때 변경되지 않았음을 확인하도록 프로그램의 해시값을 공개하는 경우가 있음
- 소프트웨어를 다운하고 같이 공개된 해시값을 이용하여 계산한 후 원본 임을 확인
- 무결성 : 수신한 데이터가 웹사이트에 있는 원래의 데이터와 동일함을 의미

4.2 메시지 인증 코드

- 메시지 인증 코드(message authentication code)
  - 메시지가 생각했던 통신 상대로부터 온 것임을 확인하는 코드
  - 메시지가 전송 도중 변경되지 않았다는 것도 확인함
  - 무결성과 인증을 제공

4.3 디지털 서명(I)

- 디지털 서명(digital signature)
  - 거짓 행세, 변경, 부인같은 위협을 방지하는 기술
  - 예 : 사업하는 밥이 앨리스로 부터 "상품을 1000만원에 구입하겠다 " 고 하는 전자메일을 받았을 때 앨리스가 보낸 것인지를 확인하기 위해 디지털 서명이 필요함
- 부인(repudiation)
  - 통신 사실을 나중에 아니라고 하는 것
  - 예 : 메일을 보낸 앨리스가 마음이 바뀌어 앨리스가 보낸 것이 아니라고 하는 행위

4.3 디지털 서명(II)

- 검증(verify)
  - 예 : 앨리스가 디지털 서명을 하여 “상품을 1000만원에 구입하겠다 " 고 메일을 보내면 밥은 디지털 서명을 검증함
- 디지털 서명 : 무결성, 인증, 부인방지

4.4 의사 난수 생성기

- 의사 난수 생성(pseudo random number generator; PRNG)는 난수열을 생성하는 알고리즘
  - 키(key generation) 생성의 역할
  - 예: SSL/TLS통신할 때 사용할 세션키(Session key)를 생성하는데 의사 난수 생성기 이용
  - 만일 난수 생성 알고리즘이 취약할 경우 도청자가 키 값을 추측할 수 있으므로 통신의 기밀성이 손상될 수 있음

Section 05
암호학자의 도구 상자

- 암호학자의 도구상자(cryptographer's toolbox)
  - 대칭 암호
  - 공개 키 암호
  - 일방향 해시함수
  - 메시지 인증 코드
  - 디지털 서명
  - 의사난수 생성기

보안 위협과 암호 기술에 의한 방지

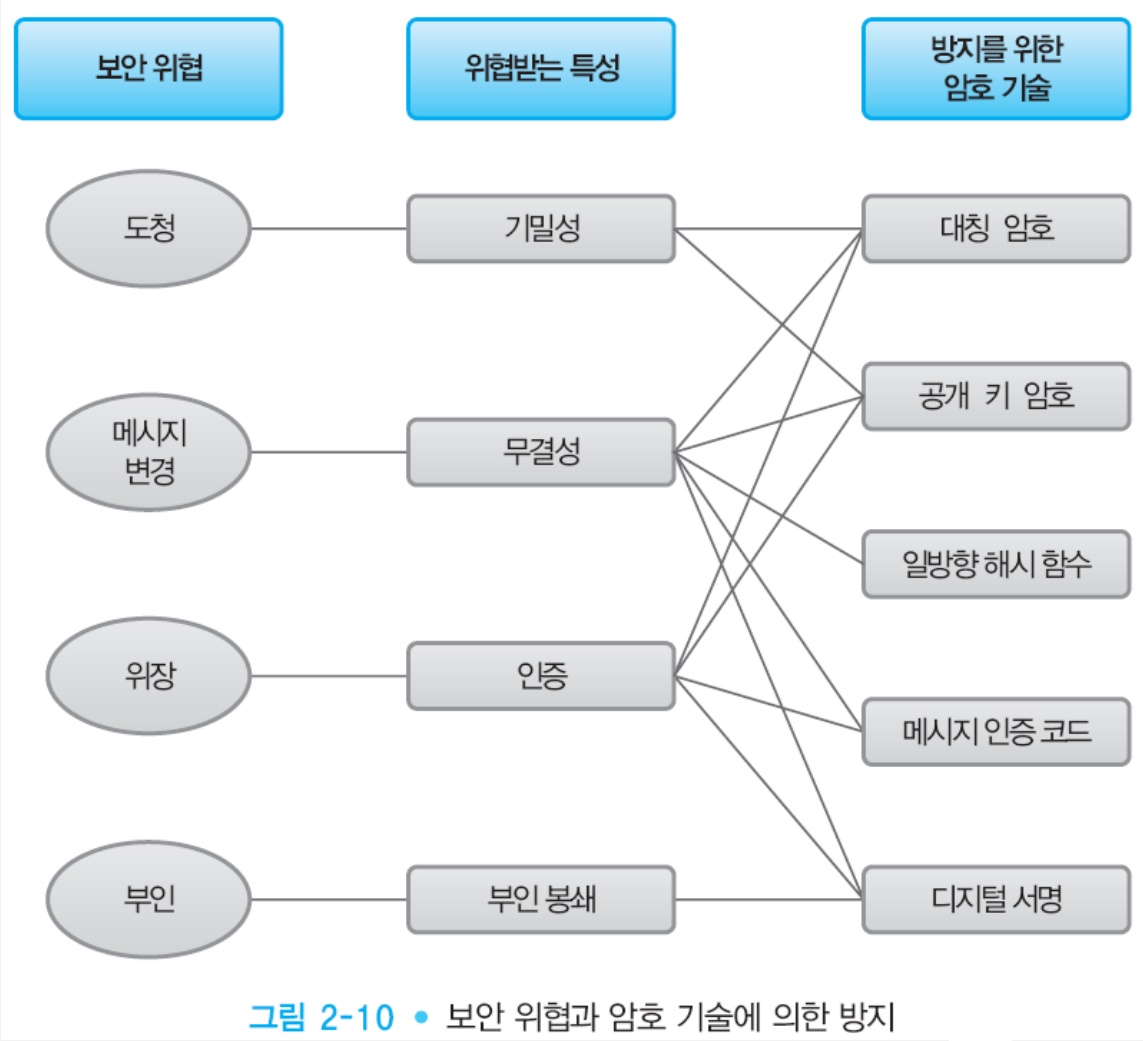


그림 2-10 • 보안 위협과 암호 기술에 의한 방지

Section 06

스테가노그래피와 디지털 워터마킹

- 크립토그래피(cryptography)
  - 메시지의 내용을 읽지 못하게 하는 기법
- 스테가노그래피(steganography)
  - 메시지의 내용을 읽지 못하게 하는 것이 아니라, 메시지의 존재 자체를 숨기는 기법
  - 메시지를 숨겨 넣는 방법을 알게 되면 메시지의 내용은 금방 노출

스테가노그래피 예

- 서로 믿을 수 있는 친구를 만나는 일은 즐겁습니다.
- 울적한 날에도 기분을 좋게 합니다.
- 역시 좋은 친구는 삶의 활력소 입니다.
- 열심히 사는 사람들도
- 시간이 없다는 핑계로 친구를 멀리하기도 합니다. 하지만
- 반드시 우리가 소중하게 생각해야 하는 것이 친구입니다.

디지털 워터마킹

- 디지털 워터마킹(digital watermarking)
  - 파일 중에 저작권자나 구입자의 정보를 집어넣는 기술
- 디지털 워터마킹 기술에 스테가노그래피 사용
  - 암호문을 화상 파일 속에 숨김

Section 07
암호와 보안 상식

7.1 비밀 암호 알고리즘을 사용하지 말 것

7.2 약한 암호는 암호화 하지 않는 것보다 위험

7.3 어떤 암호라도 언젠가는 해독된다

7.4 암호는 보안의 아주 작은 부분

7.1 비밀 암호 알고리즘을 사용하지 말 것

- 비밀 암호 알고리즘을 만들어서 사용할 것이 아니라, 공개되어 있는 강한 암호 알고리즘을 사용해야 함
  - 암호알고리즘의 비밀은 반드시 폭로됨
    - 1999년 DVD 암호알고리즘 폭로
    - 2007년 NXP의 비접촉형 IC카드 MIFARE Classic 암호알고리즘 해석
    - 익명의 개인이 RSA사의 RC4와 호완성있는 프로그램 공개
  - 강한 암호 알고리즘을 만드는 것은 매우 어려움

숨기는 것에 의한 보안

- **숨기는 것에 의한 보안**(security by obscurity)
  - 암호 알고리즘을 비밀로 해서 보안을 유지하려고 하는 행위
  - 전문가가 볼 때 위험하고, 어리석은 행위로 간주
  - 강한 알고리즘을 만들기 위해 전문가들이 협력하여 경쟁 방식을 통해 선정
    - 대칭 알고리즘 AES
    - 일방향 해시 함수 알고리즘 SHA-3

7.2 약한 암호는 암호화 하지 않는 것보다 위험

- 사용자는 암호의 강도와는 상관없이 '암호화 되어 있다'는 사실만으로 안심하는 경향이 있는데 위험한 생각임
  - 16세기 스코틀랜드 여왕 Mary 가 엘리자베드 여왕 암살계획을 세웠으나 노출되어 처형됨
  - 스마트 기기의 유료 앱도 안전하지 않을 수 있음
- 약한 암호를 사용하려면, 처음부터 암호 따위를 사용하지 않는 것이 나을 수 있음

7.3 어떤 암호라도 언젠가는 해독

- 모든 키를 하나도 빠짐없이 시도해 봄으로서 언젠가는 반드시 해독
- 암호문이 해독되기까지 시간과, 암호를 사용하여 지키고 싶은 평문의 가치와의 밸런스(tradeoff)가 중요

일회용 패드

- **일회용 패드**(one-time pad)
  - 절대로 해독되지 않는 암호 알고리즘
  - 현실적으로 활용하기에는 적합하지 않은 암호

7.4 암호는 보안의 아주 작은 부분

- 사회공학적인 공격 방법은 암호의 강도 그 자체와는 아무런 관계가 없음
  - 피싱(Phishing)
  - 트로이 목마
  - 키로거
- 보안 시스템의 강도는 보안 시스템을 구성하는 여러 링크 중 가장 약한 링크의 강도와 같음
  - 가장 약한 링크는 암호가 아니라 사람

8. 이 장의 정리

- Quiz 2 기초 지식의 확인(p 52)

(1) 평문을 암호문으로 변환하는 것을 암호화라고 한다.

(2) 평문은 사람이 읽는 데이터이고 암호문은 컴퓨터가 읽는 데이터이다.

(3) 메일 송신자(From:)난을 조사하면 그 메일의 송신자가 누구인지 정확하게 판단할 수 있다.

(4) 대칭암호에서는 암호화 키와 복호화 키가 같다.

(5) 공개되어 있는 암호 알고리즘은 악의적인 의도를 가진 자로부터 공격을 받기 쉽기 때문에 회사에서 자체 개발한 비밀 암호 알고리즘을 사용하는 것이 더 안전하다.