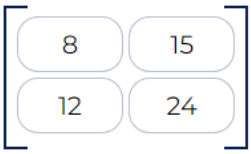
[SW보안 개론- 3분반] 6월 17일, 첫 번째 단기 진행과제 (총 105점, 5점은 보너스)

다음 문제를 읽고 물음에 구체적이고 상세하게 보고서를 작성하시오.

1. 피싱(phishing)의 유형을 2가지 이상 설명하고, 이러한 피싱 방지 방법에 대해 자세히 설명하시오. (10점)
2. 해킹된 컴퓨터는 어떻게 악용될 수 있는지를 서로 다른 방식 5가지 이상 설명하시오. (10점)
3. 안드로이드 앱에 대해, 어떠한 보안 위협이 존재할 수 있는지 3가지 이상 설명하시오. 이 보안 위협을 방어하는 기법에 대해 자세히 설명하시오. (10점)
4. 한국에 있는 길동(송신자)이가 한국에서 작성된 1GB 서류를 전자 서명(digital signature)하여 미국의 Bob(수신자)에게 효율적이면서 안전하게 전송하고자 한다. 둘은 먼저 어떤 알고리즘들을 어떤 순서로 사용할 것인지를 정한 다음, 진행해야 한다. 어떤 알고리즘들을 사용하여 무엇을 어떻게 전송하는 것이 효율적이고 안전한인지를 설명하시오. 선택한 방식으로 효율적으로 전송하는 과정을 단계별로 나누어 자세히 설명하시오. (15점)
5. Mono-alphabetic substitution cipher와 Poly-alphabetic substitution cipher 중에서 무엇이 더 안전한가? 그 이유는? (5점)
6. DES와 SEED 암호 기법(암호 알고리즘)를 비교하는 표를 작성하시오. 어느 알고리즘이 더 안전한가? 그 이유는? (10점)
7. 패스워드를 AES로 암호화하여 저장하는 방법과 SHA-256으로 해시화하여 저장하는 방법 중에서 어느 방법이 안전한지 설명하시오. 그 이유를 자세히 설명하시오. (10점)
8. Hill cipher를 사용하여, "word"를 암호화 하시오. 또한, 암호화 된 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)



9. 4 개의 rail을 가진 rail fence cipher가 사용될 때 다음 물음에 답하시오. 단, 1번 rail부터 시작하며 key=4라고 가정하며 대소문자 구별 없습니다. 필요하다고 판단되면 추가 가정을 하면 됩니다. 다음 평문을 암호화 하시오. (5점)

   (평문) **Seeing is believing**

10. 6개의 column을 기반으로 하는 Columnar transposition이 있다. 암복호화에 사용되는 키워드는 "friend"이다. 다음 암호문에 대한 평문은? 그 과정을 보이시오. 블록 단위로 처리하는 것은 권장합니다. (5점)

    (암호문) **LRNUCWVWYAYLKTTUEOLYIEUOBONNIR**

11. 한 학급에 20명의 사용자가 있을 때, 생일이 같은 사람이 존재할 확률은? 계산식만 자세하게 작성해도 좋습니다. 이 문제는 암호학적 해시 함수가 가져야 할 어떤 특성과 관련이 가장 많은가요? 그 이유를 설명하시오. (10점)