2010-1학기 현대암호학

1장 암호의 세계

박 종 혁

Tel: 970-6702
Email: jhpark1@snut.ac.kr

Thinking

- Cryptography ?
- Security ?

보안관련 국가기관, 자격증 등

- 국가정보원
- ETRI
- KISA
- 국가보안연구소
- 검찰청 사이버테러대응센터 / 사이버수사대
- 기무사
- 금융보안연구원
- 금융감독원

- CISA
- CISSP
- SIS

보안의 세부 연구 분야들

- 암호학/분석
- 대칭키/공개키연구
- 시스템
- 네트워크 / 인터넷(웹)
- 임베디드 / 하드웨어
- 멀티미디어
- 디지털 포렌식
- 개인정보보호(프라이버시)
- 정보보호 법률/정책
- 보안프로토콜

1.0 주요 내용

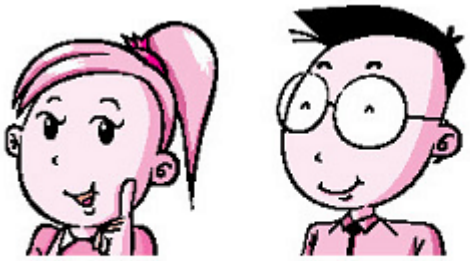
- 암호와 관련된 기술에는 여러 가지 많은 것들이 있는데, 이들은 서로 연관성을 가지고 있다.
- 암호 기술 내용에 대한 전반적인 내용을 공부한다

1.1 암호

1.1.1 암호에서 사용하는 이름

- 암호를 설명할 때에 정보를 주고/받는 사람이나 컴퓨터를 나타내는 이름으로 **앨리스(Alice)**와 **밥(Bob)**이라는 이름을 사용한다

주요 등장 인물



앨리스와 밥 _Alice and Bob

정보를 보내고/받는 사람

이브 _Eve

주고/받는 정보를 도청하는 사람

맬로리 _Mallory

능동적 공격자로서 통신을 방해하거나 메시지를 위조하는 사람

트렌트 _Trent

신뢰할 수 있는 제 3자

빅터 _Victor

검증자

1.1.2 송신자, 수신자, 도청자

그림 1-2 앨리스가 밥에게 메일 보내기(송신자/수신자)

도청자

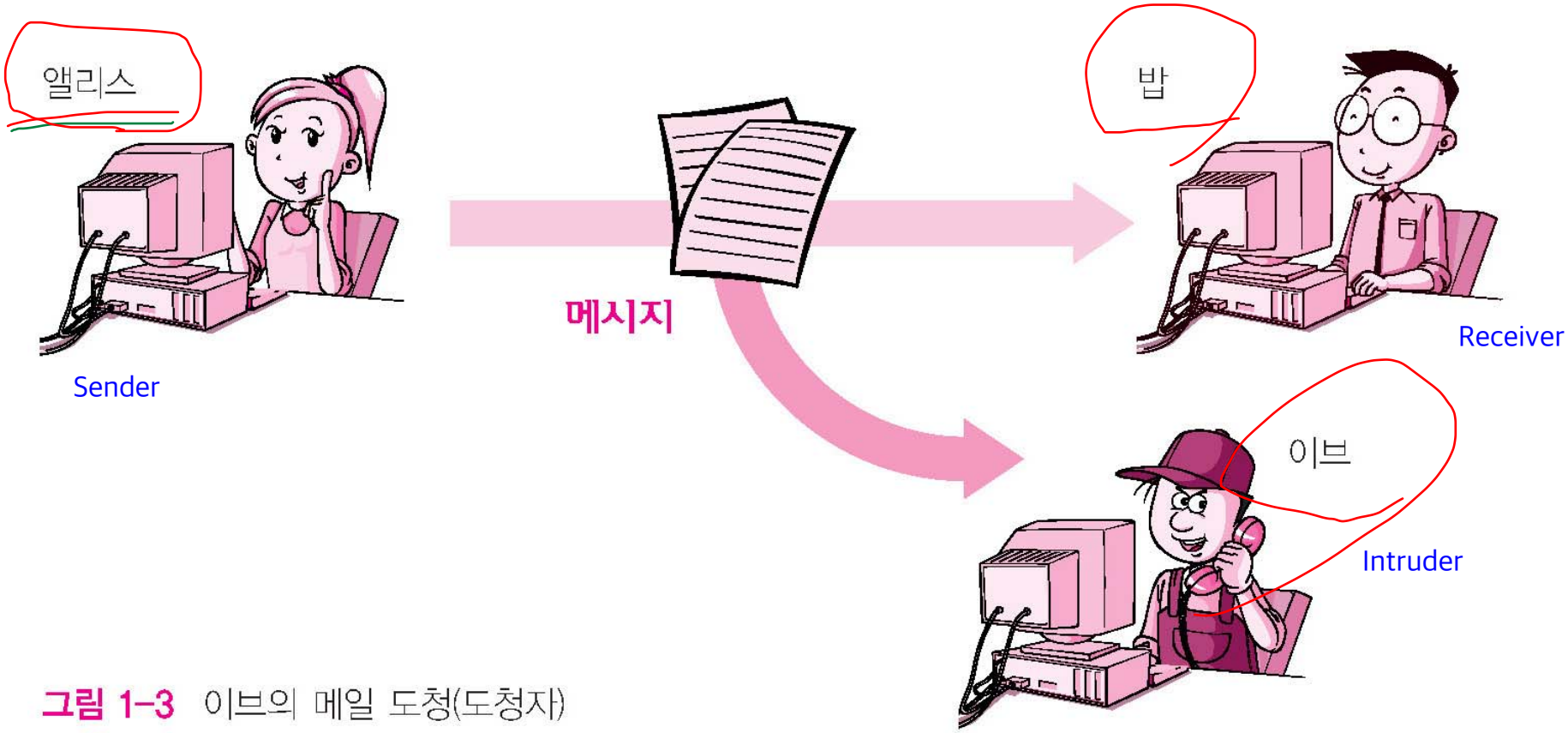


그림 1-3 이브의 메일 도청(도청자)

1.1.3 적극적 공격과 소극적 공격

- 보안 공격(security attack) 의 분류
  - 소극적 공격(passive attack)
    - 소극적 공격이란 시스템으로부터 정보를 도청하여 얻거나 그 결과로 얻은 정보를 사용하려는 시도
    - 시스템 자원에는 영향을 끼치지 않는 공격 형태
  - 적극적 공격(active attack)
    - 적극적 공격이란 시스템 자원을 변경하거나 시스템의 작동에 영향을 끼치는 공격 형태

1. Read the Meassage
2. Key

1. 변조 (Message Alter)
2. 위장

대개 이름을 멜로리라고 한다.

소극적 공격

- 소극적 공격이란 자료를 전송할 경우에 전송중인 자료에 대한 도청이나 감시를 의미한다.
- 소극적 공격자의 목표는 전송중인 정보를 취득하는 것이다.
- 여기에는 두 가지 유형의 공격이 있는데 이들은 **메시지 내용 갈취**와 **트래픽 분석**이다.

적극적 공격

- 적극적 공격은 전송중인 데이터를 수정하거나 가짜 데이터를 만드는 행위
- 적극적 공격의 4 가지 분류
  - 신분위장(masquerade)
  - 재전송(replay)
  - 메시지 수정(modification of messages)
  - 서비스 거부(denial of service)

메시지를 제 3자가 몰래 읽기

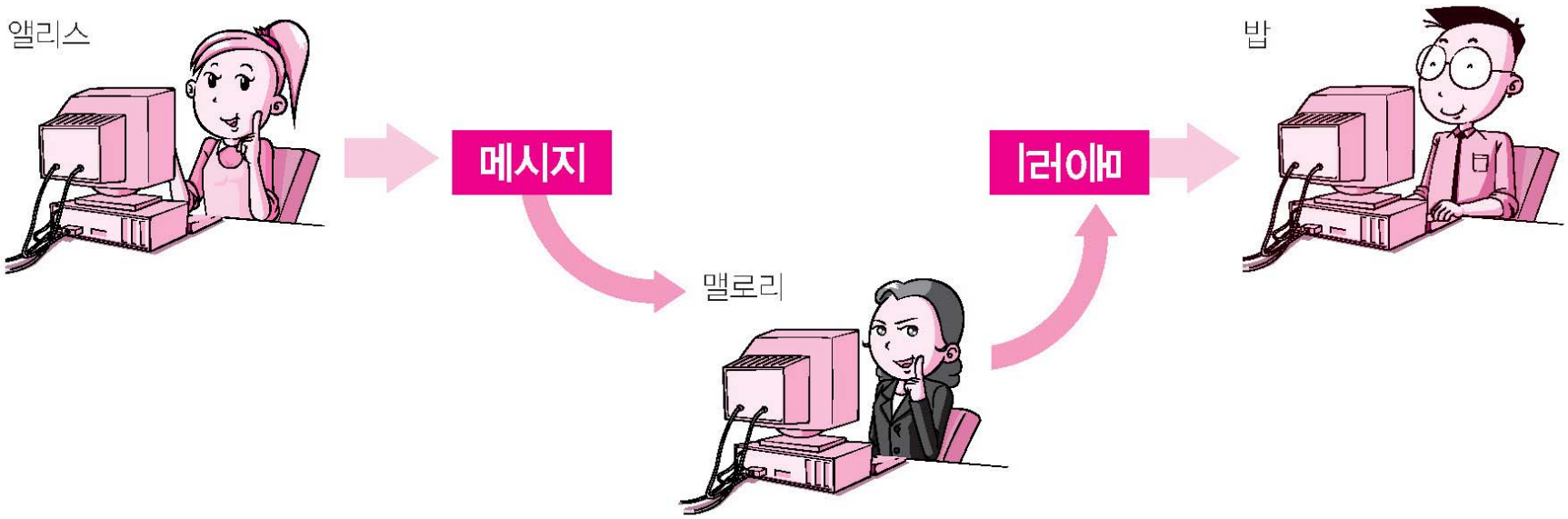


그림 1-4 맬로리의 메일 수정

1.1.4 암호화와 복호화

- 메일을 **암호화(encrypt)**해서 보낸다
- 암호화하기 전의 메시지를 **평문(plaintext)**
- 암호화한 후의 메시지를 **암호문(ciphertext)**

암호 체계는 3가지 과정을 가진다.

1. Encryption
2.Decryption
3. Key Generation

평문의 암호화

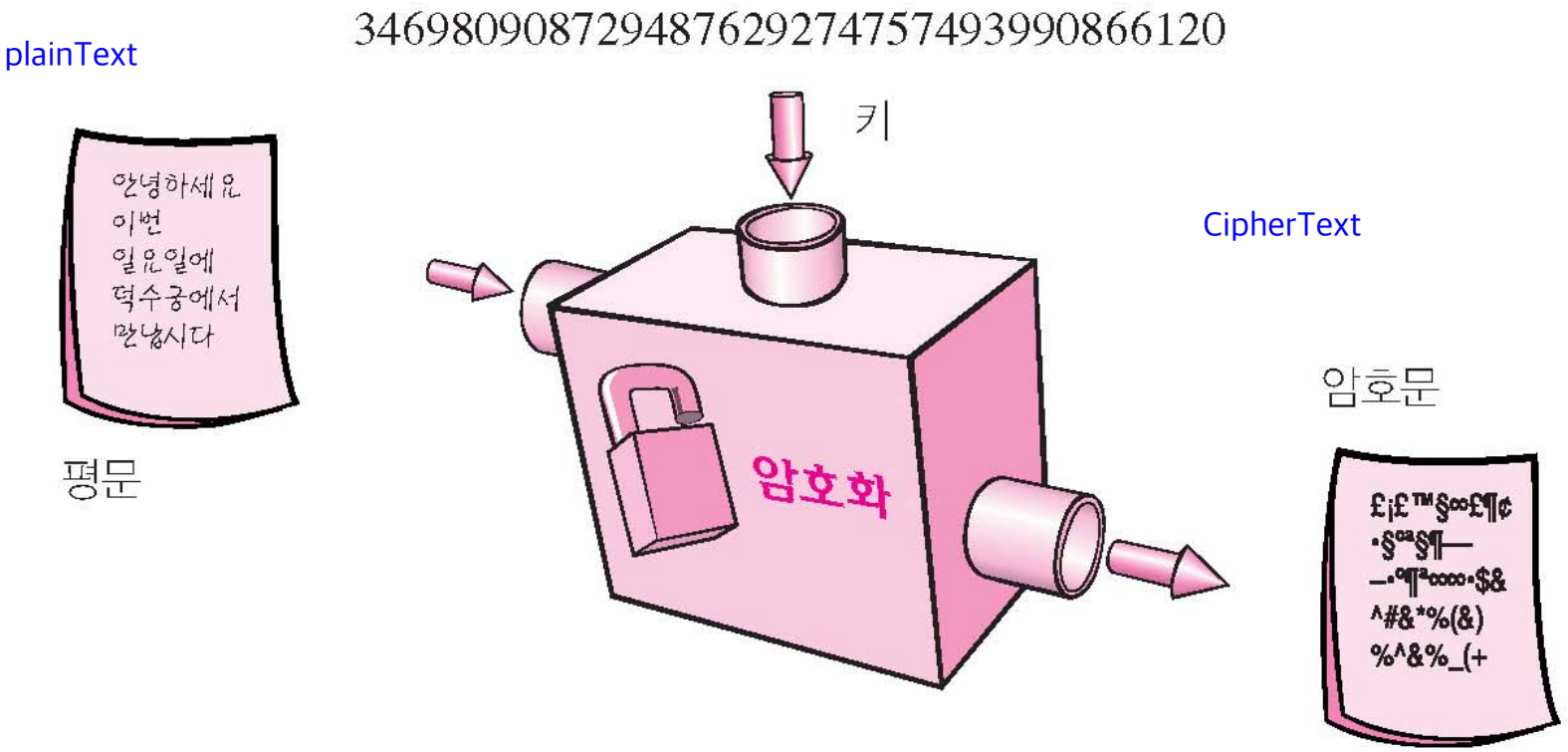


그림 1-5 암호화 과정

암호문의 복호화

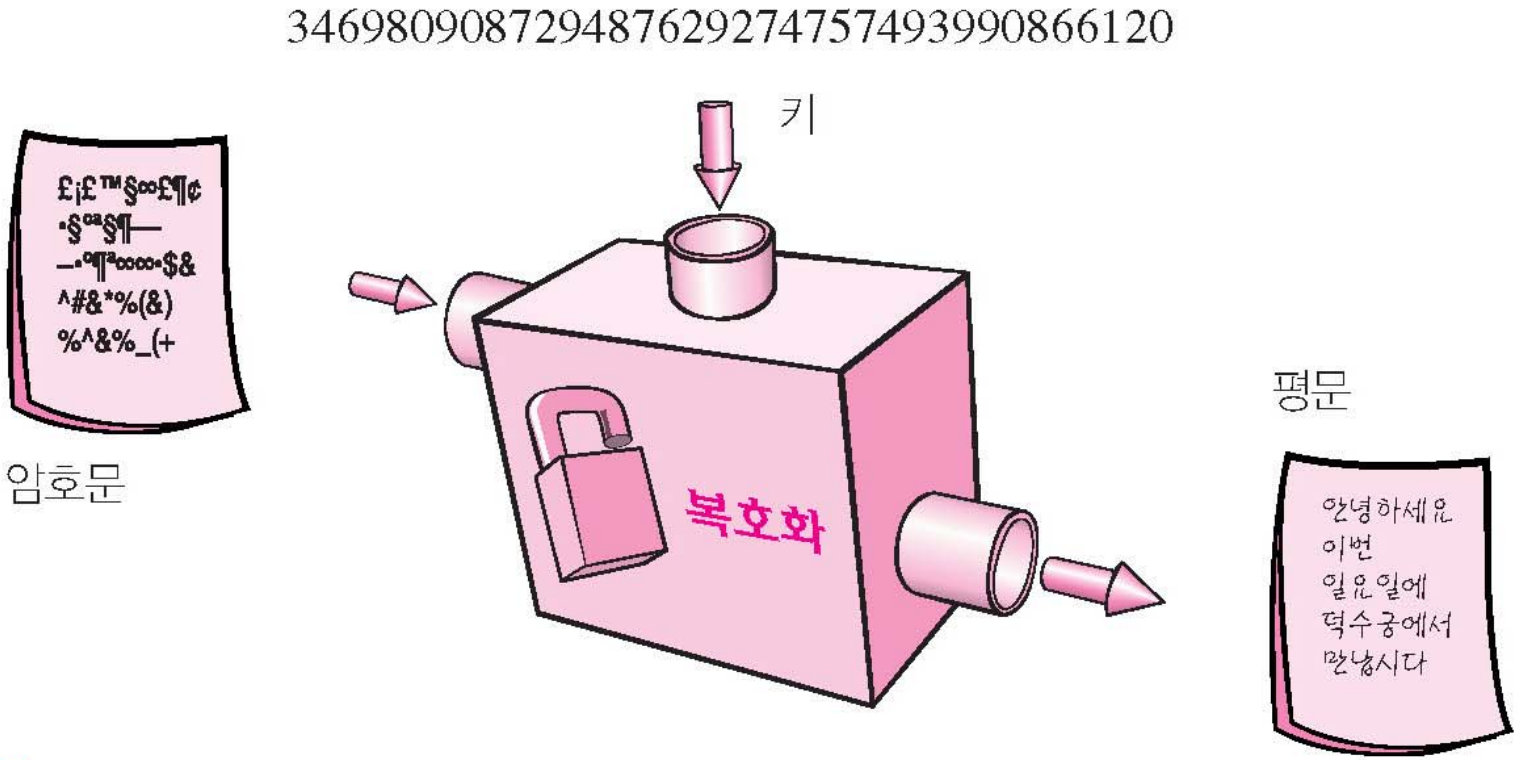


그림 1-6 복호화 과정

도청자가 얻을 수 있는 것

- 메시지를 암호화해서 보낼 경우를 생각해보자
- 만약 중간에서 도청이 이루어진다면 도청자가 얻게 되는 것은 암호문이다
- 따라서 도청자가 암호문을 복호화할 수 없다면 암호화 되기 이전의 메시지(평문) 내용을 알 수 없다

도청자가 얻을 수 있는 것

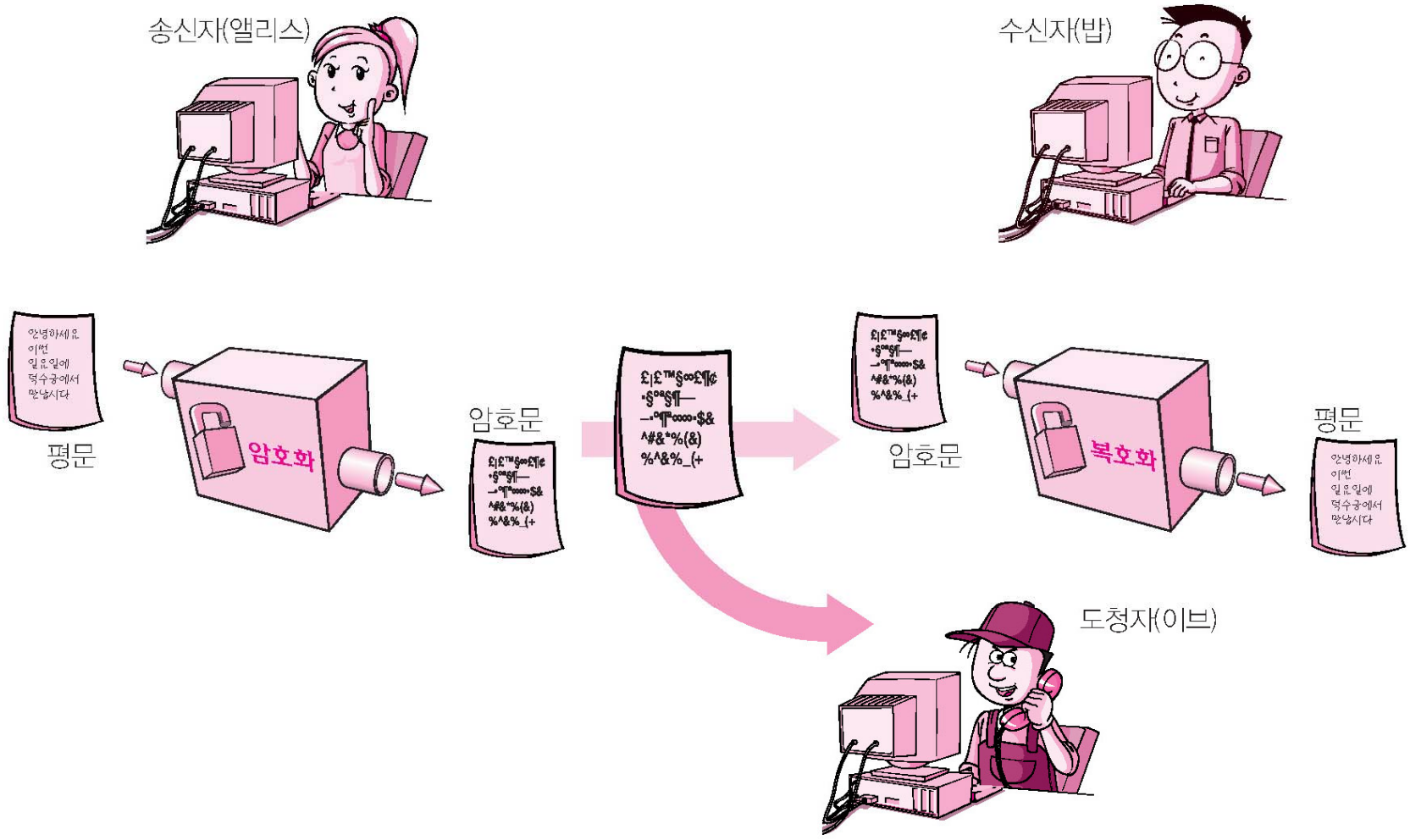


그림 1-7 도청자가 보는 것은 암호문뿐이다

1.1.5 암호를 이용한 기밀성 보장

- 앨리스와 밥은 **암호**(cryptography)라는 기술을 써서 메일의 내용을 두 사람만이 알 수 있도록 하는 **기밀성**(confidentiality, **또는 비밀성**)을 유지

1.1.6 해독

- **복호화**:

  정당한 수신자가 암호문을 평문으로 바꾸는 것

- **암호 해독(cryptanalysis)**:

  정당한 수신자 이외의 사람이 암호문을 평문으로 복원하려고 하는 것

  - 간단하게 **해독**이라고 하기도 하고
  - **암호 해석**이라고 부르기도 한다

암호 해독자(cryptanalyst)

- 암호 해독자: 암호 해석을 하는 사람
- 암호 해독자라고 해서 반드시 나쁜 의도를 가진 사람은 아니다
- 암호를 연구하는 연구자인 경우는 암호의 강도(암호해독의 난이도)를 연구하기 위해 자주 암호를 해독한다. 이 경우에는 암호 연구자가 암호 해독자이다

퀴즈 1 : 디자인 파일의 암호화

- 앨리스는 자동차 회사의 모델 디자이너이다.
- 앨리스는 자신이 디자인한 자동차 모델 파일을 암호화하여 자신의 컴퓨터에 저장하고 관리한다.
- 디자인을 업데이트 하거나 수정할 필요가 있을 경우에는 그 때마다 복호화해서 자료를 가져온다.
- 이 경우 송신자와 수신자는 누구인가?

1.2 대칭 암호와 비대칭 암호

- 암호 알고리즘
- 키
- 대칭 암호와 비대칭 암호
- 하이브리드 암호시스템

1.2.1 암호 알고리즘

- **암호화 알고리즘** : 평문을 암호문으로 만드는 과정인 암호화 과정
- **복호화 알고리즘** : 복호화 과정
- **암호 알고리즘** : 암호화와 복호화 알고리즘을 합한 것

1.2.2 키

- 현실 세계의 키
- 암호 세계의 키

현실 세계의 키

- 현실 세계에서 필요한 키(key, 열쇠)
  - 현실 세계의 키:
    - 아주 복잡한 형태로 된 작은 금속
    - 마그네틱 카드

그림 1-8 금속 키와 마그네틱 카드

암호 세계의 키

- 암호 알고리즘에서 필요한 키(key)
  - 암호 알고리즘의 키는 매우 긴 숫자
    - 예: “203554728568477650354673080689430768”

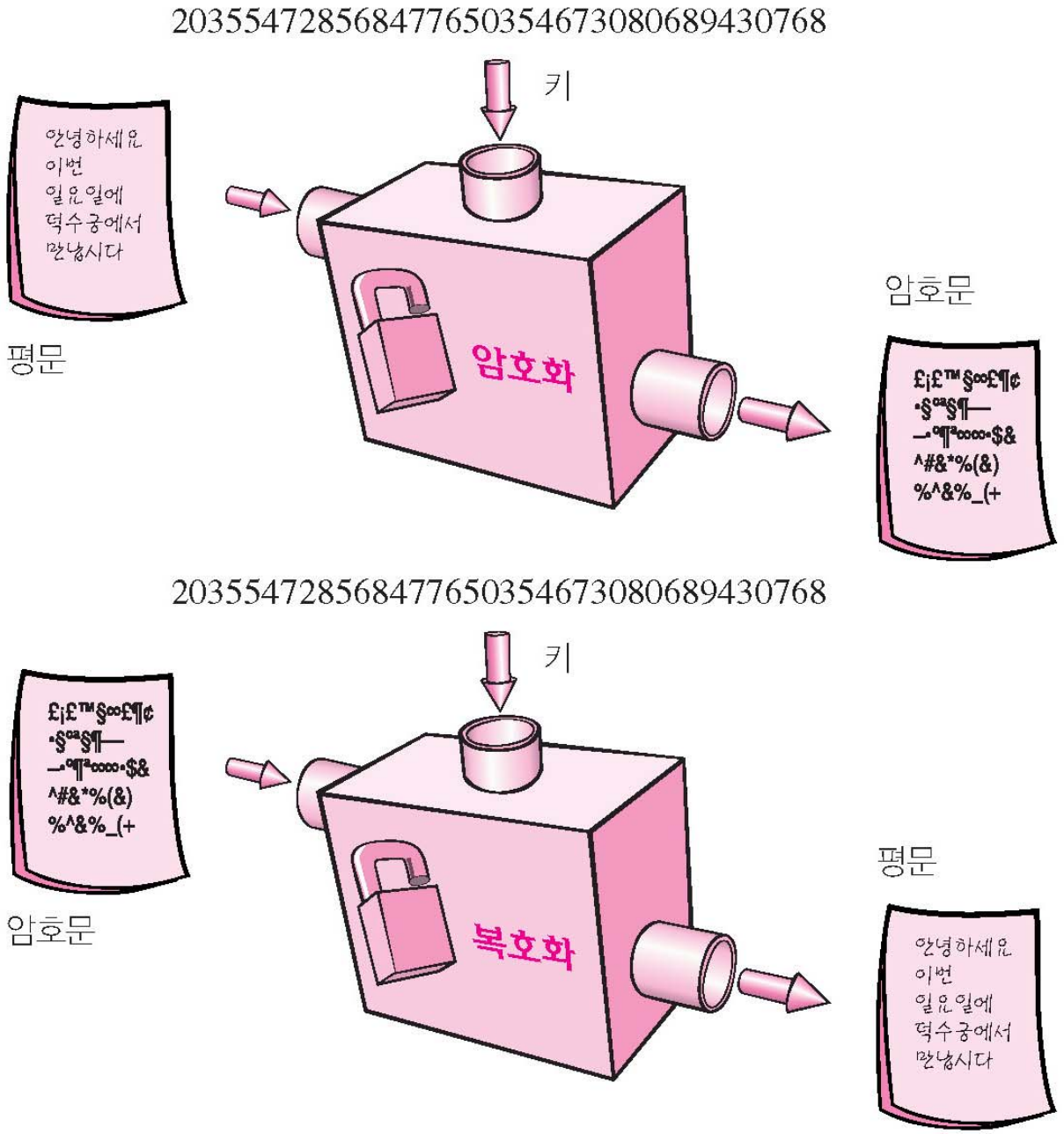


그림 1-9 암호화 및 복호화와 키의 관계

1.2.3 대칭 암호와 비대칭 암호

- 암호는 키의 사용 방법에 따라 대칭 암호와 공개 키 암호로 분류
- **대칭 암호**(symmetric cryptography)는 암호화를 할 때 사용하는 키와 복호화 할 때 사용하는 키가 동일한 암호알고리즘 방식
- **비대칭 암호**(asymmetric cryptography)는 암호화를 할 때 사용하는 키와 복호화 할 때에 사용하는 키가 서로 다른 암호알고리즘 방식

대칭 암호의 다른 이름

- 대칭 암호에는 다양한 이름이 있다
  - 공통키 암호(common-key cryptography)
  - 관용암호(conventional cryptography)
  - 비밀키 암호(secret-key cryptography)
  - 공유키 암호(shared-key cryptography)

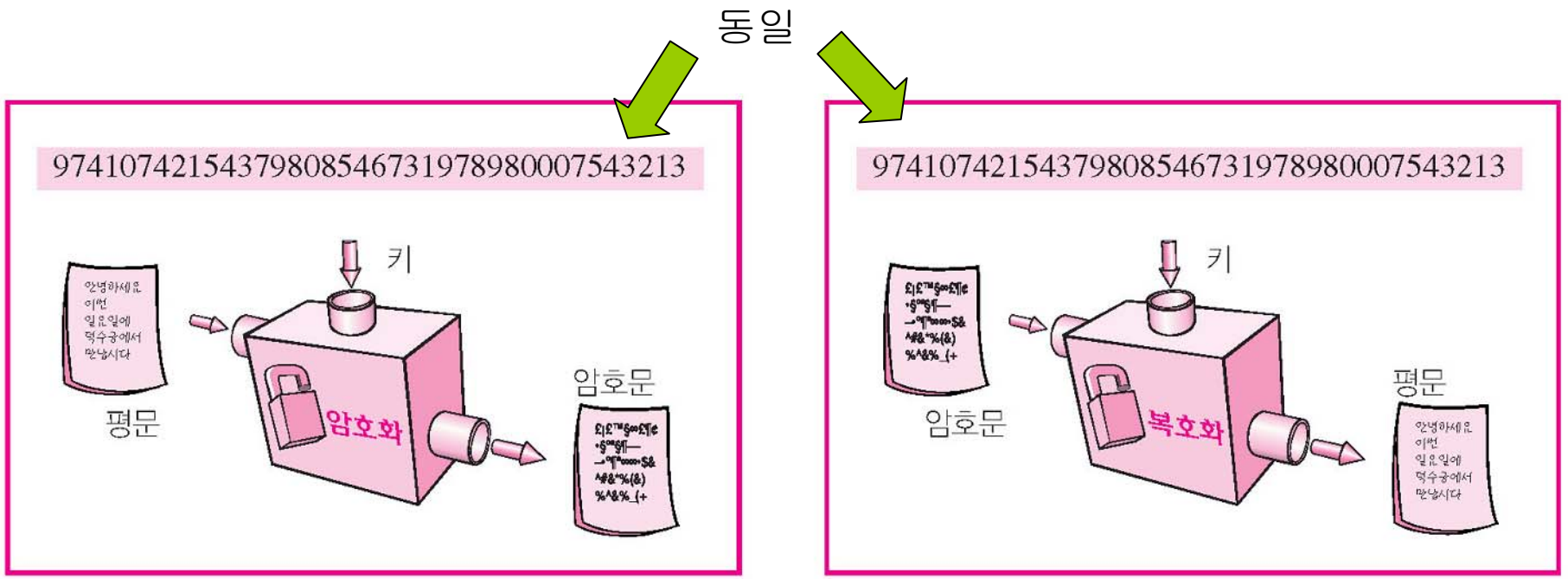
비대칭 암호의 다른 이름

- 비대칭 암호를
  - 공개키 암호(public-key cryptography)라고 한다
  - 비대칭 암호와 대칭 암호는 형식적으로 그 메커니즘을 구별하기 위해 사용하는 용어이다
  - 비대칭 암호 대신에 공개키 암호라는 용어를 더 많이 사용한다

공개키 암호

- 공개키 암호는 1970년대에 발명
- 암호의 세계에 일대 변혁을 가져온 방법
- 현대 컴퓨터나 인터넷에서 보안(security, 정보 보호)은 공개키 암호에 크게 의존

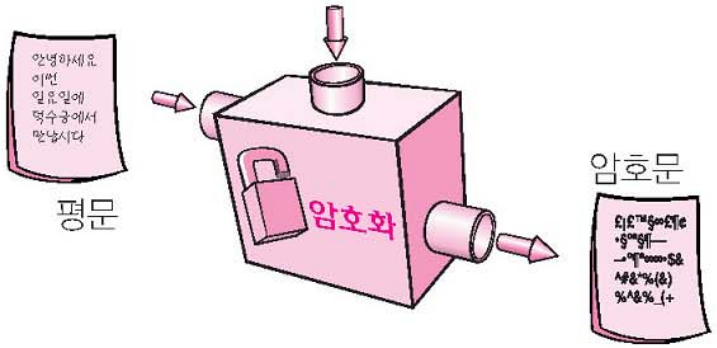
대칭 암호의 암호화와 복호화



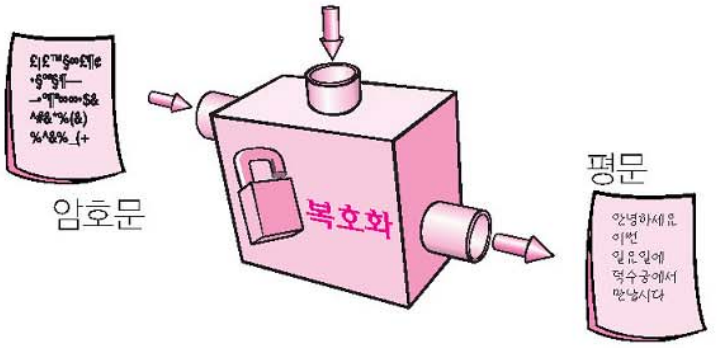
공개키 암호의 암호화와 복호화

다름

610044354361096725260592154472411O



796531880963046086612109147634 4



1.2.4 하이브리드 암호시스템

- 하이브리드 암호시스템(hybrid cryptosystem)
  - 대칭 암호와 공개키 암호를 조합한 암호 방식
  - 대칭 암호와 공개키 암호의 장점을 조합한 시스템

1.3 암호기술에 의한 보호

- 암호 기술이 제공하는 것
  - **기밀성**: 송신자와 수신자만 메시지 내용을 아는 것
  - **무결성**: 정보가 전송 도중에 변경이 되지 않았다는 것
  - **인증**: 틀림없이 송신자 본인이라는 것을 확인하는 것
  - **부인방지**: 보낸 사람이 보낸 사실을 나중에 부인하거나, 받은 사람이 받은 사실을 부인할 경우에 증명하는 기술

1.3.1 기밀성

- 정당한 사용자만 데이터를 볼 수 있게 하는 기술
- 설사 불법자가 데이터를 볼 수 있다고 하더라도 그 내용이 암호화 되어있어서 해독할 수 없도록 하는 것
- 송수신 당사자가 아니면 데이터나 메시지를 판독 할 수 없도록 하여 이것이 유출되더라도 변조되거나 위조되지 못하게 하는 기본적인 보안 기술

1.3.2 무결성

- 송신자와 수신자 사이에 전송되거나 교환되는 자료가 도중에 변경되지 못하도록 하는 기술
- 무결성을 검증하기 위해서는 메시지 인증자 등을 추가로 붙인 다음에 전송

1.3.3 인증

- 개체인증:
  - 통신을 하고 있는 상대방에 대해서 상대방이 주장하는 것처럼 정말로 그 당사자인지를 확인해주는 것
- 데이터 근원지 인증:
  - 수신된 데이터가 정말로 데이터에 나타난 출발지로부터 온 것인지를 확인하는 것

인증의 개념

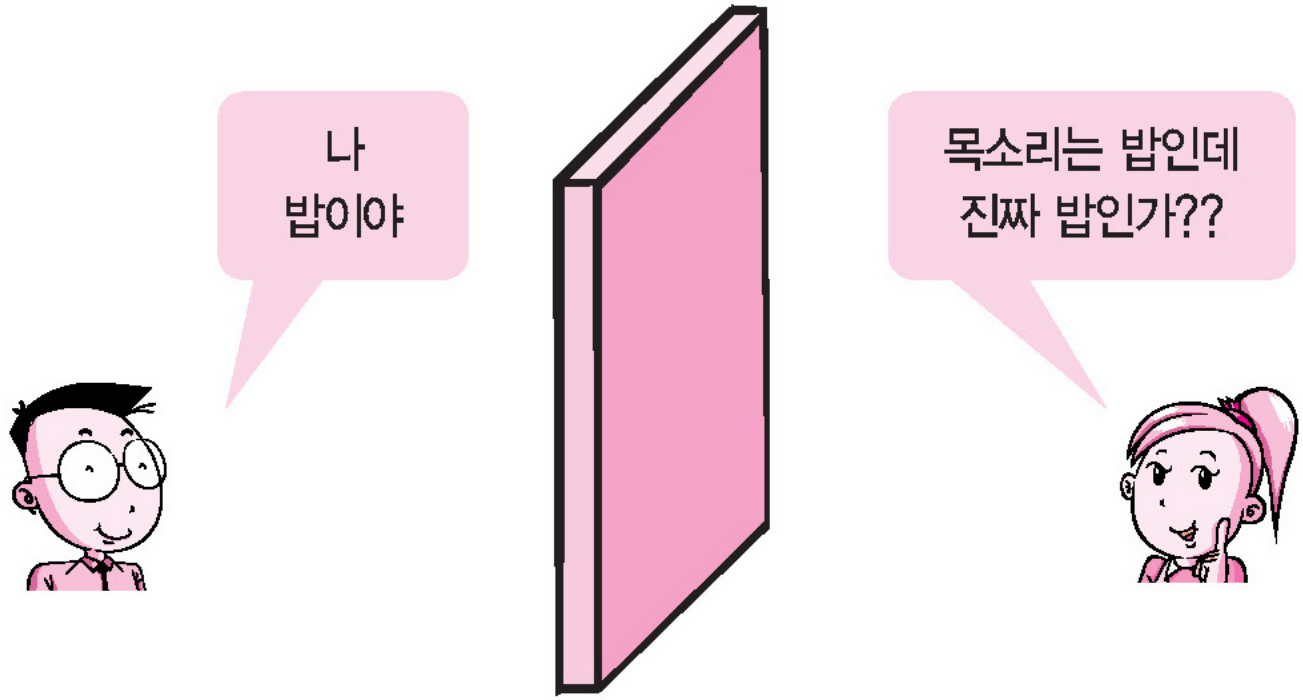


그림 1-11 개체 인증의 필요성

발신지 인증이 필요한 경우

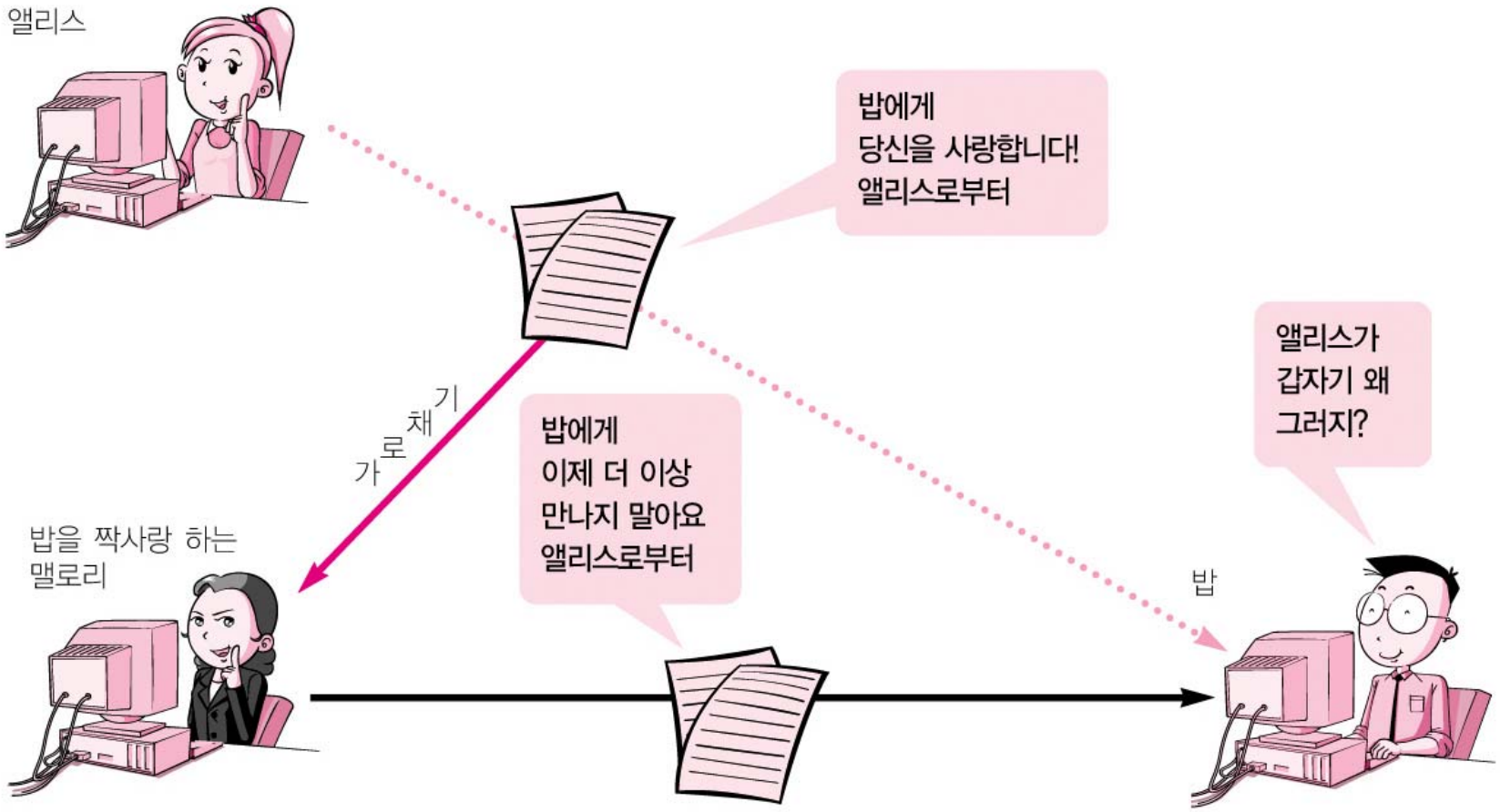


그림 1-12 발신지 인증이 필요한 경우

1.3.4 부인방지

- 메시지의 송수신이나 교환 후에 그 사실을 사후에 증명함으로써 송신한 사실이나 수신한 사실을 부인하지 못하도록 하는 보안 기술
  - **송신 부인 방지(non-repudiation of origin)**: 메시지를 송신하고도 송신하지 않았다고 주장하는 송신자의 부인을 막는 기술
  - **수신 부인 방지(non-repudiation of receipt)** : 메시지를 수신하고도 수신하지 않았다고 주장하는 수신자의 부인을 막는 기술

소프트웨어 다운로드

- 인터넷을 통하여 프리 소프트웨어를 다운받았다고 하자.
- 이 소프트웨어가 작성자가 만든 원본과 같은 것인지?
- 도중에 나쁜 의도를 가진 자가 소프트웨어에 이상한 조작을 하지는 않았는지를 어떻게 확신할 수 있는가?

1.3.5 일방향 해시 함수 (one-way hash function)

- 제공하고자 하는 프로그램이 변경되지 않았음을 확인할 수 있도록 프로그램 제공자는 프로그램을 공개함과 동시에 그 프로그램의 **해시 값**을 공개하는 경우가 있다.
- 해시 값이란 일방향 해시 함수를 사용하여 계산한 값이다.
  - 해시값의 다른 이름들
    - 암호화 검사합(cryptographic checksum)
    - 지문(fingerprint)
    - 메시지 다이제스트(message digest)

해시함수

그림 1-13 해시함수

해시 함수의 기능

- 기밀성은 보장하지 못한다
- **무결성(integrity)을 보장한다**
  - 무결성이라는 것은 그 데이터가 원래의 내용 그대로인 진짜라는 것을 말한다.
  - 무결성은 **완전성**이라고 하기도 한다.
  - 일방향 해시함수를 사용하면 데이터가 전송되는 도중에 변경되었는지 아닌지를 확인할 수 있다

1.3.6 메시지 인증 코드

- 메시지 인증 코드(MAC; Message Authentication Code) :메시지가 생각했던 통신 상대로부터 온 것인지를 확인하는 기술
- 메시지가 전송 도중에 변경되지 않았다는 것과, 생각했던 통신상대로부터 왔다는 것을 확인
- 메시지 인증 코드는 무결성 뿐만 아니라 **인증**(authentication)도 제공

메시지 인증코드

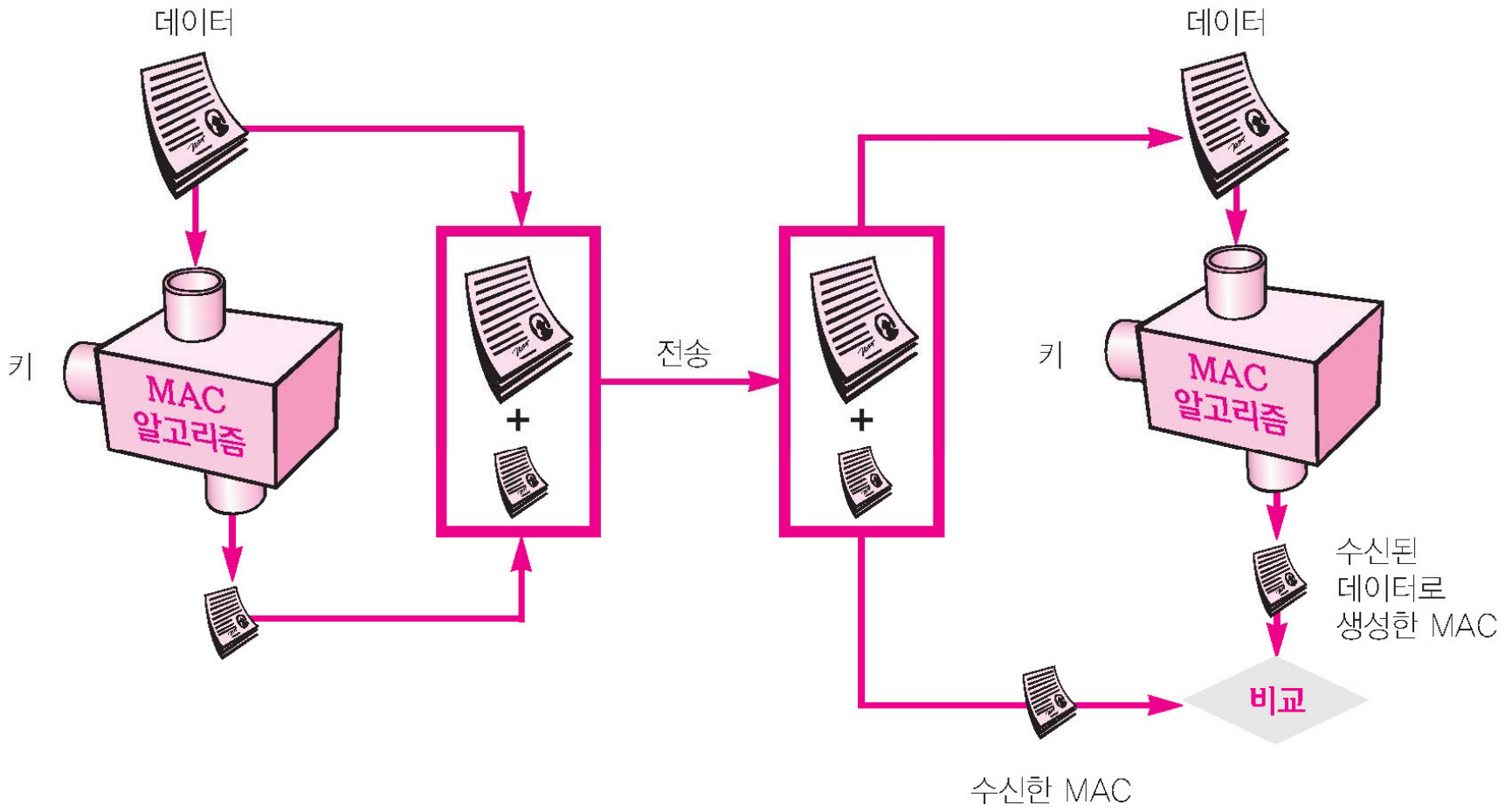


그림 1-14 메시지 인증 코드

1.3.7 디지털 서명

- 자신이 했던 것을 나중에 뒤집는 것을 **부인(repudiation)**이라고 한다.
- 거짓 행세, 변경, 부인 등의 위협을 방지하는 기술이 **디지털 서명(digital signature)**이다
- 디지털 서명이란 현실 세계의 서명이나 날인을 디지털 세계에 적용한 것

1.3.8 의사난수 생성기

- 의사난수 생성기(pseudorandom number generator; PRNG): 난수열을 의사적으로 생성하는 알고리즘
- 난수가 암호 기술과 관련이 있다는 것은 다소 의외일지도 모르지만, 난수는 **키 생성**이라는 매우 중요한 역할을 담당하고 있다

1.4 암호학자의 도구상자

- 대칭 암호
- 공개키 암호
- 일방향 해시함수
- 메시지 인증코드
- 디지털 서명
- 의사난수 생성기

보안 위협과 암호 기술에 의한 방지

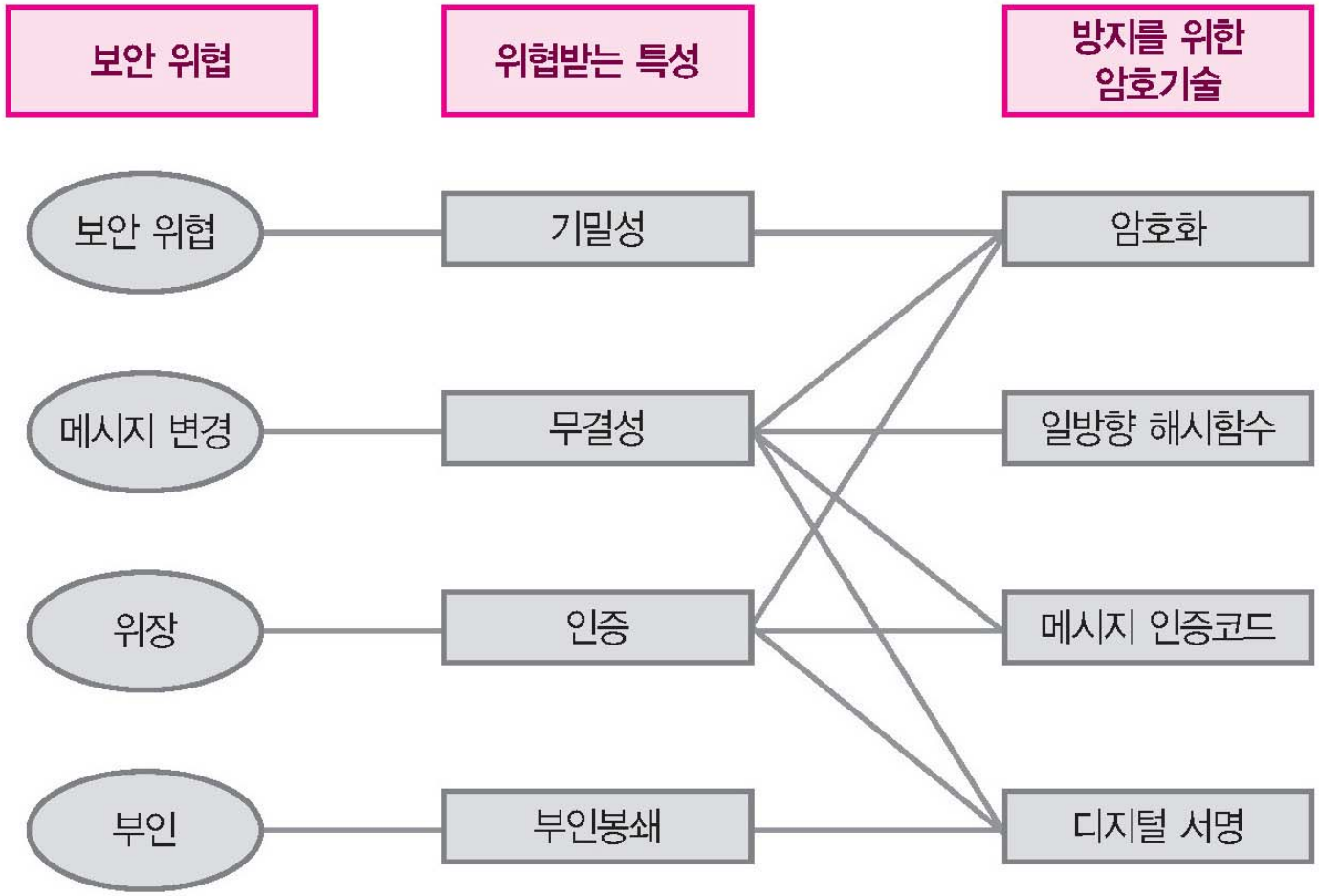
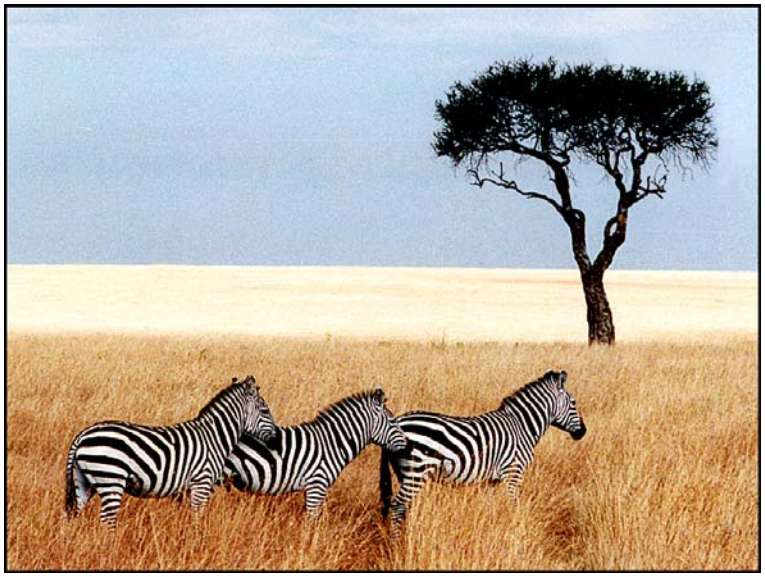


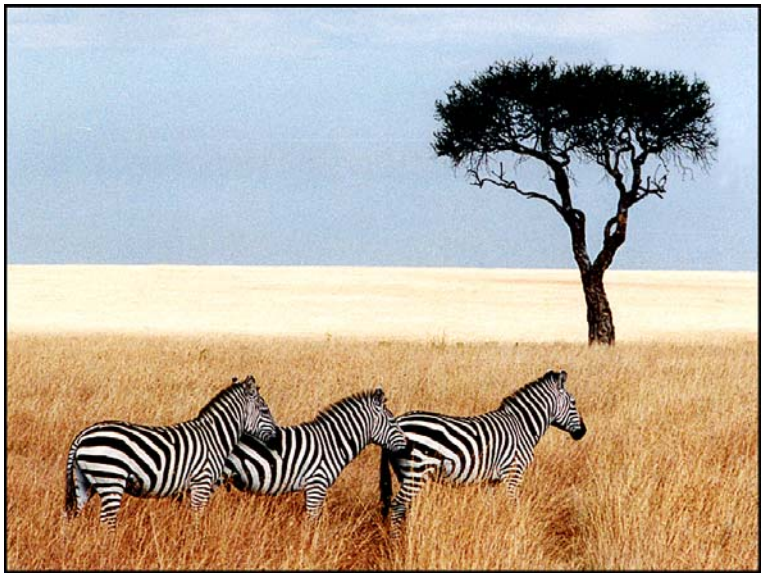
그림 1-15 보안 위협과 암호 기술에 의한 방지

1.5 스테가노그래피와 디지털 워터마크

- 암호란 메시지의 내용을 읽을 수 없도록 하는 기법을 말하며, 영어로는 **크립토그래피**(cryptography)라고 한다.
- 메시지의 내용을 읽을 수 없도록 하는 것이 아니라 메시지의 존재 자체를 감추어 버리는 기법도 있다. 이것을 **스테가노그래피(steganography)**라고 한다.

스테가노그래피를 이용한 자료 숨기기





다음 사이트 http://www.cs.vu.nl/~ast/books/mos2/zebras.html에 접속하여 다음 두 그림(그림 1-16 참조)을 비교해보기 바란다.

워터마크를 적용하기 전과 적용 후

1.6. 암호와 보안 상식

- 공개되지 않은 비밀로 된 암호 알고리즘을 사용하지 마라
- 약한 암호는 암호화하지 않는 것보다 위험하다
- 어떤 엄호라도 언젠가는 해독된다
- 암호는 보안의 일부에 지나지 않는다

1.6.1 공개되지 않은 비밀 알고리즘

- 비밀로 되어있는 암호 알고리즘을 사용해도 높은 보안을 얻을 수 없다
- 비밀로 된 암호 알고리즘을 새로 만들어서 사용할 것이 아니라, 이미 공개되어 있는 알고리즘 중에서 검증된 강한 암호 알고리즘을 사용할 것을 권장한다.

암호 알고리즘의 비밀

- 암호 알고리즘 그 자체를 비밀로 해서 기밀성을 유지하려고 하는 암호 시스템은, 암호 알고리즘의 규격이 폭로되어 버리면 끝이라는 것이다.
- 이에 비해 공개되어 있는 알고리즘은 원래 처음부터 비밀이 아니기 때문에 누구나 알고 있으며, 알고리즘의 규격이 알려져 있어서 강도가 떨어진다는 위험이 있다.

강한 암호 알고리즘

- 전문 암호 해독자들에게 암호 알고리즘의 규격을 제대로 알려 주고, 프로그램의 소스 코드도 건네주고, 샘플로 평문과 그에 해당되는 암호문 쌍을 많이 건네주었어도, 새로운 암호문을 해독하는 데 시간이 매우 오래 걸린다고 한다면 그것이 바로 강한 암호가 되는 것이다.

1.6.2 약한 암호알고리즘

- 「아무리 약한 암호라도 암호화를 하지 않는 것보다는 나을 것이다」라는 생각도 위험하다.
- 「약한 암호를 사용할 거라면 처음부터 암호 따위를 사용하지 않는 것이 낫다」라고 생각하는 것이 좋다

1.6.3 암호 해독

- 절대로 해독되지 않는 암호 알고리즘은 존재하지 않는다
- 해독을 하는데 시간이 걸릴 뿐이지 해독을 하지 못하는 것은 아니다.

1.6.4 암호와 보안

- 사회 공학(social engineering)
  - 피싱(Phishing)
  - 트로이 목마(Trojan Horse)
  - 키로거(Keylogger): 사용자의 키보드 입력을 몰래 빼내는 방법
  - 협박이나 회유를 통해 패스워드를 알아내는 방법
- 이상과 같은 공격은 암호의 강도 그 자체와는 아무런 관계도 없다.