Introduction to Software Security

The 12th Quiz (6월 2일/3일 수업 내용)

Computer Security & OS Lab
Dept. of Software Science, DKU

Cho, Seong-je (조성제)

Spring, 2020

Answer the following three questions

1. Explain the differences between DES and AES ciphers
   (번역) DES와 AES 암호 기법의 차이점에 대해 설명하시오.

2. What is the difference between the AES and RSA algorithms?
   Explain the advantage and disadvantage of AES algorithm and RSA algorithm, respectively.
   (번역) AES 알고리즘과 RSA 알고리즘의 차이점을 설명하시오.
   AES 알고리즘과 RSA 알고리즘의 장점 및 단점에 대해 각각 설명하시오.

3. Explain digital signature. (1) What is the use of digital signature? And (2) How digital signature works?
   (번역) 전자서명(디지털 서명)에 대해 설명하시오. (1) 전자 서명의 용도는 무엇인가? (2) 전자 서명은 어떻게 작동하는가? 동작 방식을 설명하시오.

Solving & Writing

- Solve the question individually (by yourself).
  - You must write a report including the answers to the quizzes by yourself.
  - No cheating

- The **cover page** of the report must include
  - Title (제목): "**The 12th Quiz of Intro. to SW Security**"
  - 분반 (2분반 또는 3분반)
  - Student name, Student number
  - Date of submission

- Deadline
  - Submit your report by **11st June**

Submission

- **File** naming of the answer report for the **12th** Quiz
  - **ISS(분반)_Qz12_이름_학번_mmdd**
  - If you are in the 2nd class, name = "전우치", student number = 32171234, submission date = 9th June, then the filename for this Quiz is **ISS(2)_Qz12_전우치_32171234_0609**

- **Submit your report to TA by email.**
  - **Email** title: " SW보안개론(분반) **12**번 Quiz 답안 제출"
    - The title for the 2nd class: "**SW보안개론(2) 12번 Quiz 답안 제출**"
    - The title for the 3rd class: "**SW보안개론(3) 12번 Quiz 답안 제출**"
  - TA: 한승재 (Seungjae Han) googgkstmdwo@naver.com