HW 2: Cryptography

Index

- Substitution cipher?
- 과제
- 제출

HW2

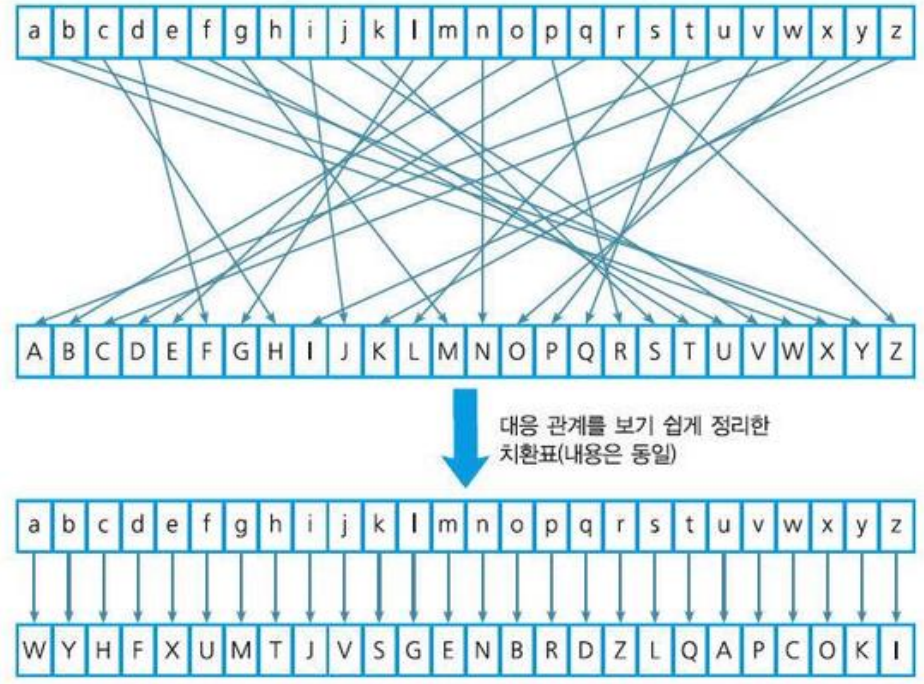
❖ 암호화 관련 실습
- 간단한 암복호화 수행 및 MD5의 충돌 실습
- HW2_Crypto 폴더

❖ 과제
1. 치환 암호 기법으로 작성된 파일(*ciphertext.txt*)을 복호화
2. 복호화된 *ciphertext.txt*에서 확인할 수 있는 key로 암호화된 이미지를 복호화
3. MD5 hash 생성 및 충돌을 확인

❖ 제출
- 과제 및 실습 수행 내용을 보고서로 제출
- 단, 복호화한 이미지가 반드시 보고서에 포함되어야 함
- 제출기간 : 5월 22일 ~ 5월 29일

Substitution Cipher?

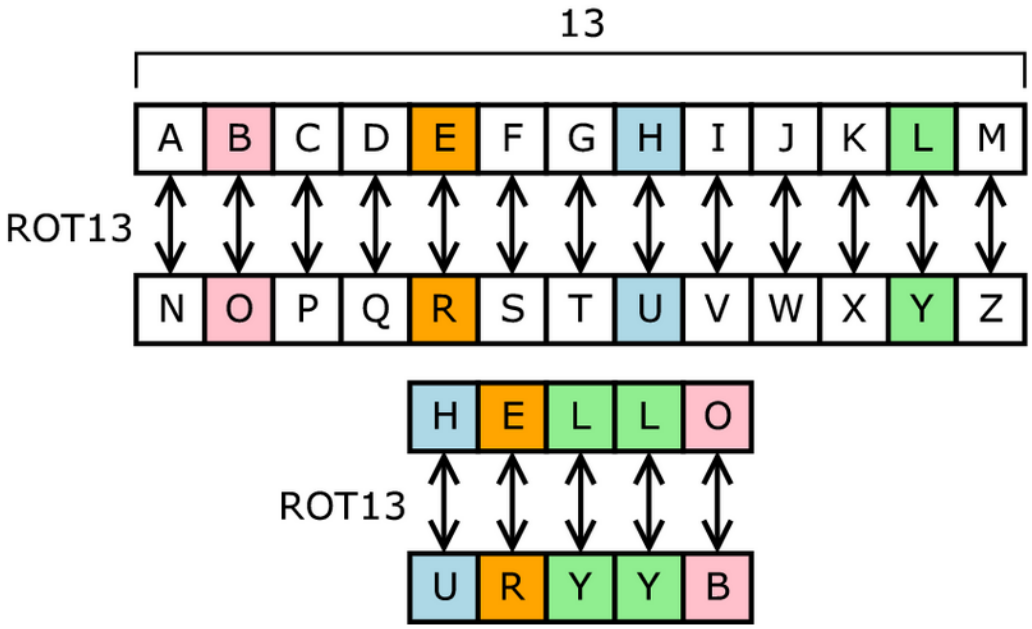
- 치환 암호
  - 평문의 알파벳을 다른 알파벳으로 변환하는 고전 암호 방식
  - 치환 방식에 따라 다양한 방식이 존재
    - 단일 치환 (알파벳의 일대일 대응)
    - 다중 치환 (알파벳의 일대다 대응)
  - 암호공격
    - bruteforce
    - 카지스키 공격 (Kasiski attack)
    - 프리드만 공격 (Friedman attack)



Substitution Cipher?

- 시저 암호(Caesar cipher)
  - 단일 치환 암호의 일종
  - 줄리어스 시저(유리우스 케사르)가 사용한 암호방식
  - 평문의 알파벳을 일정 문자 수만큼 순차적으로 이동(**Key**)시켜 암호화

  - 예시의 key는 13
  - 평문 'HELLO'는 URYYB로 암호화



과제

1. 치환 암호 기법으로 작성된 파일(*ciphertext.txt*)을 복호화
2. 암호화된 이미지 복호화
3. MD5 hash의 충돌을 확인

과제 - 1

❖ 치환 암호 기법으로 작성된 파일(*ciphertext.txt*)을 복호화

- T1 폴더 내 카이사르 암호기법으로 암호화된 문서인 *ciphertext.txt*가 존재
  - 숫자는 암호화되지 않음, 알파벳의 대소문자는 유지됨
- 암호화된 파일을 복호화하며 다음을 만족하는 프로그램을 작성
  - ***ciphertext.txt*를 복호화하여 *decrypted.txt*를 생성**할 것
  - 언어는 c, java, python 중 하나를 선택

```
Qrofkd afpzlsbop qexq Zxfokzolpp fp x Plsfbq pmv. Tebk Qrofkd zlkcolkqp
efj, Zxfokzolpp xodrbp qexq qeb Plsfbqp xob xiifbp tlohfkd clo qeb pxjb
dlxip, xka qeobxqbkp ql obqxifxqb yv afpzilpfkd Qrofkd'p pburxifqv. Tebk
qeb JF6 xdbkq Pqbtxoq Jbkwfbp xmmbxop ql qeobxqbk Zixohb, Qrofkd obsbxip
qexq Zxfokzolpp fp x pmv. Jbkwfbp obsbxip eb hkbt qefp xiobxav xka
mixkqba Zxfokzolpp ql ibxh jbppxdbp ql qeb Plsfbqp clo Yofqfpe ybkbcfq.
Cbxofkd clo ebo pxcbqv, Qrofkd qbiip Zixohb ql ibxsb Yibqzeibv Mxoh,
obsbxifkd qexq eb fp dxv. Ebxoqyolhbk, Zixohb pqxqbp peb xitxvp prpmbzqba
yrq fkpfpqp qebv tlria exsb ybbk exmmv qldbqebo xkvtxv. Xcqbo qeb txo,
Jbkwfbp qbiip qeb zovmqldoxmebop ql abpqolv qebfo tloh xka qexq qebv zxk
kbsbo pbb lkb xklqebo xdxfk lo pexob texq qebv exsb alkb.
```

ciphertext.txt

```
Turing discovers that Cairncross is a Soviet spy. When Turing confronts
him, Cairncross argues that the Soviets are allies working for the same
goals, and threatens to retaliate by disclosing Turing's sexuality. When
the MI6 agent Stewart Menzies appears to threaten Clarke, Turing reveals
that Cairncross is a spy. Menzies reveals he knew this already and
planted Cairncross to leak messages to the Soviets for British benefit.
Fearing for her safety, Turing tells Clarke to leave Bletchley Park,
revealing that he is gay. Heartbroken, Clarke states she always suspected
but insists they would have been happy together anyway. After the war,
Menzies tells the cryptographers to destroy their work and that they can
never see one another again or share what they have done.
```

decrypted.txt

과제 - 1

❖ 치환 암호 기법으로 작성된 파일(*ciphertext.txt*)을 복호화

- 보고서는 다음을 포함하여야 함
  - 프로그램의 소스코드와 설명
  - 복호화된 문서의 일부 (스크린샷 첨부)
  - 암호화 시 몇 글자를 밀어내어 암호문을 형성하였는지?(**Key**)

과제 - 2

❖ 암호화된 이미지 복호화

- T2 폴더 내 암호화된 이미지(*p1.bmp*)를 복호화
  - 복호화 시 **암호화 유형**(cipher type)과 **암호화 키**(crypto key)를 알아야 함
  - 필요한 암호화 유형과 암호화 키는 **과제 - 1의 복호화된 *ciphertext.txt*에서 확인 가능**
  - openssl enc 명령어로 복호화가 가능
    - openssl enc -d [cipher_type] -in [input_filename] -out [output_filename] -k [crypto-key]

```
seed@VM:~/.../2$ openssl enc -d -des-cbc -in p1.bmp -out p1_de.bmp -k "thisispassword"
```

→ 복호화된 이미지를 보고서에 포함

과제 - 3

❖ MD5 hash의 충돌을 확인

① 동일한 두 파일의 비교

- T3 폴더 내 *1.bin*, *2.bin*을 바이트 단위로 비교
  - vbindiff [input_file1] [input_file2]

```
[03/10/19]seed@VM:~/Desktop$ vbindiff 1.bin 2.bin
VBinDiff 3.0_beta4, Copyright 1995-2008 Christopher J. Madsen
```

- *1.bin*, *2.bin*의 hash를 비교
  - md5sum 명령어로 MD5 hash 생성 가능
  - md5sum [input_file]

```
[03/10/19]seed@VM:~/Desktop$ md5sum example
ad23b1f8ea80f5f3252de5799cdbcb32  example
```

과제 - 3

❖ MD5 hash의 충돌을 확인

② 1bit가 차이나는 두 파일의 비교

- T3 폴더 내 *1.bin*, *3.bin*에 대하여 ①을 반복

과제 - 3

❖ MD5 hash의 충돌을 확인

③ MD5 충돌이 일어나는 서로 다른 binary의 생성

- md5collgen : 고의로 MD5 충돌이 발생하는 두 binary를 생성하는 프로그램
- md5collgen –o [filename1] [filename2]

```
[03/10/19]seed@VM:~/Desktop$ md5collgen -o o1.bin o2.bin
MD5 collision generator v1.5
by Marc Stevens (http://www.win.tue.nl/hashclash/)

Using output filenames: 'o1.bin' and 'o2.bin'
Using initial value: 0123456789abcdeffedcba9876543210

Generating first block: ...........
Generating second block: S10.........................
Running time: 12.9269 s
```

- 생성된 두 파일에 대하여 ①을 반복

→ ①, ②와 ③ 과정을 통해 도출되는 결과를 보고서에 포함

제출

- 보고서는 다음을 포함하여야 함
  - 과제 1~3의 수행 과정 및 결과
  - 수행 과정 및 분석에 대한 논리적인 서술과 스크린샷

- 제출 기간: 5월 22일 ~ 5월 29일
- 수업시간에 제출하거나 미디어센터 505호로 방문 제출
  (부재 시 504호로 제출)

문의사항

- 조교 이름 : 정재민
- 연락처 : s17orlax@gmail.com

Thank you!

Q & A