

Introduction to Software Security

The 10th Quiz (5월 19일/20일 수업 내용)

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

Cho, Seong-je (조성제)

Spring, 2020

Answer the following questions about Crypto

1. Explain a codebook and the Enigma machine in detail, respectively.
(번역) codebook과 Enigma machine에 대해 각각 자세히 설명하시오.
2. What is Kerckhoffs's principle?
(번역) Kerckhoffs의 원리에 대해 설명하시오.
3. What is the Turing Award?
(번역) Turing Award에 대해 설명하시오.
4. What is the Turing Test?
(번역) Turing Test에 대해 설명하시오.
5. Explain the differences between Caesar cipher and Vigenère Cipher.
Which cipher is more secure between them? Why?
(번역) Caesar cipher과 Vigenère Cipher의 차이점을 설명하시오. 둘 중에서 어떤 암호가 더 안전한가? 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 10th Quiz of Intro. to SW Security**”
 - 분반 (2분반 또는 3분반)
 - Student name, Student number
 - Date of submission

- Deadline
 - Submit your report by **25th May**

Submission

- **File** naming of the answer report for the **10th** Quiz
 - **ISS(분반)_Qz10_이름_학번_mmdd**
 - If you are in the 2nd class, name = “전우치”, student number = 32171234, submission date = 22nd May, then the filename for this Quiz is **ISS(2)_Qz10_전우치_32171234_0522**

- **Submit your report to TA by email.**
 - **Email** title: “ SW보안개론(분반) 10번 Quiz 답안 제출”
 - The title for the 2nd class: “SW보안개론(2) 10번 Quiz 답안 제출”
 - The title for the 3rd class: “SW보안개론(3) 10번 Quiz 답안 제출”
 - TA: 한승재 (Seungjae Han) googgstmdwo@naver.com