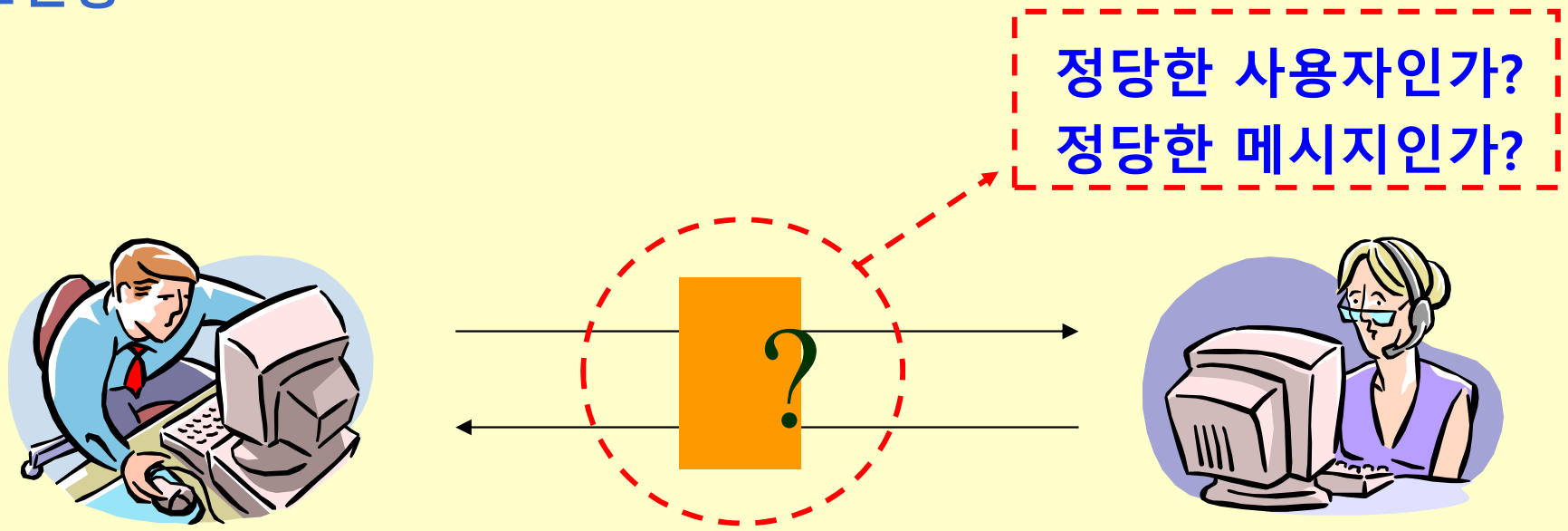
제8장 메시지 인증 및 해쉬함수

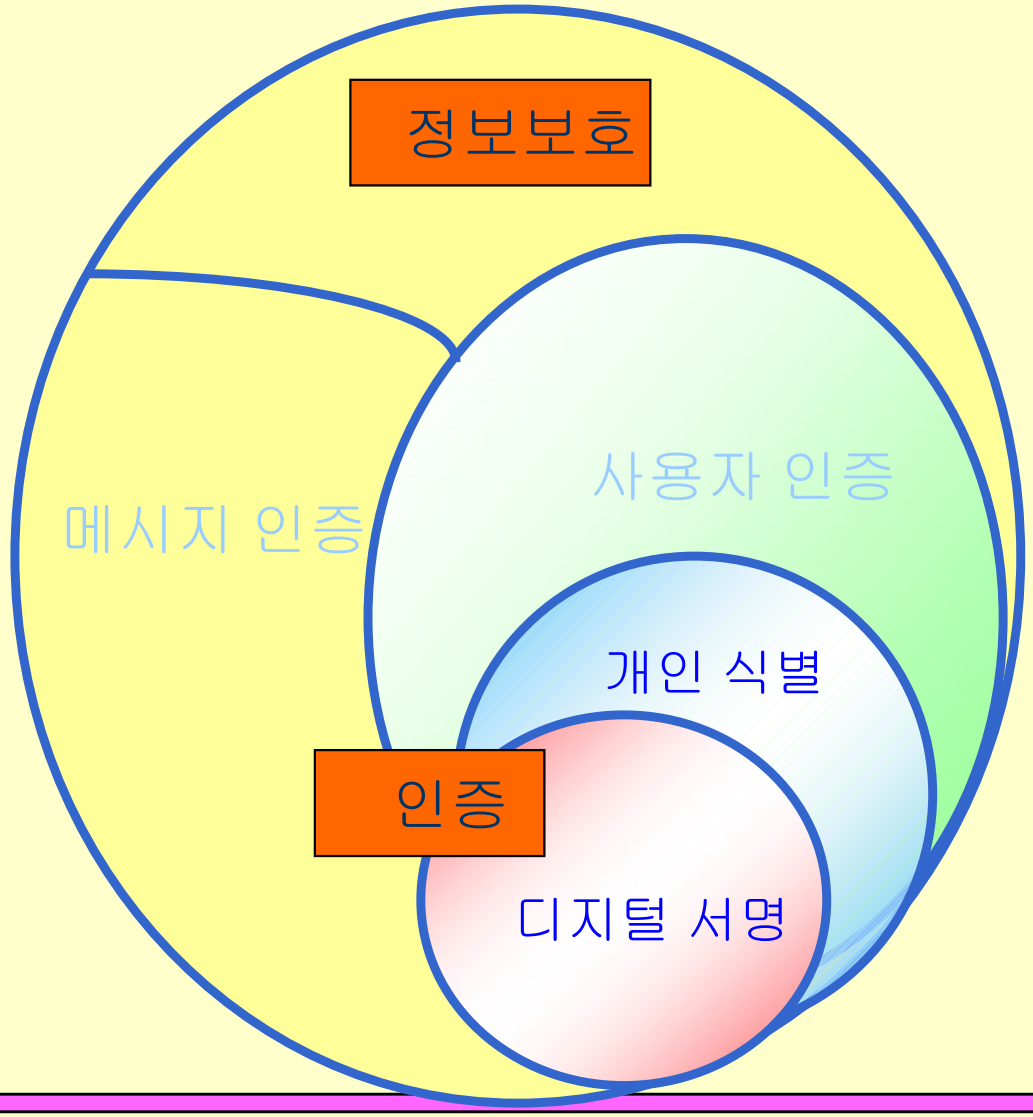
인증

❑보안 서비스의 등장

❖기밀성, 무결성, 부인봉쇄, 접근제어, ***인증***

❑인증




정보보호
메시지 인증
사용자 인증
개인 식별
인증
디지털 서명

❑개인식별(Identification)

- ❖개인에게 할당된 identity에 의해 식별
- ❖보안 시스템은 각 사용자에게 유일한 ID를 할당
- ❖사용자 식별자 : userID

❑인증(Authentication)

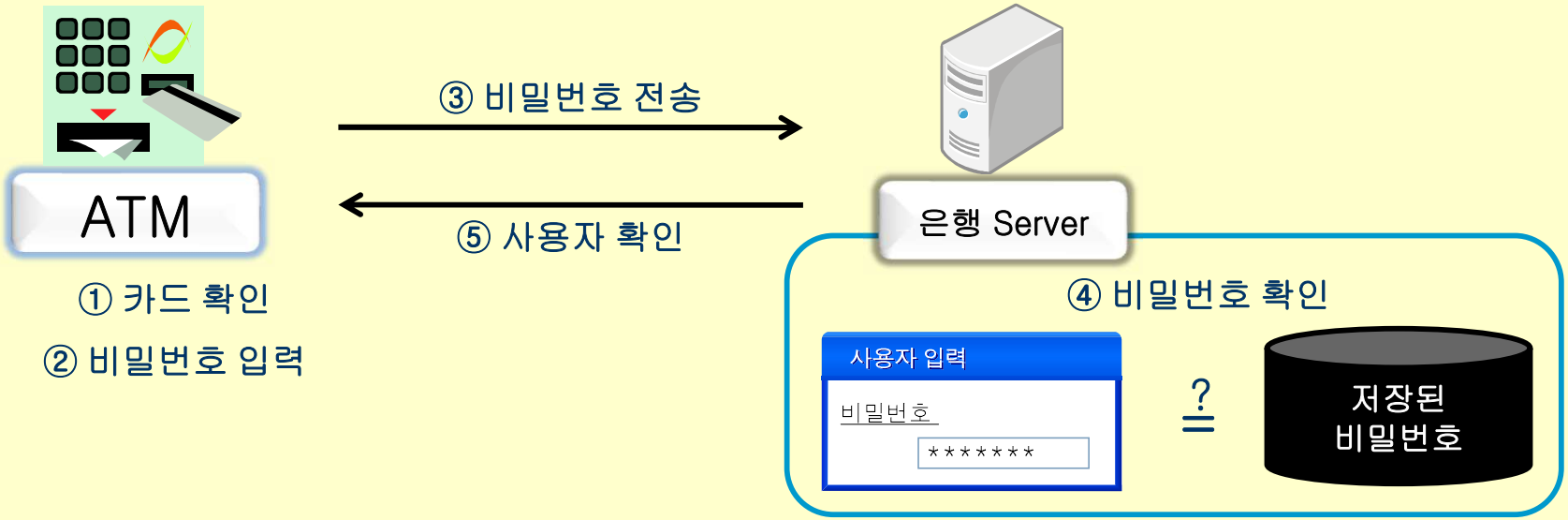
- ❖메시지 인증
- ❖사용자 인증

요소	설명	인증기술
지식	알고 있는 것(Something you know)	ID•PWD, PIN
소유	가지고 있는 것(Something you have)	토큰, 스마트카드, OTP, SMS
존재	생물학적 특성(Something you are)	지문, 홍채•망막, 얼굴, 장문, 정맥 등
행위	행동학적 특징(Something you do)	서명, 걸음걸이, 음성, 키보드입력

- 생체인증이 범용적인 인증수단으로 사용되기 위해 필요한 항목
  - **보편성** : 누구나 가지고 있어야 함
  - **유일성** : 고유해야 함
  - **지속성** : 시간이 지나고 나이가 들어도 변화하거나 변화시킬 수 없어야 함
  - **성능** : 정량적으로 측정하기 쉬워야 하고, 실사용 환경에서도 인식의 정확도가 높고 속도가 빠름
  - **수용성** : 사용자들의 생체 정보를 저장하고 활용하는 데에 거부감이 없어야 함
  - **저항성** : 생체정보 모방이나 해킹 등 외부로부터의 공격도 방어할 수 있어야 함

❑ 패스워드

- ❖ 컴퓨터 시스템에 접속을 요구하는 사용자가 실제 사용허가를 받은 **본인인지 여부를 확인**하기 위해 사용되는 일련의 문자열
- ❖ 컴퓨터 시스템의 설정에 따라 다르긴 하지만, 대체로 4~16글자 사이에서 결정하는 경우가 많음



❖ 패스워드 선정 시 피해야 할 기준

- 7자리 이하 또는 두 가지 종류 이하의 문자구성으로 8자리 이하 패스워드
- 사용자 ID를 이용한 패스워드
- 한글, 영어 등을 포함한 사전적 단어로 구성된 패스워드
- 특정 인물의 이름이나 널리 알려진 단어를 포함하는 패스워드
- 숫자와 영문자를 비슷한 문자로 치환한 형태를 포함한 구성의 패스워드
- 시스템에서 초기에 설정되어 있거나 예제로 제시되고 있는 패스워드

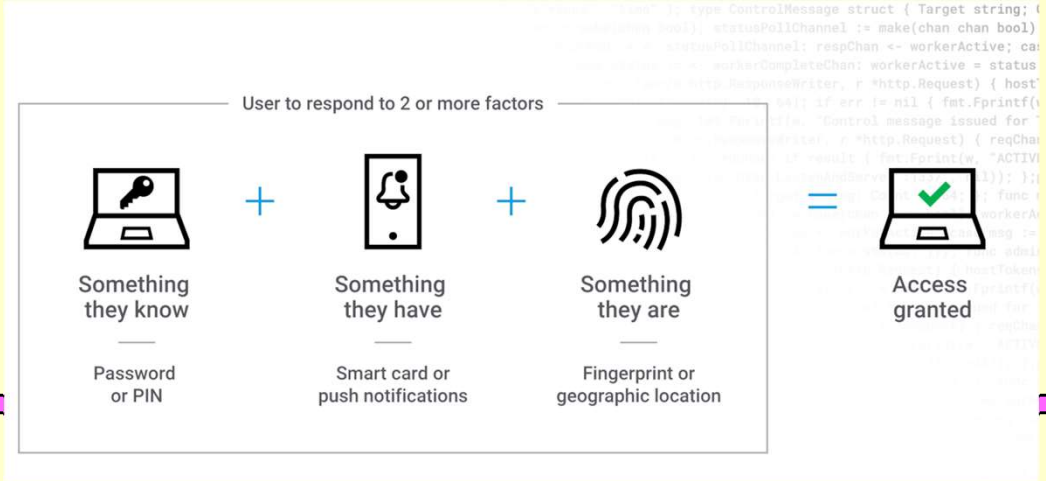
❖ 안전한 패스워드 생성 방법

- 특정 명칭을 선택하여 예측이 어렵도록 가공하여 패스워드 설정
- 특정 명칭의 홀 짝수 번째의 문자를 구분하는 등의 가공 방법을 통해 설정
- 노래 제목이나 명언, 속담, 가훈 등을 이용 가공하여 패스워드 설정
- 알파벳 대소문자 구별할 수 있을 경우, 혼합하여 설정
- 자신의 기본 패스워드 문자열을 설정하고 사이트별로 특정 규칙을 적용하여 패스워드 설정

사용자 인증을 위한 주요방식들

- One-factor 인증/확인 (단일 요소 인증) : 사용자 ID/Password 조합 방식
  - 가장 오래된 패스워드 기반의 인증 방식
  - 고정 Password 방식
    : 한번 엑세스 때 만으로 암호 유효 (암호변경 불요)
  - One Time Password(OTP) 방식
    : 엑세스할 때 마다 다른 암호가 적용됨

- Two-factor 인증/확인 : 이중 요소 인증, 2단계 인증
  - 카드번호 및 비밀번호, ID/Password 및 임시 비표 사용 .
  - 인증서 : 개인 식별용 + 보안 카드 / USB / OTP : 개인 비밀값



사용자 인증을 위한 주요방식들

❖ 공유 비밀 키 (Shared Secret Key) 방식
- ➢ 양측 간에 공유되고 있는 비밀 키에 의함

❖ 시도 응답 인증 (Challenge-Response) 방식
- ➢ 검증자(verifier)가 매회 다른 질문(Challenge,Nounce : 난수, 타임스탬프 등)을
- ➢ 주장자(claimant)는 그 값에 함수를 적용하여 나온 응답으로 비밀을 안다는 것을 증명하는 방식

❖ 생물학적 방법(지문인식,홍체인식) 방식

보안 위협요소

❑ 네트워크 통신상에서 발생할 수 있는 공격

- ❖ 노출(disclosure): 암호키 가지고 있지 않은 사람에게 메시지 내용이 노출
- ❖ 트래픽 분석(traffic analysis): 통신 주체 사이의 어떤 트래픽 형태를 발견

  ==➔ 기밀성으로 해결

- ❖ 위장(masquerade): 부정한 출처로부터 네트워크에 메시지 삽입
- ❖ 내용 수정(content modification): 삽입, 삭제, 전치, 수정을 포함한 메시지 내용의 변경
- ❖ 순서 수정(sequence modification): 통신 상대방간의 메시지들의 순서 수정
- ❖ 시간 수정(timing modification): 메시지의 지연과 재전송

  ==➔ 인증으로 해결

- ❖ 부인(repudiation): 메시지의 송신이나 수신 부인

  ==➔ 디지털 서명으로해결

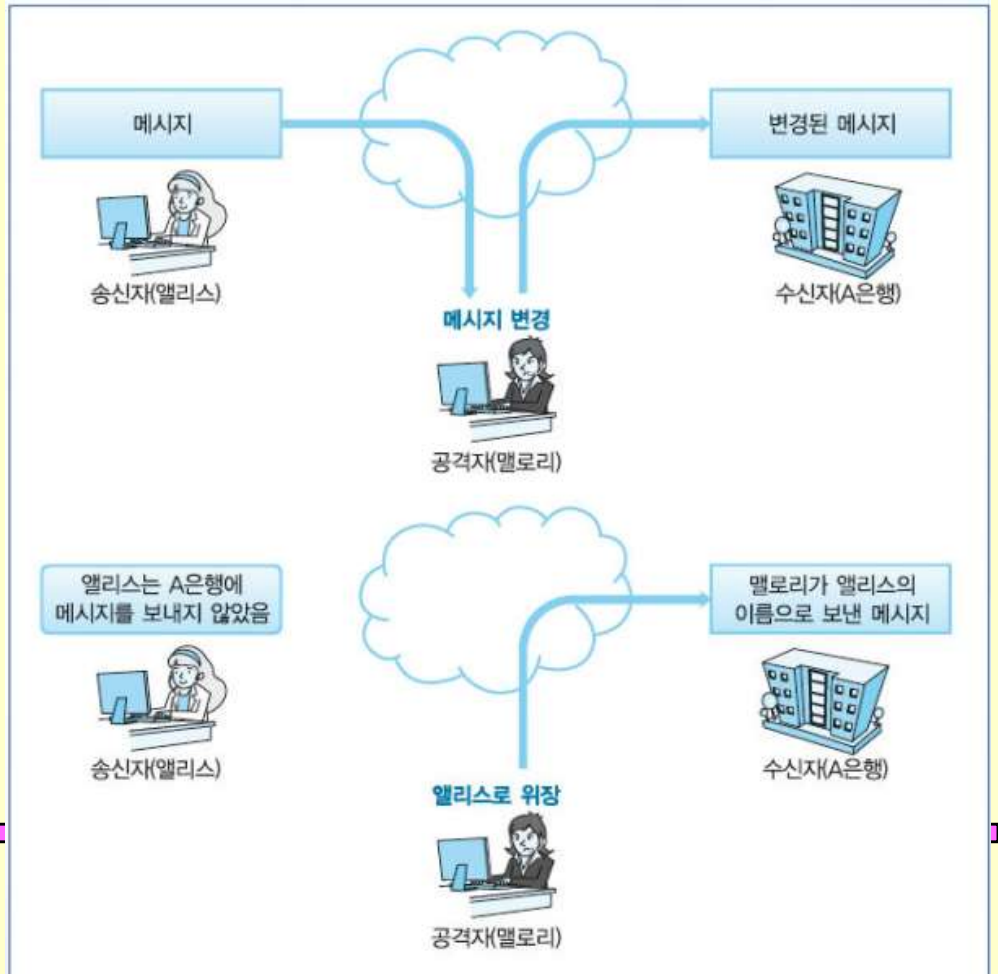
메시지 인증 코드(Message Authentication Code)

❑ 올바른 송금

- ❖ 앨리스 : 은행 A의 고객, 밥 : 은행 B의 고객
- ❖ A은행에 앨리스로부터 송금 의뢰가 도착
- ❖ "내 계좌 앨리스-5374에서 B은행의 계좌 밥-6671로 1억 원을 송금바랍니다."

❑ A은행이 해야 할 일

- ❖ 메시지 출처
  : 사용자 인증(위장 방지)
- ❖ 통신 중 내용 변경 유무
  : 메시지 인증(무결성)

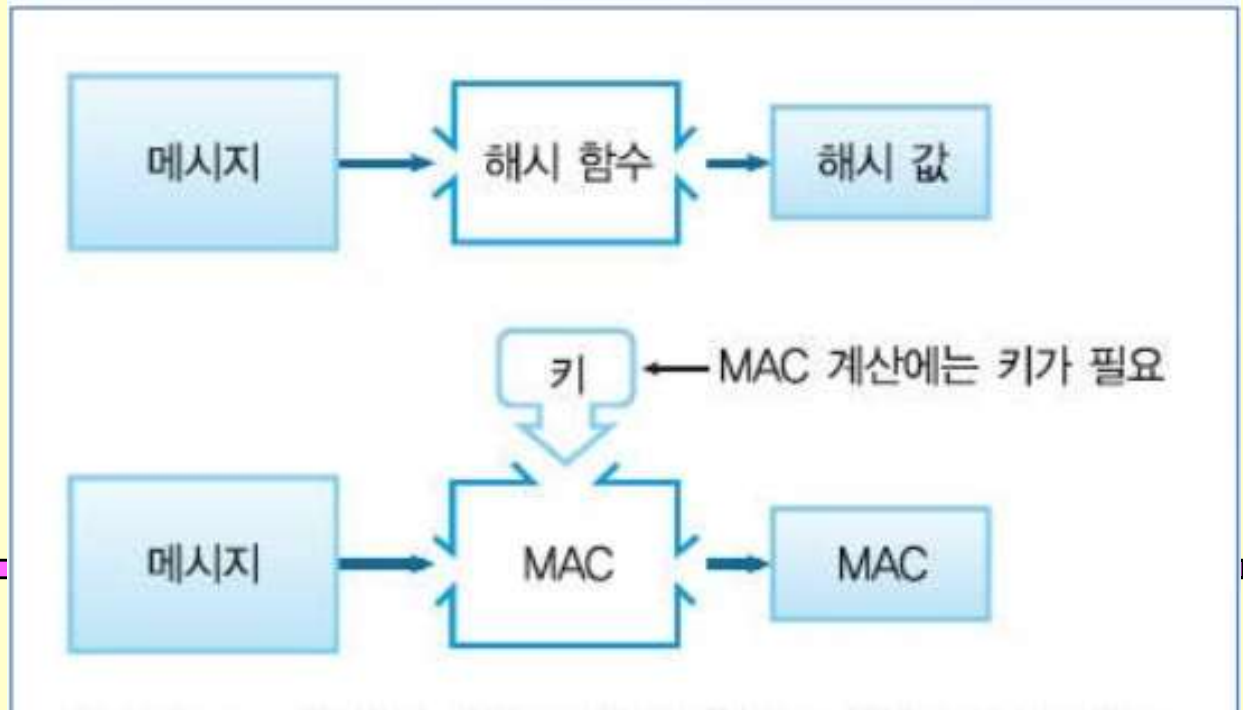


❑ 메시지 인증 코드란?

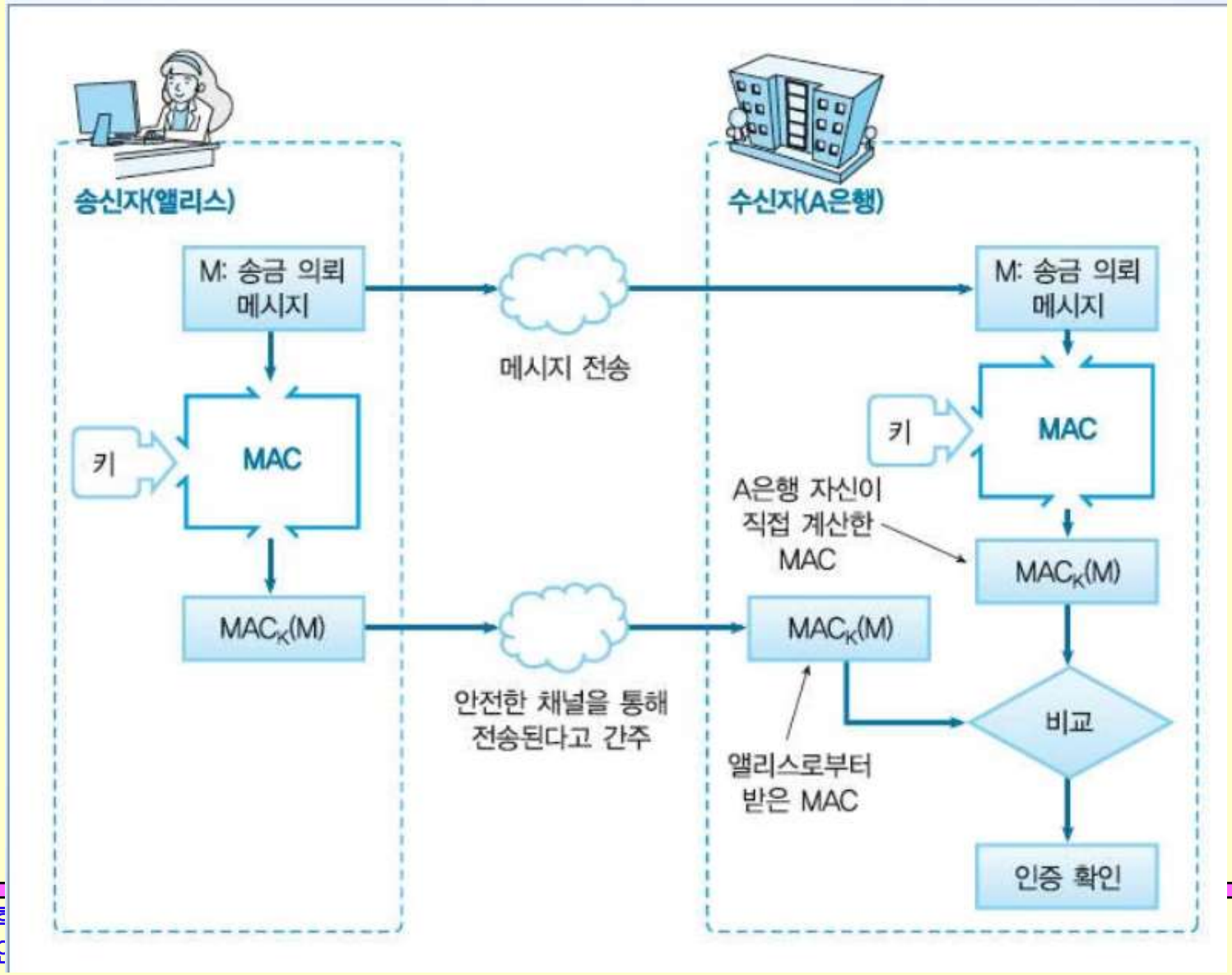
- ❖ 무결성을 확인하고, 메시지에 대한 인증을 위한 코드
- ❖ 첫 글자를 따서 MAC (Message Authentication Code)
- ❖ 입력 : 메시지, 공유하는 키
- ❖ 출력 : 고정 비트 길이의 코드

❑ 일방향 해시와 메시지 인증 코드의 비교

- ❖ 일방향 해시
  - ➢ 키를 사용하지 않음
- ❖ 메시지 인증 코드
  - ➢ 키를 사용



❑ MAC의 이용 순서


송신자(앨리스)
수신자(A은행)
M: 송금 의뢰 메시지
메시지 전송
M: 송금 의뢰 메시지
키
MAC
키
MAC
A은행 자신이 직접 계산한 MAC
$MAC_K(M)$
$MAC_K(M)$
$MAC_K(M)$
안전한 채널을 통해 전송된다고 간주
비교
앨리스로부터 받은 MAC
인증 확인

❑ MAC의 이용 순서

1. Alice와 수신자 A은행: 사전에 키(K) 공유
2. Alice : 송금 의뢰 메시지(M) 작성, MAC 값($MAC_K(M)$)을 계산
3. Alice : 수신자 A은행으로 송금 의뢰 메시지(M)와 MAC 값을 전송
4. 수신자 A은행: 수신한 송금 의뢰 메시지를 기초로 해서 MAC 값을 계산
5. 수신자 A은행: Alice 로부터 수신한 MAC 값과 자신이 계산한 MAC 값을 비교
6. 수신자 A은행:
    1. 인증성공: 2개의 MAC 값이 동일하면 송금 의뢰가 틀림없이 Alice로부터 온 것이라고 판단
    2. 인증실패: 2개의 MAC 값이 동일하지 않으면 Alice로부터 온 것이 아니라고 판단

❑ MAC의 키 분배 문제

- ❖ 대칭 암호 때의「키 분배 문제」와 같은 문제가 메시지 인증 코드에도 발생
- ❖ 키 분배 문제를 해결
  - ➢ 공개 키 암호
  - ➢ 키 분배 센터
  - ➢ 키를 안전한 방법으로 별도로 보내기

MAC로 해결할 수 없는 문제

- 제3자에 대한 증명
  - Alice로부터 메시지를 받은 Bob이 "이 메시지는 Alice가 보낸 것이다"라는 것을 제3자인 검증자 Victor에게 증명할 수 없음
  - 이유 :
    - 일단 키를 Victor에게 알려줘야 함
    - Alice와 Bob 모두가 키를 가지고 있으므로 둘 중 누가 작성했는지 알 수 없음

- 부인방지
  - Bob이 MAC 값이 첨부된 메시지를 받았고, 「이 메시지는 Alice로부터 온 것이다」라는 걸 확실히 알 수 있다.
  - 하지만 Alice가 전송 자체를 부정할 경우 제3자에게 이 사실을 증명할 수 없다.
  - Alice의 송신자체에 대한 부정을 부인(repudiation)이라고 한다.
  - 메시지 인증 코드로는 부인 방지(nonrepudiation)를 할 방법이 없다.

인증 위협요소

- 신분위장 형태
  - 도청: 도청하다가 중간에 A 또는 B로 위장하여 개입
  - A로 위장: A라고 주장하면서 통신 개시
  - B로 위장: C가 B의 네트워크 주소에서 대기하다가A가 B에 연결하면 B로 행세
  - A와 B사이 쌍방위장: A와 B사이에서 C가 A에게는B로, B에게는 A로 위장
- 재전송 형태
  - 전송 메시지 복사후 나중에 단순 재전송
  - 시간 범위 내에서 재전송(time stamp, sequential number)
  - 발견될 수 없는 재전송 : 원본 메시지 정지후, 재전송 메세지만 전송
  - 수정없이 역방향 재전송 : 송신자에게 재전송, 내용차이가 없을때

인증 종류

- 메시지 내용 인증(message content authentication)
  - verifying that the content of a received message is the same as when it was sent.
  - MAC (송신자 계산 MAC : 수신자 계산 MAC)
- 메시지 출처 인증(message origin authentication)
  - verifying that the sender of a received message is the same one recorded in the sender field of a message.
  - 디지털 서명 (송신자 필드 내용 : 실제 송신자)
- 실체 인증(general entity authentication)
  - verifying that a principal's identity is as claimed.
  - 인증 프로토콜 (신청자 주장 : 검증자 확인)
- 단독인증(unilateral or one-way authentication)
  - only one principal verifies the identity of the other principal.
- 상호인증(mutual authentication)
  - both communicating principals verify each other's identity.

인증 함수

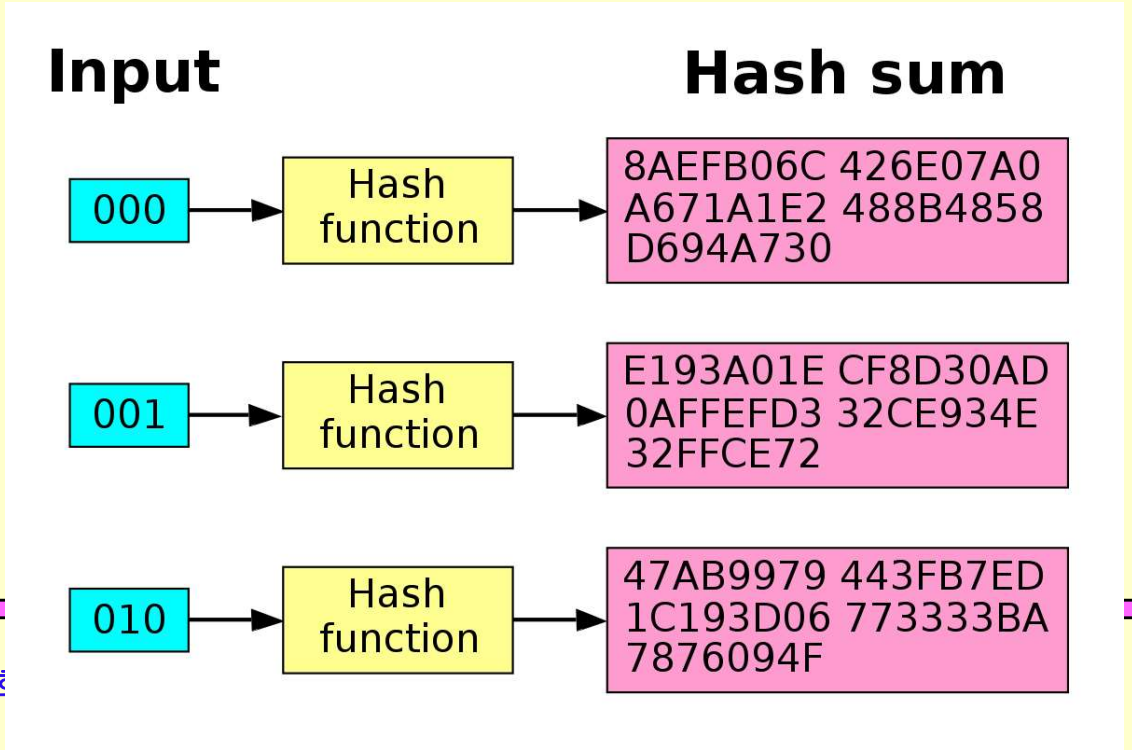
- 메시지 인증과 디지털 서명에서 인증
  - 2단계로 구분 가능
    - 하위단계: 인증에 사용할 인증자 (authenticator) 생성
    - 상위단계: 상위 프로토콜에서 인증자를 사용하여 인증성 검증
- 인증자 생성
  - 메시지 암호화: 메시지 전체 암호문이 인증자
  - 메시지 인증 코드(MAC): 인증자로 사용될 고정될 길이의 어떤 값
    - 메시지와 비밀키를 적용하여 생성한 공개 함수
  - 해쉬함수: 임의의 길이 메시지를 고정된 길이의 해쉬값으로 대응
    - 메시지가 축약 된 것과 같은 특성을 반영

해쉬함수(Hash function)

- 메시지 인증 코드에 대한 변형
- 메시지의 모든 비트들에 대한 함수
  - ❖ 쇄도 효과가 크다.
- 정의
  - ❖ 임의의 길이(M)를 취해서 정해진 크기(h)의 Message Digest를 만드는 one-way function(H)

  - ❖ 디지털서명, 인증, 무결성, 부인 봉쇄 등의 서비스 제공

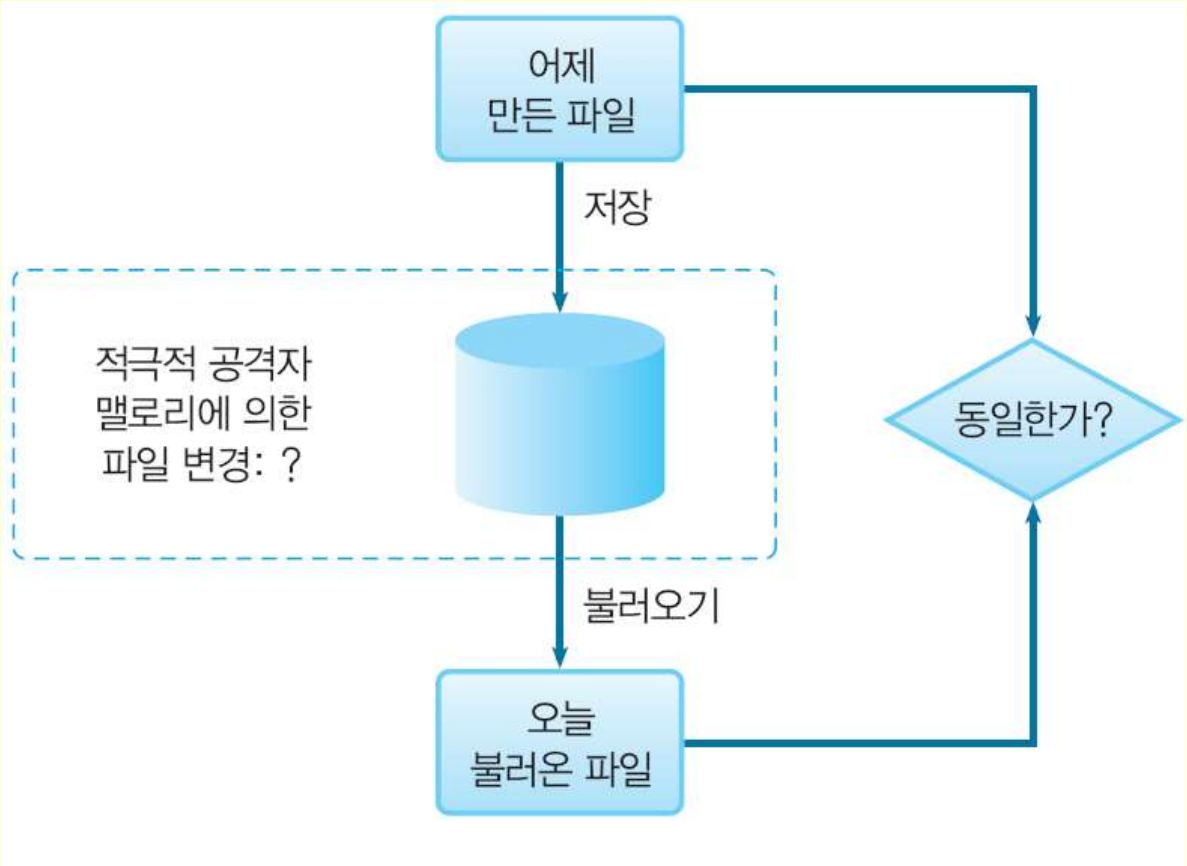
- 쇄도 효과 (Avalanche Effect)
  - ❖ 눈사태 효과
  - ❖ 어떤 암호 알고리즘이 입력값에 미세한 변화를 줄 경우 출력값에 상당한 변화가 일어나는 성질
  - ❖ 모든 암호에서 핵심적으로 요구되는 **암호학적 특성**
  - ❖ 특히 **블록 암호나 단방향 해시 함수**에서 주로 요구
  - ❖ 혼돈과 확산(confusion, diffusion) 개념에서의 **확산**



해쉬함수(Hash function)

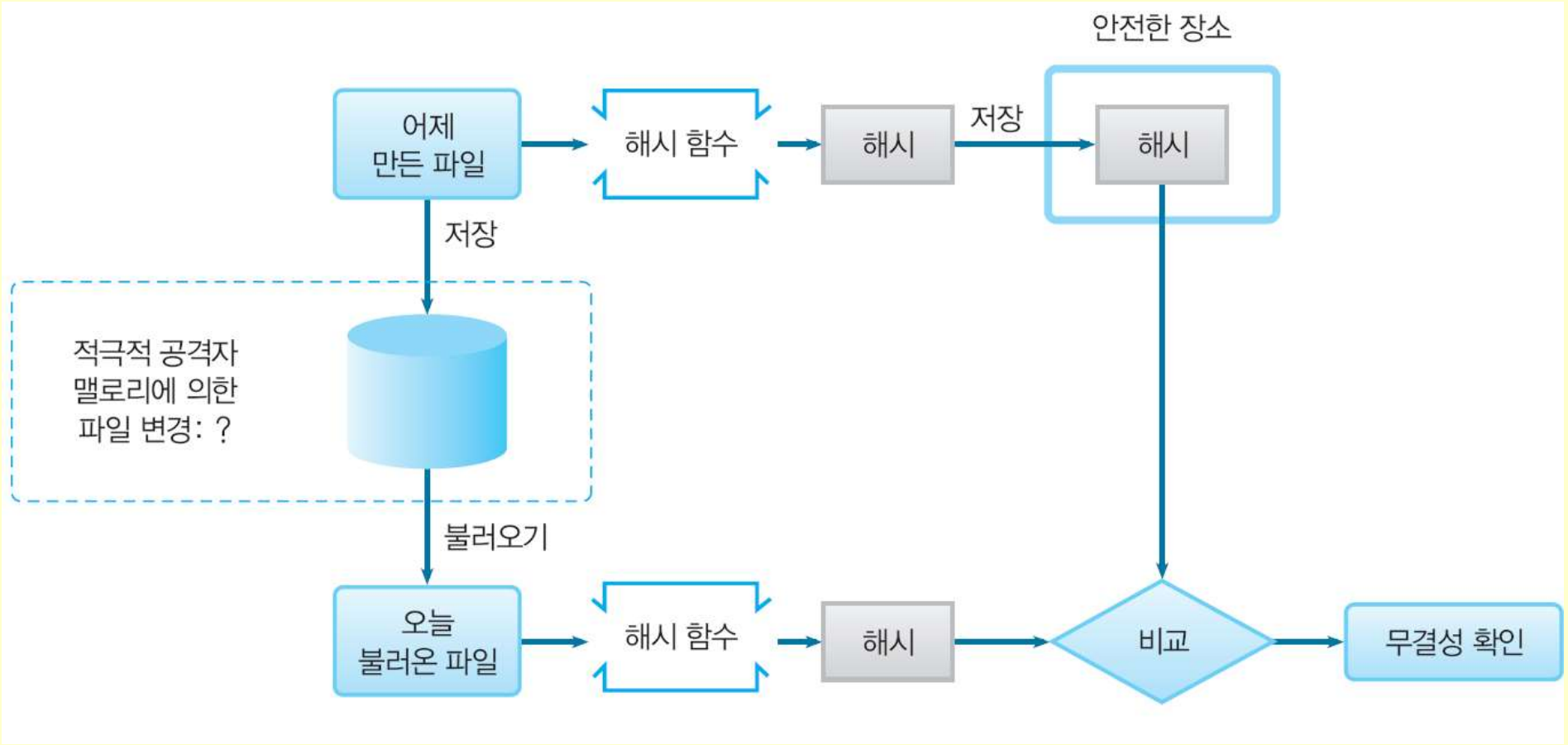
❑ 무결성(integrity) : 파일이 변경되지 않았음

❖ 어제 저장한 파일과 오늘의 파일 비교



해쉬함수(Hash function)

- **파일을 비교하는 대신에 해시 값을 비교하는 방법**



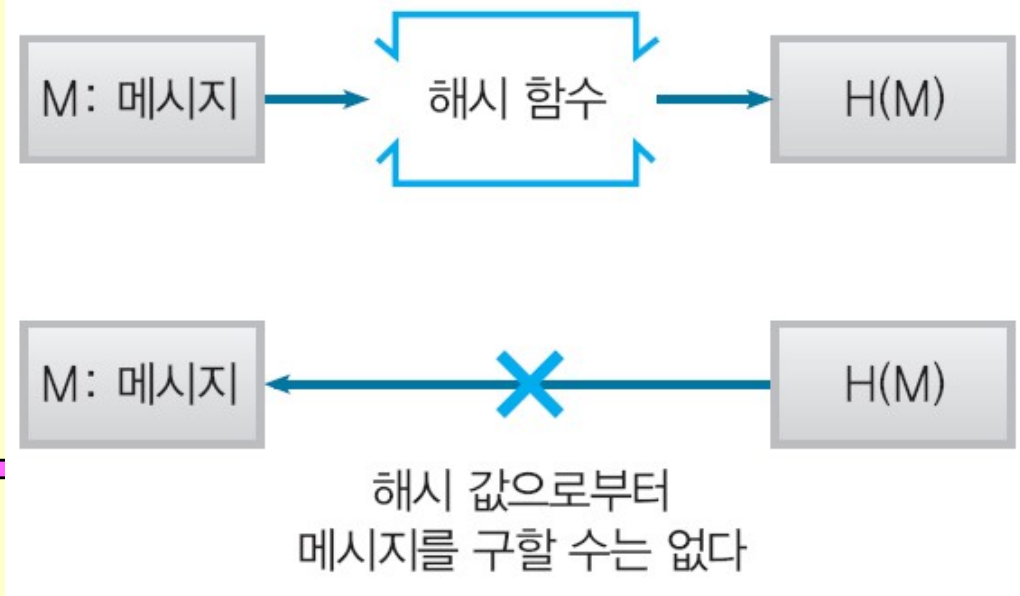
일방향 해쉬함수(One way Hash function)

- 일방향 해시 함수(one-way hash function)
  - 입력과 출력이 각각 1개씩 있다.
    - 입력은 메시지(message)
    - 출력은 해시 값(hash value)
  - 일방향 해시 함수는 메시지를 기초로 해서 해시 값을 계산
  - 해시 값의 길이는 메시지의 길이와는 관계가 없다.
    - 입력 값에 관계없이 고정된 길이의 해시 값을 출력(예: SHA-1의 출력은 항상 160비트(20바이트))

일방향 해쉬함수(One way Hash function)

❑ 일방향 해시 함수의 성질

- ❖ 임의의 길이 메시지로부터 고정 길이의 해시 값을 계산한다
- ❖ 해시 값을 고속으로 계산할 수 있다
- ❖ 메시지가 다르면 해시 값도 다르다
- ❖ 일방향성을 갖는다
  - ➢ 해시 값으로부터 메시지를 역산할 수 없다는 성질
  - ➢ 메시지로부터 해시 값을 계산하는 것은 간단히 할 수 있다
  - ➢ 해시 값으로부터 메시지를 계산하는 것은 불가능해야 한다



일방향 해쉬함수(One way Hash function)

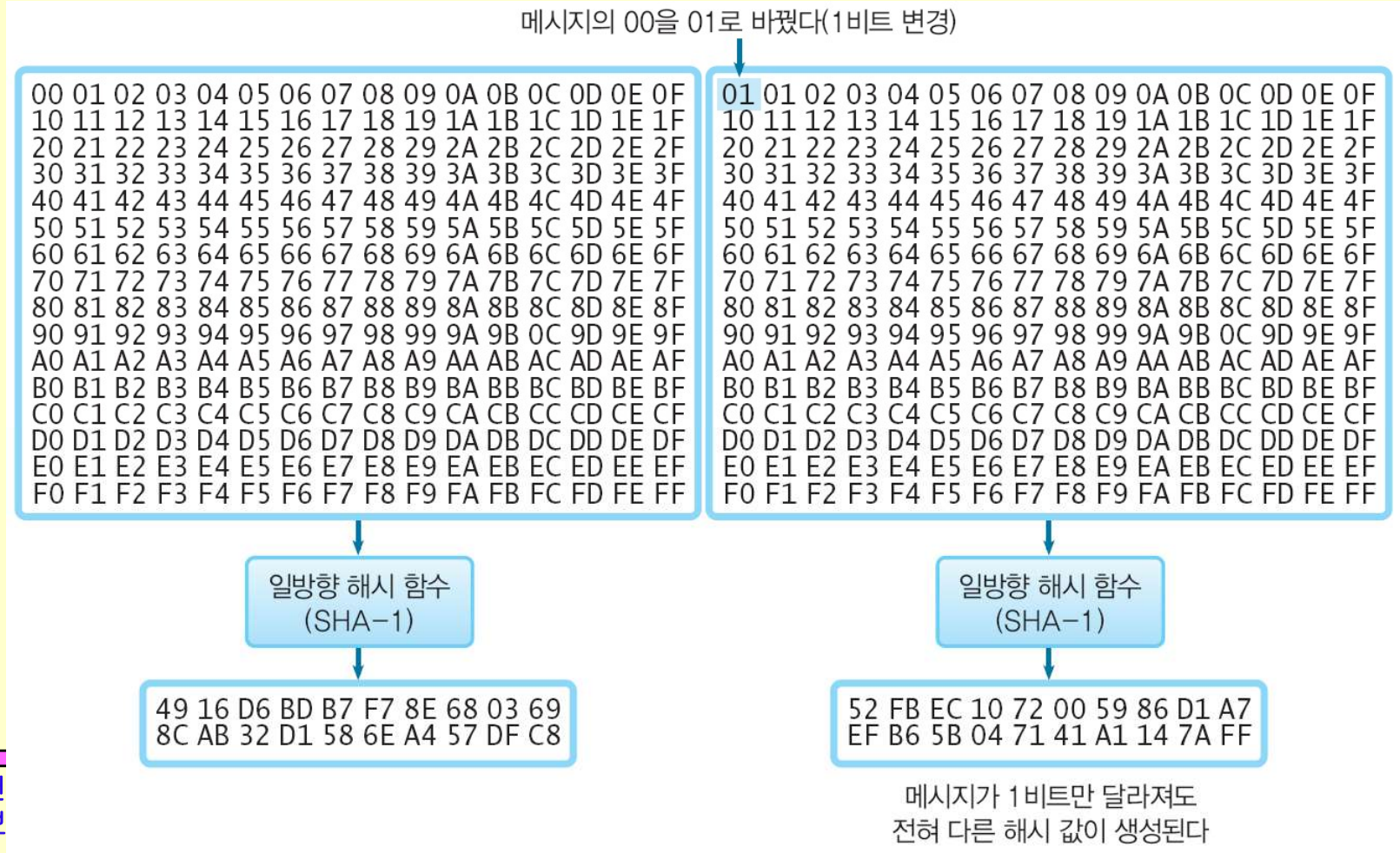
- 일방향 해시 함수의 성질
  - 고정길이 출력
    - 어떠한 크기의 메시지라도 크기에 관계없이 입력으로 사용할 수 있어야 한다
    - 어떤 길이의 메시지를 입력으로 주더라도 일방향 해시 함수는 짧은 해시 값을 생성
  - 빠른 계산 속도
    - 해시 값 계산은 고속이어야 한다
    - 메시지가 길어지면 해시 값을 구하는 시간이 길어지는 것은 어쩔 수 없다
    - 현실적인 시간 내에 계산할 수 없다면 소용이 없다

일방향 해쉬함수(One way Hash function)

❑ 일방향 해시 함수의 성질

❖ 메시지가 다르면 해시 값도 다르다

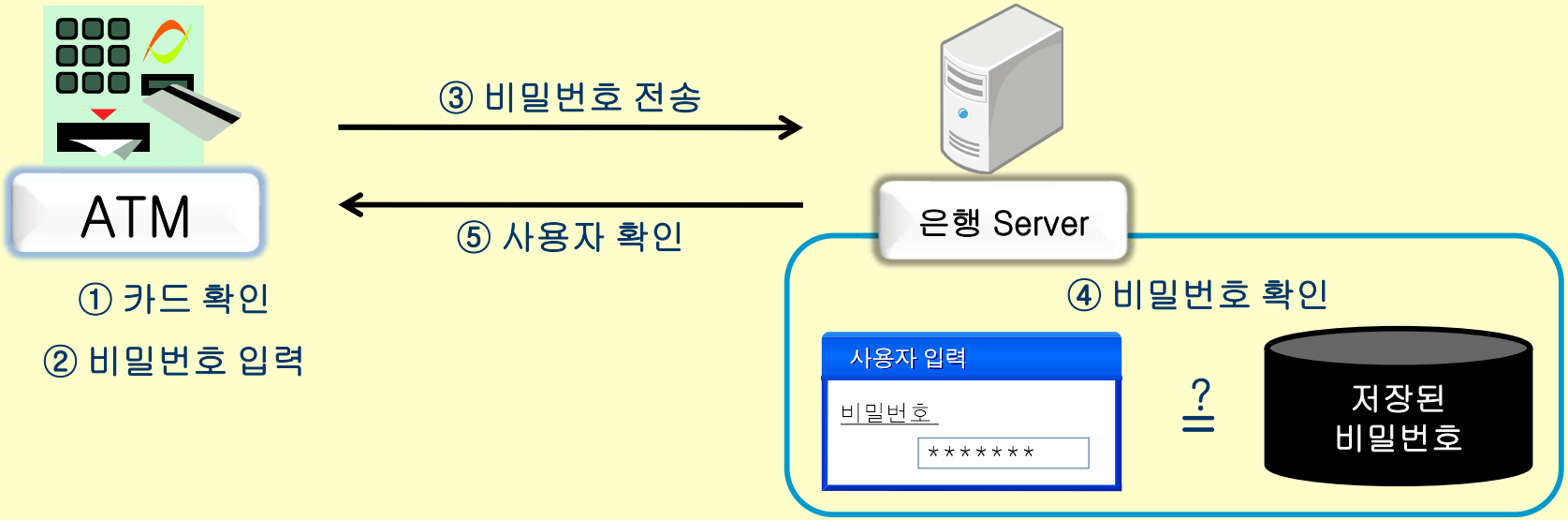
- ➢ 메시지가 1비트라도 변화하면 해시 값은 매우 높은 확률로 다른 값이 돼야 한다



패스워드 기술

❑ 패스워드

- ❖ 컴퓨터 시스템에 접속을 요구하는 사용자가 실제 사용허가를 받은 **본인인지 여부를 확인**하기 위해 사용되는 일련의 문자열
- ❖ 컴퓨터 시스템의 설정에 따라 다르긴 하지만, 대체로 4~16글자 사이에서 결정하는 경우가 많음



패스워드 기술

- 사용자와 서버간에 이루어지는 가장 일반적인 신원 확인 방식
- Password
  - group password :
    - 한 시스템에서 모든 사용자에게 공통적으로 사용
    - 유출 가능성
  - unique password :
    - 높은 보안성, password 관리상의 문제점
  - 유일하지는 않으나 개인 신분 확인이 가능한 password :
    - 사용자의 신원과 그들의 password를 함께 관리
  - one-time password
    : password replay attack 방지
    : password를 동적으로 산출
    : 가장 강력한 인증 시스템

❑ 기존 패스워드 방식

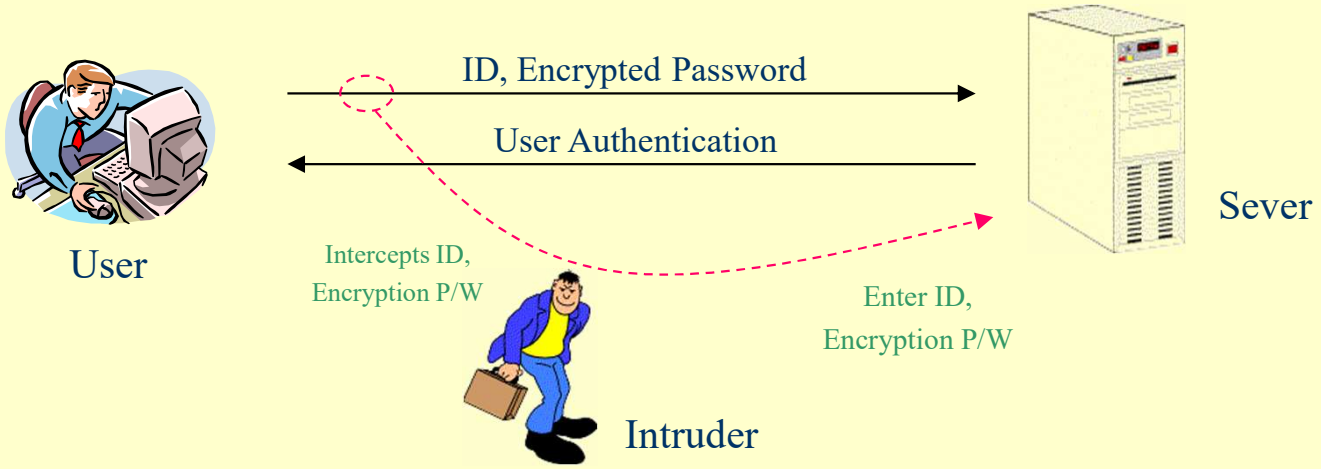
- ❖ 정적인 패스워드
- ❖ 보안성이 낮으며 쉽게 노출 가능한 불완전한 인증방식
- ❖ 보통 사용자들은 기억하기 쉽고 추측이 가능한 단어, 숫자들로 패스워드 구성

❑ OTP (One Time Password)

- ❖ 매번 다른 비밀번호로 사용자를 인증하는 일회용 비밀번호
- ❖ 현재 사용하는 비밀번호로부터 다음번에 사용할 비밀번호를 유추하는 것이 수학적으로 불가능한 특성이 있음
- ❖ 의미있는 단어, 숫자패턴, 특정사용자와 연관된 문자 등으로 구성되지 않음
- ❖ 매번 다른 비밀번호를 생성하는 동적인 특성을 가짐

Password Theft

➔ 전송 도중 침입자에 의해 가로채어지고 해석될 수 있다.



❑대책

❖전송시 암호화

- ➢단말기에서 암호화, Server에서 복호화
- ➢password replay attack이 가능

❖one-time password : 토큰 카드의 사용

❑ One-Time Password

❖ 개념

- ➢ 보안 시스템에 단 하나의 접근을 허락하는 유효한 password를 예측할 수 없도록 동적으로 산출하는 것
- ➢ 종종 토큰 카드 사용
- ➢ one-time password는 재사용되지 않음

❖ 목적

- ➢ 인증시에 사용되었던 서로 다른 password를 구분
- ➢ replay attack 방지

❖ password 결정 방법

- ➢ 랜덤한 password 목록에 대한 동기화
- ➢ 의사-난수 발생기를 사용하는데 각 end-user들은 순차 생성기 상태를 동기화
- ➢ time-stamp를 사용, 동기화된 시간을 유지

❑ OTP의 개요

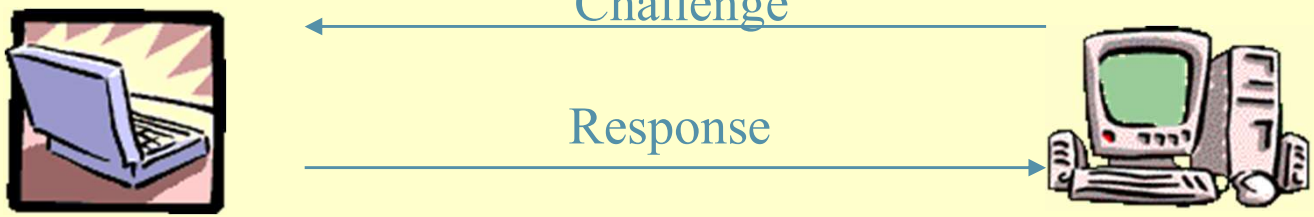
❖ OTP (One-Time Password)

- ➢ 일회용 패스워드
- ➢ 매번 다른 패스워드로 사용자 인증
- ➢ 현재의 패스워드로부터 다음에 사용할 패스워드를 유추하는 것이 수학적으로 불가능함

❖ OTP 종류

- ➢ 비동기화 방식 OTP
  - ▪ 질의-응답 방식(Challenge-Response)
- ➢ 동기화 방식 OTP
  - ▪ 시간 동기화 방식(Time-Sync)
  - ▪ 이벤트 동기화 방식(Event-Sync)
  - ▪ 시간-이벤트 조합 방식(Time-Event-Sync)

- One-Time Password의 종류
  - Challenge-Response 방법
    - 1) 사용자의 login 시도
    - 2) 서버가 사용자에게 Challenge 전송
    - 3) 사용자는 생성기에 비밀문장(Pass-Phrase) 입력
    - 4) 생성기는 One-time password를 생성
    - 5) 서버에게 password 전송



❖DES Challenge-Response 방법

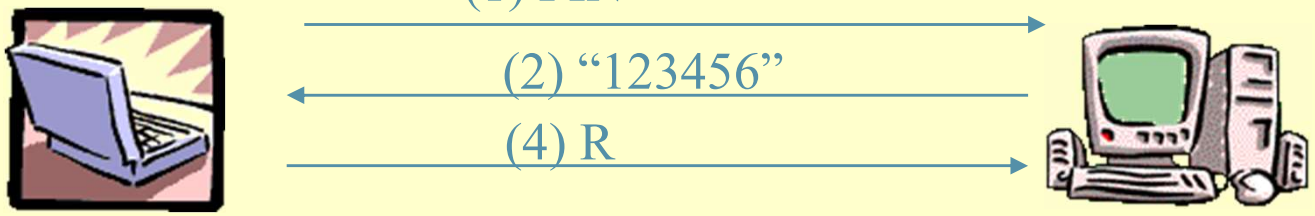
1) 사용자는 인증 서버에게 식별번호(PIN) 전달

2) 서버는 난수를 생성해서 Challenge로 반환

3) 사용자는 자신의 비밀키로 난수를 DES 알고리즘으로 암호화

4) 암호화된 난수로 Response 전달

5) 서버는 사용자의 PIN으로 키를 검색, 난수를 DES로 암호화한 후 비교



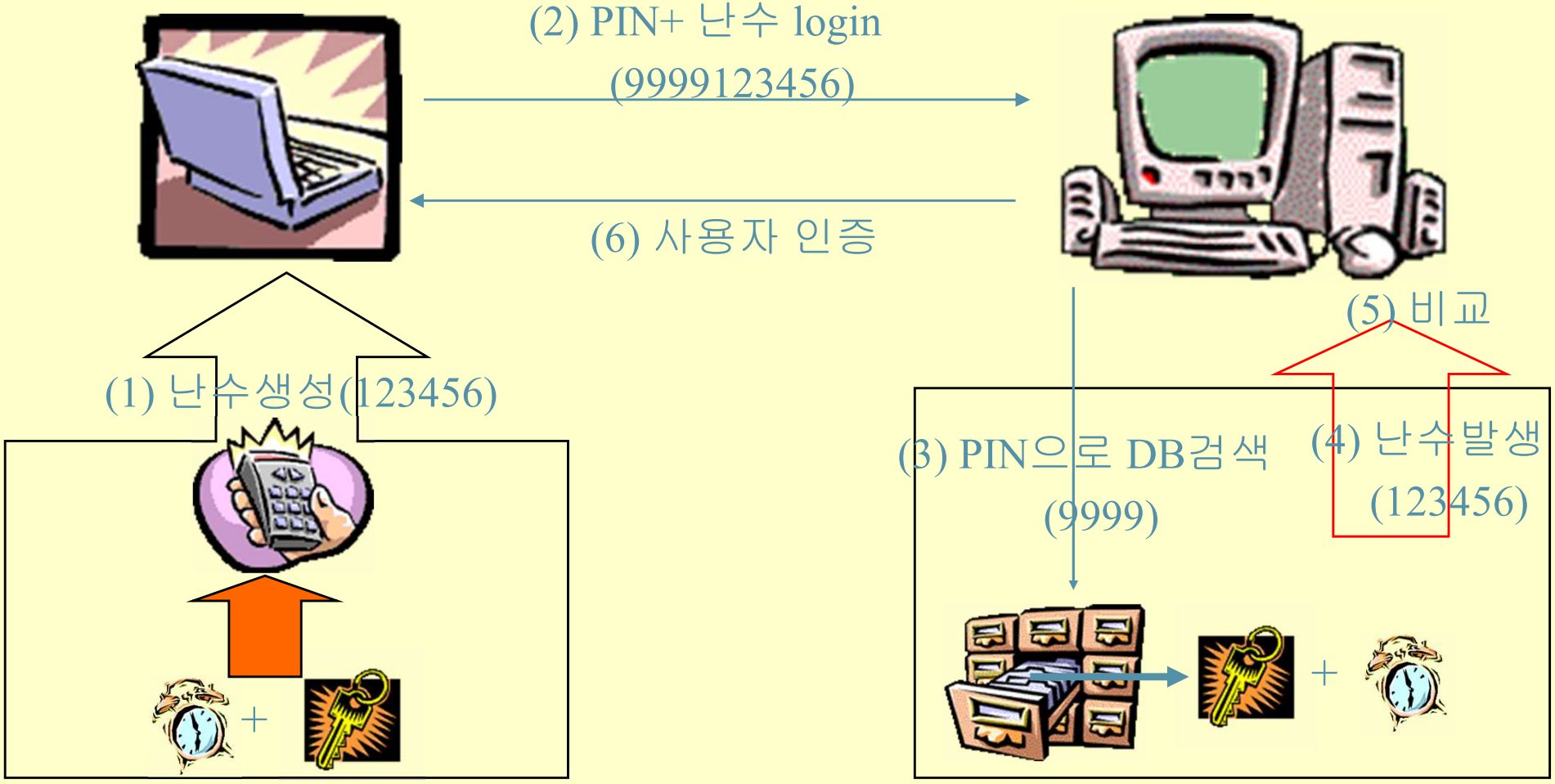
(3) $R=E_{KEY}(123456)$

(5) $R=?=E_{KEY}(123456)$

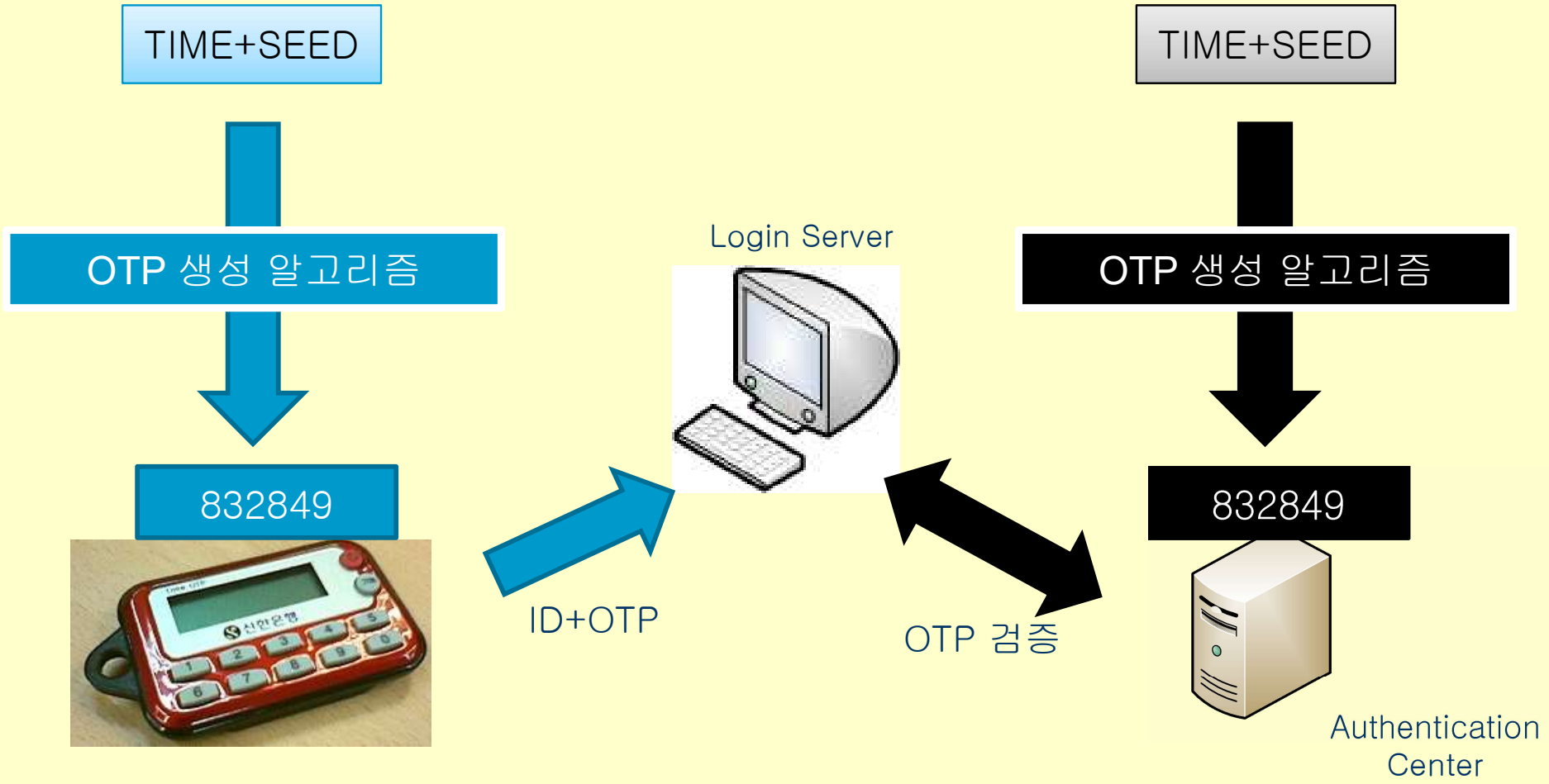
❖Time-Synchronous 방법

1) 각각의 사용자에게 특정한 Key 할당
2) 사용자가 서버에 로그인 시도
3) 사용자는 키와 현재 시간을 알고리즘에 입력해서 난수 생성
4) 사용자는PIN(Personal Identification Number)과 난수 발송
5) 서버는 PIN을 Index로 사용자의 키 검색
6) 검색된 키+ 현재시간을 알고리즘에 입력해서 난수 생성
7) 두 개의 난수를 비교

✓동일한 난수 생성을 위한 시간의 동기화 문제
✓주어진 입력 시간내에 도청/공격 가능


(2) PIN+ 난수 login
(9999123456)
(6) 사용자 인증
(1) 난수생성(123456)
(5) 비교
(3) PIN으로 DB검색
(9999)
(4) 난수발생
(123456)

❖ Time-Synchronous 방법



❑ OTP 기기 구성

❖ 기존의 고정된 35개 숫자를 반복하는 보안카드 비밀번호 대신 OTP 기기가 생성하는 6자리 숫자로 된 일회용 비밀번호를 이용하여 보다 안전하게 거래할 수 있음