컴퓨터 보안_01

실습 3주차

동국대학교 CSDC Lab.
실습조교 김선규
2022.03.22 (Wed.)

Index

1. 시저 암호란?
2. 실습과제 1: 시저 암호 생성 및 복호화 실습
3. 전치 암호란?
4. 부가과제 1: 전치 암호 생성 및 복호화 실습

실습 강좌 소개

➢ 실습 진행 방법

- 간단한 이론 복습 및 해당주차 실습문제 설명
- 실습 후 보고서를 작성하여 다음주 화요일 자정(23:59) 까지 E-Class에 제출(이메일 제출 불가, 반드시 E-Class를 통해 제출)
- 실습 과제 제출 기한 엄수 **(제출기한 이후로는 0점 처리)**

➢ 실습 보고서 [1/2]

- 실습 문제에 대한 요구 사항 파악, 해결 방법 등 기술
- 프로그램 설계 / 알고리즘
  - 해결 방법에 따라 프로그램 설계 및 알고리즘 등 기술
  - 문제 해결 과정 및 핵심 알고리즘 기술
- 결과 / 결과 분석
  - 결과 화면을 캡쳐 하여 첨부, 해당 결과가 도출된 이유와 타당성 분석
- 소감
  - 실습 문제를 통해 습득할 수 있었던 지식, 느낀 점 등을 기술

실습 강좌 소개

➢ 실습 보고서 [2/2]

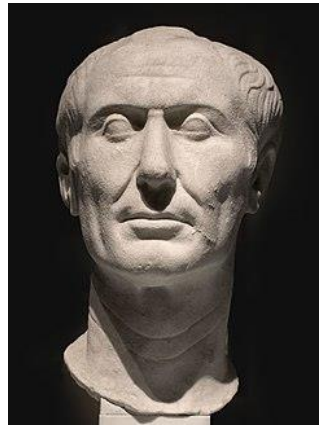
- 제출 방법
  - 보고서를 작성하여 E-Class "과제" 메뉴를 통해 제출
    - **"이름_학번_실습주차.zip" 형태로 제출 (e.g. : 홍길동_2022123456_실습3주차.zip)**
    - 파일명에 공백, 특수 문자 등 사용 금지

- 유의사항
  - 보고서의 표지에는 학과, 학번, 이름, 담당 교수님, 제출일자 반드시 작성
  - 정해진 기한 내 제출
    - **기한을 넘길 시 0점 처리**
    - E-Class가 과제 제출 마지막 날 오류로 동작하지 않을 수 있으므로, 최소 1~2일 전에 제출
    - 당일 E-Class 오류로 인한 미제출은 불인정
  - 보고서를 자신이 작성하지 않은 경우 실습 전체 점수 0점 처리

시저 암호(Caesar Cipher)

dongguk UNIVERSITY

➢ 시저 암호(Caesar Cipher)란?



- 시저 암호는 카이사르 암호라고도 불리며, 로마시대의 정치가이자 장군이었던 줄리어스 시저(Julius Caesar)가 처음 사용한 것으로 알려져있는 간단한 치환암호의 일종이다.
- 줄리어스 시저는 각 알파벳 순으로 3칸 뒤로 물려 읽는 방법으로 암호문을 작성하였으며, 이러한 치환 방식을 표로 만들면 다음과 같다.

원문자	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
대체문자	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

- 유명한 일화로, 시저는 양아들처럼 생각하던 브루투스에게 암살 당했으며, 그 직전에 전달받은 암호화된 편지는 다음과 같다.
  - 암호문: "RUSQHUVKBVEHQIIQIYDQJEH"
  - 복호화된 평문: "BECAREFULFORASSASINATOR"

실습과제 1: 시저 암호 생성 및 복호화 실습

dongguk UNIVERSITY

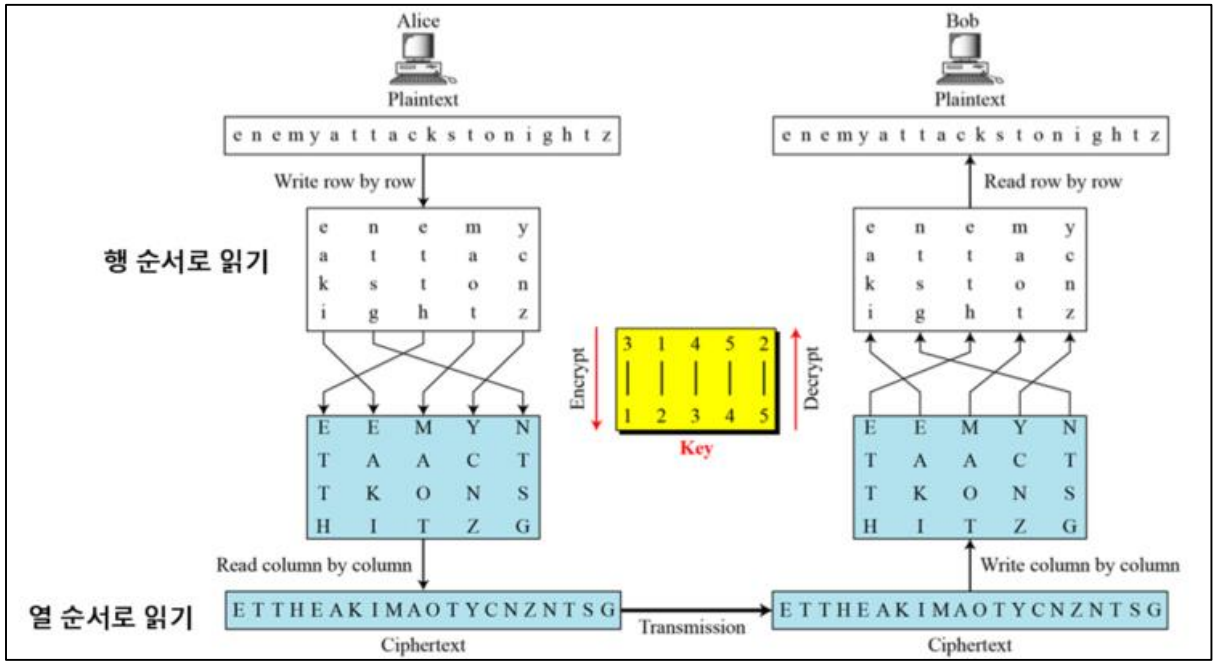
➢ 시저 암호(Caesar Cipher) Cracking Program 작성하기

1) 키워드 7개 ~10개 사이로 구성된 한 문장을 생성하는 기능을 작성하시오.
   - 해당 문장은 꼭 말이 되는 정확한 문장일 필요는 없음.
   - 단, 단어는 실존하여 사용되는 단어여야 함.
2) 생성된 문장(평문)에 시저 암호를 적용하여 암호문을 생성하는 기능을 작성하시오.
   - n만큼 shift 하는 것은 랜덤으로 생성
   - 단, shift 가능한 n의 범위는 1~25
3) 생성된 암호문을 대상으로 암호를 해독하여 평문으로 복호화 할 수 있는 일종의 해독기 기능을 작성하시오.
   - 해독기 프로그램은 n만큼 shift를 통해 말이 되는 단어와 문장의 후보군을 찾을 수 있어야함.
4) 위 내용을 100회 반복 후 암호문을 복호화 하는데 걸리는 평균 시간을 측정하여 성능 분석을 진행하시오.
5) 상용되고 있는 시저 암호 해독기 툴이 있다면, 1) 항에서 생성된 문장을 대상으로 복호화를 진행하고 4) 항과 성능을 비교 및 분석 하시오.

전치 암호(Transposition cipher)

➢ 전치 암호(Transposition cipher)란?

- 평문에 나타난 문자 또는 숫자의 기호만 바꾸는 방법으로 평문 문자의 순서를 어떤 특별한 절차에 따라 재배치하고 평문을 암호화하는 방식으로 전치(Transposition) 암호 또는 순열(Permutation) 암호 라고 한다. 대표적으로는 단순 전치 암호(simple transposition cipher) 와 Nihilist 암호가 있다.
- 단순 전치 암호(simple transposition cipher) 예제



단순 전치 암호 예제 시나리오

⊖ 평문의 작업 단위를 결정한다. 예) 다섯 문자

⊖ 작업 단위를 맞추기 위해 마지막 'ight' 에 'z' 를 추가해 평문을 정해진 열 단위로 표현한다.

⊛ 자리바꿈 맵을 이용해 행의 순서를 변경한다.

④ 변경된 문자를 열 단위로 표현한다.

부가과제 1: 전치 암호 생성 및 복호화 실습

dongguk UNIVERSITY

➢ 전치 암호(Transposition cipher) Cracking Program 작성하기

❖ 본 실습은 부가과제로써, 실습과제1을 수행한 후 본 실습을 수행할 시 가산점을 부여함.

❖ 본 실습은 앞서 살펴본 단순 전치 암호 예제를 기반으로 암호화 및 복호화를 진행함.

1) 키워드 7개 ~10개 사이로 구성된 한 문장을 생성하는 기능을 작성하시오.
   - 해당 문장은 꼭 말이 되는 정확한 문장일 필요는 없음.
   - 단, 단어는 실존하여 사용되는 단어여야 함.
2) 생성된 문장(평문)에 전치 암호를 적용하여 암호문을 생성하는 기능을 작성하시오.
3) 생성된 암호문을 대상으로 암호를 해독하여 평문으로 복호화 할 수 있는 일종의 해독기 기능을 작성하시오.
4) 위 내용을 100회 반복 후 암호문을 복호화 하는데 걸리는 평균 시간을 측정하여 성능 분석을 진행하시오.
5) 상용되고 있는 전치 암호 해독기 툴이 있다면, 1) 항에서 생성된 문장을 대상으로 복호화를 진행하고 4) 항과 성능을 비교 및 분석 하시오.

Q & A

Thank you