# ▣ 학습목표

1. 인터넷 보안 서비스 요구사항에 대해 설명할 수 있다

2. 암호화 기법을 구분하고 설명할 수 있다

# ▣ 학습내용

1. 인터넷 보안 서비스 요구사항

1) 악의적인 인터넷 이용자

* 통신중인 특정 정보에 대한 접근
* 입수한 정보를 악의적으로 이용
* 특정 시스템에 대한 악의적인 공격

2) 인터넷 보안 서비스 종류

* 기밀성(Confidentiality)
* 무결성(Intergriy)
* 인증(Authentication)
* 부인방지(Non-repudiation)
* 접근제어(Access Control)

3) 기밀성(Confidentiality)

* 정보가 제3자에게 노출이 되더라도 통신에 참여하지 않는 제 3자는 해당 정보를 이해할 수 없게 만드는 기법

4) 기밀성 보장 원리 : 암호화(Encryption)

* 송신자 : 미리 정의된 열쇠(Key)를 보유하고 있는 수신자만이 이해할 수 있는 형태로 데이터를 암호화
* 수신자 : 자신의 열쇠를 사용하여 복호화(Decryption)
* 열쇠가 없는 제 3자: 데이터 복호화 불가능

5) 무결성(Interity)

* 교환되는 정보가 제3자에 의해 변경되지 않았음을 보장

6) 무결성 보장 원리 – 해시(Hash) 함수

* 해시 함수 : 서로 다른 메시지를 축약(Digest)할 때 항상 다른 결과 생성
* 송신자 : 해시 함수 적용 결과를 원래 정보와 함께 송신
* 수신자 : 동일한 해시 함수를 수신 정보에 적용한 결과와 송신자가 전송한 해시 함수 결과를 비교

7) 인증(Authentication)

* 신원 식별로 상대방이 원하는 당사자인지 확인

8) 인증 서비스의 기본 – 인증서(Certificate)

* 믿을 수 있는 인증 기관(CA-Certification Authority)에서 발급하는 인증서로 상대방의 신원을 식별

9) 부인방지(Non-repudiation)

* 일상 생활에서 사용하는 서명과 동일한 서비스

10) 부인방지의 기본 – 디지털 서명(Digital Signature)

* 고유하게 부여된 열쇠(Key)로 문서(문서의 일부)를 암호화하여 송신
* 복호화 된 문서의 작성자가 자신임을 보장

11) 접근제어(Access Control)

* 허가된 사용자만 특정 자원을 사용할 수 있게 제어
* 악의적인 사용자가 시스템 또는 정보를 접근하는 것을 원천적으로 차단

12) 인터넷의 접근 제어 기법

* 방화벽(Firewall)

13) 인터넷 보안 서비스 구현 구조

암호화

(비밀키, 공개키)

디지털 서명

사용자인증

키관리

보안 기본 기술

보안 프로토콜&시스템

PGP

SSL/

TLS

IPsec

방화벽

1. 인터넷 보안 서비스 종류

* 기밀성(Confidentiality), 무결성(Integrity), 인증(Authentication), 부인방지(Non-repudiation), 그리고 접근제어(Access Control) 등

2. 기밀성 서비스

* 암호화(Encryption)를 통해 제공

3. 암호화 기법

* 대칭 열쇠 암호화(Symmetric Key Encryption)
* 공개 열쇠 암호화(Public Key Encryption)