170112 - 데이터베이스, 네트워크, 암호화

데이터베이스(db)

여러 사람에 의해 공유되어 사용될 목적으로 통합하여 관리되는 데이터의 집합

통합된 정보들을 저장하여 운영할 수 있는 공용 데이터들의 묶음

자료구조와 데이터베이스의 차이

자료구조 : 대부분 주기억장치에서 이루어질 내용
데이터베이스 : 대부분 보조기억장치에서 이루어질 내용(주로 잠자고 있는 데이터에 대한 것)

데이터베이스의 종류 – 관계형, 키-값형, 객체형, 문서형, 컬럼형

관계형(RDB) – 데이터 간의 관계도를 서로서로 만들어 놓는 것, 구조를 바꾸거나 추가하고 삭제하는 과정이 오래 걸리거나 까다로울 수 있다.

데이터를 입력하는 폼을 테이블이라고 하고, 그 하나하나 칸을 칼럼이라고 한다.

Ex) 사람을 이름 나이 학교로 나누어 저장을 할 때, 학교에 대한 자세한 정보가 아니라, 00학교에 대한 정보를 입력해 놓으면 학교이름만 물어보면 그 학교가 어떤 것인지 알게 되는 것,
Ex2) 서로 링크로 연결되어 있는 나무위키 같은 경우

Ex3) 게임 서버점검을 새벽에 하는 경우에 이런 작업일 확률이 높다.

DBMS

DataBase Management System

DataBase에 접근할 수 있는 기능을 제공하는 소프트웨어
즉, 데이터베이스계의 운영체제

Ex) MySQL, SQLite, MariaDb, PostgreSQL….

*데이터베이스는 DBMS와는 다르다.

SQL

Structured Query Language

DBMS를 통해 데이터를 관리하기 위한 구조화된 질의문을 작성하기 위한 언어

관계형 데이터베이스 관리 시스템에서 사용

구조화된 지리어

네트워크(Network)

LAN

근거리 통신망

Local Area Network

MAN

도시권 통신망

Metropolitan Area Network

WAN

광역 통신망(주로 국가 단위)

Wide Area Network

인터넷(Internet)

컴퓨터로 연결하여 TCP/IP 프로토콜을 이용해 정보를 주고 받는 컴퓨터 네트워크

InterNetwork

TCP/IP

TCP (Transmisiion Control Protocol)

IP (Internet Protocol)

즉 전송 규약이라고 생각하면 된다.

WWW

World Wide Wep

문서(웹페이지)들이 있는 정보의 저장소

분산과 연결

URL

Uniform Resource Locator

[Protocol]://[Host]:[Port]/[Path]

ftp://id:pw@192.168.1.10:777/mydir

file://localhost/movie/baseball.avi

Protocol

프로토콜

통신규약

장비 사이에서 메시지를 주고 받는 양식과 규칙의 체계,
즉 통신(네트워킹) 할 때 정해진 메시지 규칙

Http, https, ftp, sftp, telnet, ssh, ssl , smtp

http – (Hyper Text Transfer Protocol)
* 하이퍼 텍스트란? 하이퍼링크를 이용해 연결 시켜 놓은 문서들

html – (Hyper Text Markup Language)
하이퍼텍스트를 구조화 시키기 위한 언어 (지금은 아니지만 처음 시작은 하이퍼텍스트를 전송하기 위한 규약)

HTTP METHOD

GET – 무엇인가 요청할 때
Ex) 나는 이런 이런게 더 필요해, 나는 애플에 대해서 더 요청하고 싶다.

POST – 겟은 너무 보안성이 떨어질 때

Get 과 Post의 차이 – 겟은 일반적으로 웹페이지를 불러올 때(바로바로 빨리빨리 답변 받을 수 있음), 그런데 새로고침 할 때 이런 때는 미리 저장되어 있는게 올 수 있기 때문에, 새로고침 할 때는 새로운 데이터를 받는 것이기 때문에 Post방식을 쓰는 것이다.
즉 get은 빠르지만 최신정보는 아닐 수 있고, Post는 조금 느리지만 최신의 정보를 받을 수 있다.

PUT DELETE HEAD TRACE OPTIONS CONNECT 등등 – 어떤 정보를 삭제해달라, 더해달라, 연결해달라 등등 작업을 요청하는 것!

FTP

File Transter Protocol(파일을 전송하기 위한 규약)

TELNET

TErminaL NETwork(다른 컴퓨터에 접속하기 위한 네트워크)

원격 로그인을 위한 프로토콜

SSH

Secure Shell

네트워크 상의 다른 컴퓨터에 로그인하거나 원격 시스템에서 명령을 실행하고 다른 시스템으로 파일을 복사할 수 있도록 해 주는 응용 프로그램 또는 그 프로토콜

텔넷의 대용 목적으로 설계, 텔넷보다 안전함(시큐어 쉘은 암호화가 되어 있기 때문에)

SSL

Secure Socket Layer

웹서버와 브라우저 사이의 보안을 위한 프로토콜

웹브라우저가 어딘가에 정보를 전송하기 위해 암호화를 시키려고 할 때 암호에 대한 약속을 미리 해두어야 한다. 그런데 이런 암호를 푸는법, 암호화하는 법을 웹서버와 웹브라우저 둘 다 알아야 한다. 그래서 이런 약속을 서로 해놓은 것이 웹브라우저이다.

SMTP

Simple Mail Transfer Protocol

전자메일 발송 프로토콜

Ex) E-mail을 보낼 때 사용할 프로토콜

Host

호스트 : 네트워크에 연결된 모든 장치

호스트 이름 : 네트워크에 연결된 장치에 부여되는 고유한 이름

예) IP 주소(인터넷 프로토콜을 사용하기 위한 주소), 도메인 주소, MAC 주소 등등

IP Address

Internet Protocol Address

컴퓨터 네트워크에서 장치들이

서로를 인식하고 통신을 하기 위해서 사용 하는 번호

Domain Address

네트워크상에서 컴퓨터를 식별하는 호스트이름

DNS - Domain Name System

호스트의 도메인 이름을 호스트의 네트워크 주소로 바꾸거나 그 반대의 변환을 수행

MAC Address

Media Access Control Address

네트워크 어댑터에 부착된 식별자

Port

가상의 논리적 통신 연결단

번호로 구분

부연설명) 우리는 여러가지 프로토콜을 동시에 사용하고 있음, 그러나 우리가 쓰는 ran은 하나뿐, 그래서 그 하나의 선을 통해 여러가지 프로토콜이 왔을 때 논리적으로 구분해줄 수 있는 항구라고 보면 된다.

암호화

암호화 기법

대칭키

공개키(비대칭키)

해시

대칭키 암호화

암호화와 복호화에 같은 암호키를 쓰는 알고리즘

DES, AES, SEED 등

- 잠그는 열쇠와 여는 열쇠가 같다.

SEED – 우리나라에서 독자적으로 개발한 대칭키(키만 알면 모든 암호를 풀어낼 수 있다)

공개키(비대칭키) 암호화

공개키로 암호화된 데이터를 비밀키를 사용하여 복호화 할 수 있는 암호화 알고리즘

RSA 등

암호화 해시 함수

임의의 데이터(암호 등)를 고정된 길이의 데이터로 매핑하여 원래의 입력값과의 관계를 찾기 어렵게 만든 것

SHA, MD5 등