Introduction to Software Security

The 4th Homework (4번째 과제)

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

Cho, Seong-je (조성제)

Spring, 2020

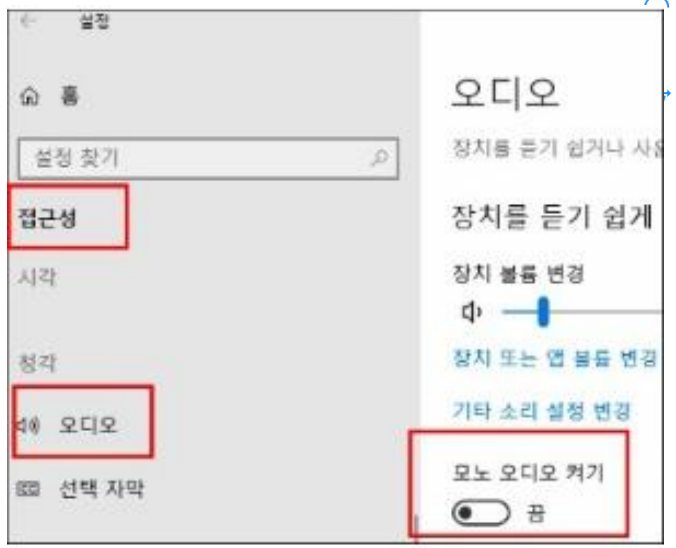
이어폰을 사용한 강의 수강에서 참고 사항

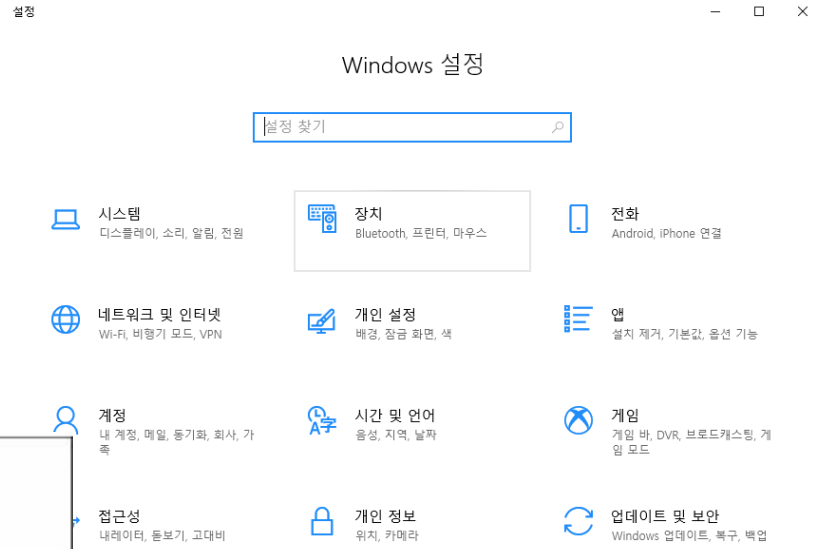
녹화 환경 설정을 조정

- 동영상 강의 내용이 한쪽 이어폰으로 들리는 현상을 해결
- 디폴트 오디오 설정으로 청취 시도

그래도, 강의 내용이 한쪽 이어폰으로 들리는 현상이 발생할 경우의 해결책:

- **Windows 10 기준**
  1. 시작 – **설정** – 접근성 클릭
  2. 접근성 – 오디오
  3. '모노 오디오 켜기 ' 를 켬(ON)으로 설정한다.
     오디오 탭의 '모노 오디오 켜기 ' 를 활성화 시키면 됨





- **"질의 응답" 칸에도 게시되어 있음.**

4번째 과제물

4번째 과제 목적 및 개요

- 4번째 과제 목적
  - Quiz 내용을 복습한다.
  - 수업 중에 익힌 중요 내용을 심층 이해한다.

- 4번째 과제 개요
  - 5번 슬라이드부터 10번 슬라이드의 질문에 대해 답하시오.
    - 각 슬라이드마다 각각 문제가 있음 (총, 10개의 문제가 있음).
    - 어떤 문제에는 sub-question이 있음.

- 4번째 과제 수행 기간
  - 5월 26일부터 6월 9일까지 (마감일: 6월 9일)

다음 질문에 답하시오. (1번과 2번)

1. 다음 Caesar Cipher와 유사한 방식으로 암호화된 다음 암호문을 복호화 하시오. 즉, 암호문에 대응하는 평문을 보이시오.
   - 암호문에 사용된 것은 단순 shift cipher로 Key는 1~25 사이임. 참고로 Caesar Cipher의 key는 3이었음.

   (암호문, ciphertext) YMJHFJXFWHNUMJWNXTSJTKYMJJFWQNJXYPSTBSFSIXNRUQJXYHNUMJWX

   (평문, plaintext)

2. Vigenère cipher가 Caesar Cipher보다 더 안전한 이유에 대해 자세히 설명하시오.

다음 질문에 답하시오. (3번)

3. 알파벳과 세 개의 구두점(, . ?)으로 구성된, 즉 전체 29개의 문자를 사용하여 Hill cipher를 설계하였다(아래 표 참조). 암호화 키로 사용되는 암호 행렬(**A**)는 다음과 같을 때, 다음 물음에 답하시오

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

P	Q	R	S	T	U	V	W	X	Y	Z	,	.	?
16	17	18	19	20	21	22	23	24	25	26	27	28	0

$$\mathbf{A} = \begin{bmatrix} 2 & 7 & 6 \\ 4 & 5 & 13 \\ 2 & 6 & 1 \end{bmatrix}.$$

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

(평문): **Hide this message**

(암호문) :

(2) 복호화 키로 사용될 행렬을 보이시오.

(3) 위 (1)에서 생성한 암호문을 복호화하는 과정을 보이시오.

다음 질문에 답하시오. (4번)

4. 7개의 column을 기반으로 하는 **Columnar Transposition**이 있다. 암복호화에 사용되는 키워드는 ***analyst*** 이며, 키워드에서 두 번째 a는 첫 번째 a보다 알파벳 순서가 나중이라고 가정한다. 이 columnar transposition으로 암호화 또는 복호화할 때 다음 물음에 답하시오.

(1) 다음 평문에 대한 암호문은?

(평문) **`The nose is pointing down and the houses are getting bigger`**

(암호문)

(2) 다음 암호문에 대한 평문은? 참고로 암호문은 총 28자로 구성되어 있음.

(암호문) **`TRLEELIGCIGEHALANTNCTECYENEN`**

(평문)

다음 물음에 답하시오. (5번)

5. 여러 개의 rail을 가진 Rail Fence Cipher가 사용될 때, 물음에 답하시오. 단 1번 rail부터 시작한다.
   - 참고로, three rails이면 key =3, five rails이면 key=5라고 볼 수 있다.

(1) Key = 3일 때, 다음 평문을 암호화 하시오.

(평문) Australian mathematics

(암호문)

(2) Key가 3일 때, 다음 암호문을 복호화 하시오.

(암호문) TRSLPEIMITRCNHBIIHODATRDNGAGHNSOOMROOISETSCUEMCEFELE

(평문)

(3) Key가 5일 때, 다음 암호문을 복호화 하시오.

(암호문) **ASNODANETISOTNMVNEMEGWFBAOGSWEREIHALVNSBTLI**

(평문)

다음 물음에 대해 답하시오. (6번, 7번, 8번)

6. 대칭키 암호 기법에서, N 명의 사용자가 서로 비밀통신을 하고자 할 때, shared secret key의 총 개수는? 그 이유는?

7. 비 대칭키 암호 기법에서, N명의 사용자가 서로 비밀통신을 하고자 할 때, 키의 전체 개수는? 그 이유는? (참고로 "비 대칭키 암호 기법" = "공개키 암호 기법"임.)

8. Diffie-Hellman key exchange 알고리즘에 대해 다음 물음에 답하시오.
   - p(소수)는 11이고 g(generator of p)는 2이라고 하자.
   - 송신자는 비밀정보(a) 9을 선정하고, 수신자는 비밀정보(b) 4을 선정했을 때,
     송신자와 수신자가 합의하게 되는 최종 비밀 값(키)를 구하시오.
     컴퓨터 계산기를 사용하거나 프로그램을 작성하여 계산 과정을 보이시오.

다음 물음에 답하시오. (9번, 10번)

9. Public-key cryptography (공개키 암호화 기법 = 비 대칭키 암호 기법)에 대해 설명하시오.
   (1) 공개키 암호화 알고리즘의 주요 용도에 대해 설명하시오.
   (2) 대칭기 암호 기법과의 차이점에 대해서 설명하시오.
   (3) Diffie-Hellman key exchange 기법과의 차이점에 대해서 설명하시오.

10. Digital signature (디지털 서명 알고리즘)에 대해 설명하시오. 동작 원리 및 용도에 대해 설명하기 바랍니다.
   - Digital signature를 전자 서명이라고도 함

☞ Public-key cryptography는 Digital signature 두 알고리즘은 “9 Algorithms that Changed the Future”(미래를 바꾼 아홉 가지 알고리즘)이란 책에서도 설명하고 있다.

보고서 작성 시 포함 내용

- **보고서 표지에 포함될 내용**
  - 과목명(SW보안 개론), 분반 표시(2분반 또는 3분반),
  - 과제번호 및 제목 (**4th 과제: 암호 기법 이해**)
  - 성명, 학번
  - 제출일 (**반드시 정확하게 표시**)

- **보고서 내용에 포함될 내용**
  1) 앞서 설명한 문제들에 대한 답변. 질문 별로 정리하면 됩니다.
  2) 참고한 교재/자료/문서/논문 등이 있으면, 해당 내용 표시하여 보고서에 포함
  3) Discussion (선택 사항)
     - 토론 및 논의 사항
     - 건의 사항

과제물 수행 방식

- 개인 과제
  - 개별적으로 조사/실습/실험하여 보고서로 정리
  - No Cheating
  - 만약, 과제 보고서 복제가 있다면, 보여준 사람과 복제한 사람 모두 0점
- 신뢰할 만한 교재/자료/문서/논문/사이트를 활용
  - 보고서 작성 시에, 참조(참고)한 교재/자료/문서/논문/사이트 정보를 포함하여 기술
  - Trusted websites: https://scholar.google.com/ , Scicece.gov, NIST – Glossary, …
- Deadline
  - 6월 9일까지

과제물 제출

- 과제 보고서 파일을 첨부하여 이메일로 제출

- 이메일 제목 및 과제보고서 파일 이름
  - 이메일 제목: "SW보안개론(분반) **4**번 과제 제출"
    - 2분반 이메일 제목: SW보안개론(2) **4**번 과제 제출
    - 3분반 이메일 제목: SW보안개론(3) **4**번 과제 제출
  - 보고서 파일 이름은 "ISS(분반)_HW**4**_이름_학번_mmdd" 형식으로
    - **예시) 3분반 홍길동 (32165678), 제출일이 6월 7일이면 →**
      "ISS(3)_HW4_홍길동_32165678_0607"

- 조재희 조교선생께 제출
  - **조재희 (jehee1204@gmail.com), 미디어센터 505호**