# 정보보호개론

제1장 암호기술 개요

## 1. 정보보호 서비스와 암호기술

### 1.1 비밀성과 무결성

정보보호(information security)란 정보에 대한 비인가된 접근, 사용, 유출(disclosure), 수정, 파괴 등을 방지하거나 발견하고 복구하기 위한 기술적 방법을 말한다. 정보를 보호할 때 가장 기본적으로 고려되는 서비스는 **비밀성**(confidentiality), **무결성**(integrity), **가용성**(availability)이다. 이들을 정보보호의 3대 핵심 서비스라고 하여 "CIA triad"로 불린다. 여기에 **인증**(authentication)을 추가하는 경우도 종종 있다. 이 중에 사용이 요구될 때 해당 서비스를 사용할 수 있도록 하는 가용성을 제외한 3가지 서비스는 **암호기술**(cryptography)을 사용하여 제공되는 경우가 많다. 암호기술이란 메시지를 안전하게 유지하는 기술과 학문을 말한다. 과거에 암호기술은 비밀성을 보장하기 위한 기술에 초점을 두었지만 현재에는 공격자들이 고의로 공격을 하더라도 운영 중인 정보 서비스가 정상적으로 동작하도록 하거나 부당한 이득을 취할 수 없도록 다양한 기술을 개발하고 연구하고 있다.

비밀성이란 인가된 개인, 단체, 프로세스만 데이터의 내용을 볼 수 있도록 해주는 서비스를 말하며, 다른 용어로 기밀성이라고도 한다. 비밀성을 제공할 때에는 보호해야 하는 데이터의 중요도, 보호해야 하는 기간에 따라 다른 강도의 메커니즘을 사용한다. 예를 들어 인터넷 쇼핑 과정에서 신용카드 정보를 인터넷 쇼핑몰에 전송할 때에는 제3자들이 얻을 수 없도록 비밀성이 보장된 형태로 전달하여야 한다.

무결성은 데이터의 수명 동안 데이터의 정확성(내용의 불법적인 변경이 없는)을 유지하고 보증하는 것을 말한다. 여기서 변경이란 데이터의 추가, 수정, 삭제 등을 말한다. 하지만 디지털 데이터는 쉽게 수정이 가능하기 때문에 비밀성과 달리 데이터를 불법적으로 변경하는 것을 물리적으로 완벽하게 막는 것은 어렵다. 특히, 개방된 네트워크로 전달되는 데이터는 더욱더 어렵다. 따라서 무결성 서비스는 보통 불법적인 변경을 발견할 수만 있도록 해준다. 예를 들어 인터넷 뱅킹에서 특정 금액을 이체할 때 이체액을 전송 중간에 변경할 수 없어야 한다. 무결성 서비스는 중간에 금액이 변경되는 것을 막아주는 것이 아니라 전송 중간에 변경되면 이를 알 수 있게 해준다.

### 1.2 인증

인증은 주장된 것을 검증하는 것을 말하며, 주장하는 것이 무엇인지에 따라 그 의미가 많이 달라질 수 있다. 통신 프로토콜에서 인증은 보통 크게 메시지 인증, 메시지 원천지(origin) 인증, 개체(entity) 인증으로 분류한다. 메시지 인증은 무결성과 같은 의미이며, 메시지 원천지 인증은 메시지가 송신된 위치 또는 송신자를 검증하는 것을 말한다. 메시지 인증과 원천지 인증을 이처럼 분리하여 고려할 수 있지만 보통 메시지 원천지 인증은 메시지 인증과 송신자 인증을 포괄하는 개념으로 많이 사용한다. 특히, 메시지의 무결성이 확인되지 않으면 보통 송신자 인증을 주장하기 어렵다. 우리가 정보보호를 논할 때 사용자를 언급하면 이것은 실제 개인을 말할 수 있고, 개인이 사용하는 소프트웨어 또는 장치를 말할 수 있다. 따라서 문맥에서 무엇을 말하고 있는지 잘 살펴볼 필요가 있다. 일반적으로 서비스가 물리적 위치에 따라 제한되지 않기 때문에 정보보호에서 위치는 보통 중요하지 않다. 하지만 응용에 따라

위치 정보가 중요한 경우도 있으며, 최근 많은 웹 서비스는 자주 사용하는 기기나 위치가 아닌 경우에는 사용자에게 알림을 주어 계정에 대한 필요한 보호 조치할 수 있게 해준다.

우리가 가장 흔하게 접하는 인증 서비스는 개체 인증이다. 즉, 주장된 신원을 검증하는 것이다. 메시지 원천지 인증에서도 송신자를 검증할 수 있지만, 개체 인증과의 차이점은 보통 개체 인증은 인증의 최근성까지 확인이 가능해야 한다. 개체를 인증할 때에는 크게 다음 세 가지 요소를 사용한다.

- 사용자만이 알고 있는 지식(what one knows)
- 사용자만의 독특한 특징(what one is)
- 사용자만이 가지고 있는 것(what one has)

우리가 웹사이트에 로그인할 때 가장 많이 사용하는 것이 패스워드이다. 패스워드는 사용자만이 알고 있는 지식을 이용하는 인증 서비스이다. 사용자만의 독특한 특징이란 사용자의 생체 정보를 이용하는 것이다. 현재 지문, 홍채인식, 얼굴인식 등 다양한 생체 정보를 이용하고 있으며, 한 가지 생체 정보만 이용하지 않고 여러 개를 동시에 사용하는 경우도 많다. 생체 정보를 이용하기 위해서는 영상인식, 음성인식과 같은 기술이 필요하다. 하지만 생체 정보를 이용한 인증이란 저장되어 있는 정보와 현재 인식된 정보가 같은지 비교하는 방식이기 때문에 인식된 정보와 저장된 정보에 대한 적절한 보호가 필요하며, 이 과정에서는 암호기술이 사용될 수밖에 없다. 열쇠, 출입 카드 등이 사용자만이 가지고 있는 것을 이용하는 인증방식이다.

보통 인증의 안전성을 높이기 위해 한 가지 요소만 사용하지 않고 여러 요소를 동시에 사용하는 경우가 많다. 특히, 두 가지 요소를 사용하면 이를 2-factor 인증이라 한다. 예를 들어 은행 ATM 기기에서 현금을 인출할 때 우리는 보통 카드나 통장을 사용하며, 추가로 비밀번호(pin 번호)까지 입력해야 인출할 수 있다. 따라서 ATM 기기에서 현금을 인출할 때는 사용자만이 가지고 있는 것과 그 사용자만이 알고 있는 것을 모두 이용하는 2-factor 인증을 사용한다. 최근에 웹 서비스를 사용할 때 보안 강도를 높이기 위해 2단계 인증을 사용하는 경우가 늘어나고 있다. 여기서 2단계 인증은 두 단계를 통과해야 접속을 허용한다는 개념이며, 각 단계에서 다른 요소를 사용하지 않을 수 있다. 예를 들어 구글의 2단계 인증은 패스워드 인증 이후 다양한 방법 중 한 가지 방법(예: 보안이 취약할 수 있지만 등록된 핸드폰 SMS로 전달된 코드를 사용할 수 있음)으로 추가 검증 코드를 제공해야 한다. 두 번째 단계에서는 보통 사용자만이 가지고 있는 핸드폰을 활용하기 때문에 사용자만이 가지고 있는 것을 활용하는 것으로 간주할 수 있다. 따라서 이 경우 이 방식은 2-factor 인증이자 2단계 인증이 된다.

## 1.3 부인방지

비밀성, 무결성, 인증, 가용성 외에 또 많이 필요로 하는 정보보호 서비스가 **부인 방지**(non-repudiation)이다. 부인방지란 지난 행위나 약속을 부인하지 못하도록 하는 서비스이다. 보통 행위를 한 사용자 또는 약속한 사용자가 그 과정에서 어떤 증거물을 남기게 되며, 나중에 이 증거물 때문에 부인할 수 없게 된다. 부인방지는 보통 제3자가 이 증거물을 확인할 수 있어야 한다. 따라서 개체 인증보다 강한 개념이다.

부인 방지는 다양한 응용에서 다양한 이유로 필요할 수 있다. 통신 프로토콜에서 메시지 송수신과 관련해서는 크게 다음과 같은 4가지 부인 방지 서비스가 필요하다[1].

- 송신 부인방지(Non-Repudiation of Origin, NRO)
- 전달 부인방지(Non-Repudiation of Delivery, NRD)
- 제출 부인방지(Non-Repudiation of Submission, NRS)
- 수신 부인방지(Non-Repudiation of Receipt, NRR)

2자 간 메시지를 직접 교환할 경우에는 송신 부인방지와 수신 부인방지만 필요하다. 하지만 중계자를 이용할 경우에는 송신과 수신 부인방지 외에 전달 및 제출 부인방지까지 필요하다. 제출 부인방지는 중계자가 메시지 중계를 위해 메시지를 받은 사실을 부인하지 못하도록 해주고, 전달 부인방지는 수신자가 중계자로부터 메시지를 받았다는 사실을 부인하지 못하도록 해준다.

앞서 언급한 바와 같이 행위자가 증거물을 남겨야 하며, 이 증거물을 부인방지 토큰이라고 한다. 즉, 송신자는 메시지를 송신하고 자신이 송신하였음을 증명하여 주는 토큰을 수신자에게 전달해야 한다. 수신자는 메시지를 수신한 후에 수신하였음을 증명하여 주는 토큰을 생성하여 송신자에게 전달해야 한다. 나중에 상대방이 행위를 부인하였을 때 보관된 토큰을 통해 누가 부정하고 있는지 확인할 수 있게 된다. NRS와 NRD는 모두 중계자가 생성하지만 한 가지 특이한 점은 NRD는 자신의 지난 행위를 부인하지 못하도록 하기 위해 사용하는 것이 아니라 지난 행위를 하였다는 증거를 남기는 형태이다. 보통 NRD에 NRR이 포함되어 있다.

## 1.4 프라이버시

앞서 설명한 비밀성부터 부인 방지까지는 전통적으로 정보보호에서 널리 사용한 서비스이다. 반면에 **프라이버시** 보호는 현재의 지식정보화 및 유비쿼터스 시대가 본격화되면서 정보보호에서 가장 중요하게 요구되는 서비스이다. 이것은 정보화의 가장 큰 부작용이 개인 프라이버시 침해이기 때문이다. 프라이버시란 개인(또는 집단)이 자신 또는 자신의 정보를 선택적으로 노출할 수 있는 권리를 말한다. 이를 위해 개인은 자신과 연관되는 정보가 수집되고 저장되는 것을 직접 제어하거나 영향을 줄 수 있어야 한다. 하지만 오늘날 사회는 George Orwell의 소설 '1984'에서 등장하는 "Big Brother"라는 독재자처럼 실제 개인의 모든 일거수일투족을 관찰하는 것이 가능하다. 도로, 건물 곳곳에 설치된 CCTV, 물건을 살 때 사용하는 신용카드 기록, 이동할 때마다 스마트폰이 접속한 기지국 정보 등 개인의 일거수일투족이 실제 기록되고 있다.

프라이버시와 관련하여 정보보호에서 제공하고 싶어 하는 서비스는 개인 정보 노출을 포함하여 컴퓨팅 서비스를 사용하는 과정에서 프라이버시 침해를 방지하는 것이다. 이 측면에서 프라이버시 보호는 익명성(anonymity)[1] 제공과 동일한 것으로 간주하기도 한다. 프라이버시 보호를 논할 때 누구로부터 프라이버시를 보호하고자 하는 것인지도 중요하다. 보통 제3자에게 노출되는 것만을 보호하는 경우가 대부분이다. 특히, 과금을 포함한 다양한 이유로 서비스 제공자에게 노출되는 것까지는 보호하기 힘들다.

프라이버시는 크게 내용 프라이버시, 행동 프라이버시, 위치 프라이버시로 분류할 수 있다. 예를 들어 사용자가 유튜브를 통해 어떤 동영상을 보고 있다고 하자. 내용 프라이버시란 어떤 동영상을 보는지 숨기는 것을 말하며, 행동 프라이버시는 유튜브 서비스를 이용하고 있다는 것 자체를 숨기는 것을 말한다. 참고로 행동 프라이버시가 보장된다고 자동으로 내용 프라이버시가 보장되는 것은 아니다. 그 반대도 마찬가지이다. 보통 내용 프라이버시는 비밀성 서비스를 통해 보장하며, 행동 프라이버시는 익명 기술을 통해 보장된다. 위치 프라이버시란 유튜브 서비스를 어디서 이용하고 있는지 숨기는 것을 말하며, 여기서 위치는 물리적 위치를 말한다. 위치 프라이버시가 지속해서 노출되면 위치 추적(location tracing)이 된다고 말한다.

디지털 서비스를 사용할 때 교환된 통신 메시지를 수집하고 관찰하면 그것을 사용한 사용자의 프라이버시가 침해될 수 있다. 행동 프라이버시가 보장되기 위해서는 다음 두 가지 요구사항이 충족되어야 한다.

- **불관찰성**(unobservability): 특정 메시지를 전송한 또는 수신한 개체를 알 수 없어야 한다는 것을 말한다.
- **불연결성**(unlinkability): 두 개의 메시지가 주어졌을 때 동일한 송신자가 전송한 것인지 또는 동일한 수신자에게 보내는 것인지 연결할 수 없어야 한다는 것을 말한다.

불연결성은 특정 메시지의 불관찰성이 깨졌을 때 그 파급효과를 최소화하기 위한 것이다. 예를 들어 홍길동이라는 하나의 익명만을 사용하여 서비스를 사용할 경우 불관찰성은 제공될 수 있지만, 불연결성은 제공되지 않으며,

[1] 익명성은 개체와 행동(또는 정보)을 연결하지 못하게 해주는 것을 말한다.

홍길동이 실제 누구인지 밝혀지면 그동안 홍길동이라는 익명으로 이용된 모든 것이 노출된다.

프라이버시가 절대 침해되지 않도록 서비스가 제공되면 사용자들은 이를 악용할 수 있다. 따라서 프라이버시는 조건부로 제공되는 것이 필요하다. 조건부 프라이버시란 법률에 따라 필요할 경우 법률에 정해진 기관이 특정 메시지의 익명을 철회(revocation)할 수 있는 경우를 말한다. 특정 기관이 단독으로 익명을 철회할 수 있는 능력을 보유하고 있으면 해당 능력을 남용하는 것이 언제든지 가능하기 때문에 사용자들이 서비스 이용을 꺼릴 수 있다. 따라서 정보보호에서는 이와 같은 문제를 해결하기 위해 권한을 분산할 수 있는 암호기술을 사용한다. 이 기술을 **임계 기반 비밀 공유기법**(threshold-based secret sharing)이라 한다.이 기법은 어떤 능력을 $n$명에게 나누고, 이 중에 $n$보다 적은 $t$명 이상이 동의하면 해당 능력을 사용할 수 있도록 하는 기술이다. 여기서 $t$는 보안 변수(security parameter)이다. 보안 변수란 해당 값을 변경함으로써 보안 강도를 조절할 수 있는 값을 말한다. $t$가 크면 클수록 보안 강도가 높아지는데 $t = n$이 되면 가용성 측면에서 꼭 필요할 때 해당 능력을 발휘하지 못할 수 있다.

## 2. 통신계층과 암호기술

현재 인터넷은 TCP/IP 프로토콜을 사용하고 있으며, 암호기술 통신 프로토콜은 확장성, 유연성 등의 이유로 여러 계층으로 나누어 구성되어 있다. 계층은 크게 송신 노드와 목적 노드 간에 이루어지는 단대단(end-to-end) 기능을 하는 것과 중간 이웃 노드 간 기능을 하는 것으로 구분된다. 이렇기 때문에 통신 메시지에 암호기술의 적용은 종단 간에 이루어질 수 있고, 중간 이웃 노드 간에 이루어질 수 있다. 하지만 두 방식은 그 효과가 다음과 같이 다르다. 이때 비밀성 서비스를 위해 암호기술이 적용한다고 가정하자.

- (안전성 측면) 첫째, 종단 간 암호기술을 적용하면 중간 노드들은 메시지 내용을 볼 수 없다. 하지만 링크 간 암호기술을 반복적으로 적용하면 메시지 내용이 중간 노드에게 공개된다.
- (효율성 측면) 둘째, 종단에서만 암호기술이 적용되므로 종단 노드들만 암호 모듈을 가지고 있으면 되지만 링크 간 방식은 모든 노드가 암호 모듈을 가지고 있어야 한다. 또 링크 간 지연을 무시하면 종단에서만 암호기술이 적용되므로 링크 간과 달리 속도가 더 빠르다.
- (강건성 측면) 셋째, 암호화하는 방식에 따라 중간에 오류가 발생하면 종단 간 방식은 메시지 단위로 암호화하기 때문에 재전송해야 하는 부분의 크기가 클 수 있지만, 링크 간 방식은 패킷 단위로 암호화할 수 있으므로 오류가 발생한 패킷만 재전송하여 문제를 해결할 수 있다.
- (프라이버시 측면) 넷째, 종단 간 방식은 헤더가 공개된 상태로 종단 간 전달되므로 트래픽 분석이 가능하지만 링크 간 방식은 종단 헤더 정보는 숨겨지고 링크 간 헤더만 공개되므로 트래픽 분석이 어려워진다.

트랙픽 분석이란 한 사용자와 다른 사용자 간에 얼마나 자주 얼마만큼의 데이터를 교환하는지 분석하는 것을 말한다. 실제 현장에서 사용되는 종단 간 비밀성을 보장하는 표준 프로토콜은 TLS(Transport Layer Protocol)이다. 웹 브라우징을 할 때 http 대신에 https를 사용하면 TLS 프로토콜이 사용되는 것이다. 반면에 링크 간 비밀성을 보장하는 표준 프로토콜은 IPsec이다[2]. 참고로 종단 간 암호화와 링크 간 암호화를 동시에 하는 경우도 있다.

## 3. 암호기술 기초

암호기술을 본격적으로 설명하기에 앞서 앞으로 사용할 몇 가지 용어부터 알아보고자 한다. 전통적으로 암호기술은 메시지의 비밀성을 보장하기 위해 사용되었다. 메시지의 비밀성을 보장하기 위해서는 기존 메시지를 암호기술을 사용하여 조작하여야 한다. 이때 암호기술을 적용하기 전 데이터를 **평문**(plaintext, cleartext)이라 하고,


<그림 1.1> 암호화와 복호화 과정

조작된 후 데이터를 **암호문**(ciphertext)이라 한다. 비밀성을 보장하기 위해 평문을 암호문으로 조작하는 과정을 **암호화**(encryption)라 하고, 암호문을 다시 평문으로 바꾸는 과정을 **복호화**(decryption)라 한다. 현대 암호화 함수와 복호화 함수는 그림 1.1처럼 키를 사용하며 그것의 안전성이 키의 비밀성에 의존한다.

암호기술은 공격자가 존재하는 상황에서 서비스가 안전하게 이루어지도록 하는 기술을 개발하고 연구하는 학문을 말하며, 암호해독기술(cryptanalysis)은 암호기술을 분석하여 그것의 문제점을 발견하는 기술을 연구하는 학문을 말한다. 문제점을 찾는 이유는 공격을 하기 위한 것이 아니라 암호기술의 문제점들을 보완하기 위한 것이다. 암호학(cryptology)이라는 용어는 암호기술과 암호해독기술을 결합한 용어이다.

암호기술은 정보보호 서비스를 제공할 때 중요하게 필요로 하는 기술이지만 다음과 같은 한계를 가지고 있다.

- 한계 1. 암호기술이 모든 보안 문제를 해결할 수는 없다. 앞서 언급한 바와 같이 가용성은 암호기술로 제공할 수 없으며, 사회공학(social engineering) 공격은 암호기술로 방어할 수가 없다. 사회공학 기술이란 시스템 내부 권한을 가진 사람을 매수하여 정보를 얻는 등, 컴퓨팅 외적으로 공격을 하는 것을 말한다.
- 한계 2. 암호기술은 제대로 구현하고 올바르게 사용하지 않으면 효과가 없을 수 있다.
- 한계 3. 비전문가가 직접 설계하여 사용할 수 있는 기술이 아니다.

이와 같은 한계 때문에 정보보호 서비스를 개발할 때 표준 기술을 사용해야 하며, 공식적으로 널리 사용하는 암호 라이브러리를 활용해야 한다. 또 다른 범죄와 마찬가지로 기술의 한계를 극복하기 위해 필요한 법을 제정해야 한다. 우리나라의 경우 개인정보 보호법과 정보통신망 이용촉진 및 정보보호 등에 관한 법률 등이 여기에 해당한다. 이와 같은 법은 공격자를 처벌할 수 있도록 하여 사이버 공격을 억제하거나 의무적으로 특정 정보를 다루는 정보서비스를 운영하면 특정 수준의 정보보호 인력과 보안장비를 갖추도록 하고 있다.

보안 문제를 해결하기 위해 암호기술을 선택할 때는 적절성(appropiateness), 강도(strength), 비용(cost)을 고려해야 한다. 주어진 보안 요구사항을 충족할 수 있는 적절한 도구를 선택해야 하며, 선택된 도구는 필요한 수준의 보안 강도를 제공해야 하고, 비용이 타당해야 한다. 여기서 비용은 금전적 비용만을 말하는 것은 아니다. 사용의 편리성, 효율성까지 포함하여 비용을 생각하여야 한다. 실제 응용에서 보안 메커니즘의 선택을 결정하는 가장 중요한 요소는 보통 비용이다.

## 참고문헌

[1] J.A. Onieva, J. Lopez, J. Zhou, Secure Multi-Party Non-Repudiation Protocols and Applications, Advances in Information Security, Vol. 43, Springer, 2009.

[2] S. Kent, K. Seo, “Security Architecture for the Internet Protocol,” IETF RFC 4301, Dec. 2005

## 퀴즈

1. 다음 중 3대 정보보호 서비스에 포함되지 않는 것은?

   ① 인증
   ② 비밀성
   ③ 가용성
   ④ 무결성

2. 다음 중 2-factor 인증이 아닌 것은?

   ① 은행 ATM 기기에서 서비스를 사용하기 위해 은행카드와 비밀번호를 요구한 경우
   ② 집 출입문이 열기 위해 비밀번호와 지문을 요구한 경우
   ③ 핸드폰 잠금을 해제하기 위해 비밀번호와 비밀패턴을 요구한 경우
   ④ 웹 서비스에 로그인하기 위해 비밀번호와 SMS로 전달된 인증 코드를 입력해야 하는 경우 (가정. 실명 가입된 핸드폰이 없으면 해당 메시지를 가로챌 수 없음)

3. 임계기반 비밀 공유기법과 관련된 다음 설명 중 틀린 것은?

   ① 권한을 분산하여 권한 남용을 방지할 때 사용하는 기술이다.
   ② $(t, n)$ 임계 기반 기법에서 $t$는 보안 변수로 $t$를 높이면 보안 강도가 내려가고 $t$를 줄이면 보안 강도가 올라간다.
   ③ $(n, n)$도 사용할 수 있지만 가용성 측면에서 바람직하지 않다.
   ④ $(t, n)$ 임계 기반 기법은 권한을 $n$명에게 분산하고, 이 중 $t$명 이상이 동의하면 해당 권한을 수행할 수 있게 하는 방식이다.

4. 불관찰성만 제공하면 약한 프라이버시, 불관찰성과 불연결성을 모두 제공하면 강한 프라이버시가 제공된다고 하자. 다음 중 강한 프라이버시에 해당하는 것은? 단, 서술된 것 외에 IP 주소, CCTV 등을 통해 프라이버시가 노출되는 것은 고려하지 않고 답하시오.

   ① 하나의 고정된 익명으로 댓글을 쓸 수 있는 경우
   ② 선불교통카드로 대중 교통을 이용한 경우 (해당 카드는 회원가입 후 등록된 카드는 아님)
   ③ 하나의 가명을 이용해 여러 책을 출판하고 있는 경우
   ④ 카카오 또는 네이버 QR 코드 체크인을 이용하여 출입 시설에 체크인을 한 경우 (QR코드는 매번 바뀐다.)

## 연습문제

1. 비트 코인에서 개인 사용자들은 주소로 식별된다. 사용자가 보유한 코인는 이 주소와 연결되며, Alice가 Bob에게 일정한 금액의 비트 코인을 전달하고 싶으면 Alice는 Bob의 주소를 알아야 한다. 사용자는 여러 개의 주소를 만들어 사용할 수 있다. 한 사용자가 주소를 하나만 사용할 경우와 여러 개 사용할 경우 불관찰성, 불연결성 측면에서 분석하시오.

2. 프라이버시 보호를 위해 불관찰성과 불연결성이 모두 요구된다고 한다. 불관찰성은 보장되지만 불연결성이 보장되지 않으면 어떤 문제가 발생할 수 있는지 설명하시오. 불연결성이 프라이버시 보호에 왜 필요한지 설명하시오.

3. 은행 ATM기기를 제외하고 일상 생활에서 여러분이 사용하는 서비스 중 하나를 선택하여 그 서비스에서는 어떻게 개체 인증(어떤 요소를)을 하고 있는지 설명하시오.

4. 본인이 직접 사용해 본 실제 암호기술이 사용되고 있는 서비스를 하나 설명하시오. 어떤 서비스에 어떤 암호기술이 어떻게 사용되고 있는지 조사하여 간단히 서술하시오.