Introduction to Software Security

The 11th Quiz (5월 26일/27일 수업 내용)

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

Cho, Seong-je (조성제)

Spring, 2020

Quiz (1번)

1. 알파벳과 #로 구성된, 즉 전체 27개의 문자를 사용하여 Hill cipher를 설계하였다. 암호화 키로 사용되는 암호 행렬(**A**)는 다음과 같다.

a	b	c	d	e	f	g	h	i	j	…	w	x	y	z	#
0	1	2	3	4	5	6	7	8	9		22	23	24	25	26

$$\mathbf{A} = \begin{bmatrix} 2 & 3 \\ 3 & 5 \end{bmatrix}$$

(1) 다음 평문(plaintext)에 대한 암호화 과정을 보이고, 생성한 암호문(ciphertext)을 보이시오.

평문: **`hello#`**

(2) 생성한 암호문을 복호화하는 과정을 보이시오.

Quiz (2번)

2. 5개의 column을 기반으로 하는 Columnar Transposition이 있다.
암복호화에 사용되는 키워드는 ***apple*** 이며, 키워드에서 두 번째 p는 첫 번째 p보다 알파벳 순서가 나중이라고 가정한다. 그리고, 사각형 모양이 꽉 채워지지 않을 경우, 마지막 부분에 xyza 순으로 패딩을 한다.
이 columnar transposition으로 암호화 또는 복호화할 때 다음 물음에 답하시오.

(1) 다음 평문에 대한 암호문은?

(평문) `This is a columnar transposition`

(암호문)

(2) 다음 암호문에 대한 평문은?

(암호문) **`TUOANIOCNASNDEMROOHBLRSTELUTPI`**

(평문)

Quiz (3번, 4번)

3. **5 x 4 matrix를 사용하는 double transposition cipher를 사용한다고 가정하자. row 키워드는 “apple”이고 column 키워드는 “code”일 때,**
   - 평 문 “**DYNAMITE WINTER PALACE**” 에 대한 암호문은?
   - 암호문:

4. **5 x 5 matrix를 사용하는 double transposition cipher를 사용한다고 가정하자. column 키와 row 키 모두 (2, 1, 3, 5, 4)일 때,**
   - 평 문 “**NOW IS THE TIME FOR ALL GOOD MEN**” 에 대한 암호문은?
   - 암호문:

Quiz (5번)

5. Two rails 기반의 Rail Fence Cipher가 있을 때, 다음 물음에 답하시오.

이 경우two rails이므로 key =2라고 볼 수 있다.

1) 평 문 “**nothing is as it seems**”에 대한 암호문은?

암호문:

2) 암호문 “**MKHSE LWYAE ATSOL**”에 대한 평문은?

평 문:

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 11th Quiz of Intro. to SW Security**"
  - 분반 (2분반 또는 3분반)
  - Student name, Student number
  - Date of submission

- Deadline
  - Submit your report by **1st June**

Submission

- File naming of the answer report for the 11th Quiz
  - ISS(분반)_Qz11_이름_학번_mmdd
  - If you are in the 2nd class, name = "전우치", student number = 32171234, submission date = 30th May, then the filename for this Quiz is ISS(2)_Qz11_전우치_32171234_0530

- **Submit your report to TA by email.**
  - Email title: " SW보안개론(분반) 11번 Quiz 답안 제출"
    - The title for the 2nd class: "**SW보안개론(2) 11번 Quiz 답안 제출**"
    - The title for the 3rd class: "**SW보안개론(3) 11번 Quiz 답안 제출**"
  - TA: 한승재 (Seungjae Han) googgkstmdwo@naver.com