[SW보안 개론- 2분반] 6월 17일, 첫 번째 단기 진행과제 (총 105점, 5점은 보너스)

다음 문제들을 꼼꼼하게 읽고 보고서를 작성하시오.

1. 최신 스마트 냉장고는 인터넷에 연결되어 사용되고 있어, connected refrigerator라고 한다. 사이버 위협 관점에서, internet-connected refrigerator가 일반 데스크톱 PC보다 더 위험한 이유를 자세히 설명하시오. (5점)
2. Internet-connected refrigerator를 보안 위협들로부터 안전하게 보호하기 위해서 취할 수 있는 방안(행위)들을 모두 나열하고 자세히 설명하시오. (5점)
3. 인터넷 뱅킹 서비스에서 발생할 수 있는 위협을 STRIDE 모델과 연관지어 설명하시오. 또한, 이들 위협을 어떤 보안 기법(메커니즘)으로 방어(또는 예방)할 수 있는지를 설명하시오. (10점)
4. Passive attack과 Active attack의 예를 들고, 또한 차이점을 STRIDE와 관련 지어 설명하시오. (6점)
5. 사용자 인증 방식으로 (1) ID/패스워드 방식, (2) 생체인증 방식(지문이나 홍채를 사용한 방식)을 사용할 수 있다. 두 가지 기법의 장단점을 서로 비교하여 설명하시오. (6점)
6. 한국에 있는 길동이(송신자)가 제작한 2GB 영화를 미국의 Bob(수신자)에게 암호화하여 안전하고 효율적으로 전송하고자 한다. 둘은 먼저 어떤 암호화 방식(들)을 사용할 것인지를 정한 다음, 진행해야 한다. 어떤 암호화 방식(들)을 사용하여 어떻게 전송하는 것이 안전하면서 효율적인지를 설명하시오. 송/수신자가 선택한 방식을 사용하여 안전하고 효율적으로 영화를 전송하는 과정을 단계별로 상세하게 설명하시오. (15점)
7. Diffie-Hellman알고리즘과 RSA알고리즘을 비교 설명하시오. 각 알고리즘의 역할 상의 차이점은? (6점)
8. Hill cipher를 사용하여, "time"을 암호화 하시오. 또한, 암호화된 암호문을 복호화 하시오. (대소문자 구별이 없으며, 단, a=0, b=1, c=2, ….). 암호화 키 행렬이 아래와 같을 때, 암호화 및 복호화 하는 과정을 자세히 설명하시오. (15점)

$$\begin{bmatrix} 12 & 3 \\ 20 & 7 \end{bmatrix}$$

9. Double Transposition을 사용하여 아래 평문(원문)을 암호화하시오. 중간 과정도 같이 보이시오. 단, Column Key는 "Keyword" 이고, Row Key는 "matrix"임. 블록 단위로 처리하기 바라며, 필요하면 추가 가정을 해도 됩니다. (5점)

   (평문) "Remember that Knowledge in youth is wisdom in age"
10. 4 개의 rail을 가진 rail fence cipher가 사용될 때 다음 물음에 답하시오. 단, 1번 rail부터 시작하고 key=4라고 가정하며 대소문자 구별 없습니다. 필요하다고 판단되면 추가 가정을 하면 됩니다. 다음 암호문을 복호화 하시오. (7점)

    (암호문) **TSAT NHIN YLDO RIEE OORA LANR ROEG**

11. 갑순이와 같은 학과에 30명(갑순이 포함)의 사람이 있을 때, 갑순이와 같은 생일을 갖는 사람이 있을 확률은? 계산식만 정확하게 작성해도 됩니다. 이 문제는 암호학적 해시 함수가 가져야 할 어떤 특성과 관련이 가장 많은가요? 그 이유를 설명하시오. (10점)
12. 공인인증서 갱신 기간이 필요한 이유는? 공인인증서를 유지하자는 의견과 공인인증서를 폐지하자는 의견이 있었습니다. 어느 쪽 의견에 찬성하나요? 그 이유를 자세히 설명하시오. (15점)