김건희 과제 2016.09.07

1. HTTP와 HTTPS는 무엇이며 그차이는 무엇인가?
   가. HTTP : 웹서버와 클라이언트간의 문서를 교환하기 위한 통신 규약
   www의 분산되어있는 서버와 클라이언트 간에 하이퍼텍스트를 이용한 정보교환이 가능하도록 하는 통신 규약
   암호화하지 않은 통신이기 때문에 도청이 가능하고, 위장 및 변조가 가능한 문제가 있습니다.

   - 하이퍼 텍스트 : 참조(링크)를 통해 독자가 한문서에서 다른문서로 즉시 접근할수 있는 텍스트입니다.
   - 프로토콜 : 컴퓨터나 원거리 통신장비 사이에서 메시지를 주고 받는 양식과 규칙의 체계이다, 상대방과의 약속

   나. HTTPS : 위의 HTTP의 문제점을 보완한 것입니다. 보안에 문제가 많은데 암호화, 인증을 더한것이 HTTPS입니다.
   이 암호화, 인증을 더하기 위해서는 HTTP통신을 하는 소켓부분을 SSL로 대체하고 있습니다.
   공통키 암호와, 공개키 암호의 양쪽 성질을 가진 하이브리드 암호 시스템입니다.

   - SSL : HTTP와 독립된 프로토콜, 네트워크 보안기술
   - 공통키 암호 : 상호간에 키를 교환하는 암호화 방식
     키를 누군가 가질경우 해독할수있는 문제가 있음
   - 공개키 암호 : 공통키 암호의 문제를 해결하기 위해 있는 방식
     서로 다른 두개의 스페어 키를 사용합니다
     비밀키(알려지면 안되는키)와 공개키(누구에게나 알려져도 되는키)

2. 국내에 공인인증서가 생긴 배경과 그 위험성은?
   가. 배경 : 1997~1999년에 IMF 경제 불황을 격으면서 정부의 외자유치를 위해 국내 통신시장을 개방하였다
   그리하여 1999년대의 뉴스를 보면 컴퓨터 보급과 인터넷 확산, 전자상거래가 생기면서
   인터넷 상거래에서 구매자의 신분이나 구입 의사를 최종확인하기위해 공인인증서가 생기게 되었다

   - 전자서명법 : 전자문서의 안전성과 신뢰성을 확보하고 그이용을 활성화하기위해 전자서명에 관한 기본적인 사항을
     정함으로서 정보화를 촉진, 국민생활의 편익을 증진시킴

   나. 위험성 : 보안상 위험, 이용자의 인증서 개인키가 쉽게 복제,유출됨, 최신의 동향에 따라가지못함
   국내인증업체의 세계인증시장진출 불가능, 공인인증서탈취용악성코드 많음, 전자금융거래법 위반
   인터넷이 보급되던 시기이기 때문에 액티브X를 어쩔수 없이 사용하게 되었다는 점

3. 위 내용을 조사하며 느낀점
   가. 느낀점 : 안전과 보안에 아주 큰 비중을 깨닫게 되었고, 알고리즘이나 자료구조가 탄탄해야겠다는 생각을 하였습니다.