Introduction to Software Security

The 13th Quiz (6월 9일/10일 수업 내용)

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

Cho, Seong-je (조성제)

Spring, 2020

Answer the following three questions

1. Explain three main differences between AES algorithm and SHA-1 algorithm
   (번역) AES 알고리즘과 SHA-1 알고리즘 사이의 주요 차이점 3가지를 설명하시오.

2. Why is a cryptographic hash function better than a public key cryptography for storing passwords securely?
   (번역) 패스워드를 안전하게 저장하기 위한 방법으로, 공개 키 암호기법보다 암호학적 해시 함수가 더 나은 지에 대해 설명하시오.

3. What is the difference between weak and strong collision resistance in cryptographic hash functions?
   (번역) 암호학적 해시 함수에서 약한 충돌 회피와 강한 충돌 회피의 차이점을 설명하시오.

4. Which is better (or more secure) of MD5 and SHA-2 hash algorithms? Why?
   (번역) MD5와 SHA-256 중에서 어떤 알고리즘이 더 나은가? 그 이유는?

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 13th Quiz of Intro. to SW Security**"
  - 분반 (2분반 또는 3분반)
  - Student name, Student number
  - Date of submission

- Deadline
  - Submit your report by **15th June**

Submission

- File naming of the answer report for the 13th Quiz
  - **ISS(분반)_Qz13_이름_학번_mmdd**
  - If you are in the 2nd class, name = “전우치”, student number = 32171234, submission date = 12th June, then the filename for this Quiz is **ISS(2)_Qz13_전우치_32171234_0612**

- **Submit your report to TA by email.**
  - Email title: “ SW보안개론(분반) **13**번 Quiz 답안 제출”
    - The title for the 2nd class: “**SW보안개론(2) 13번 Quiz 답안 제출**”
    - The title for the 3rd class: “**SW보안개론(3) 13번 Quiz 답안 제출**”

  - TA: 한승재 (Seungjae Han) googgkstmdwo@naver.com