Report

제출일 2019년 5월 29일
과목명 SW보안개론
담당교수 조 성 제 교 수 님
전공 공대 소프트웨어학과
학번 32144548
이름 조 창 연

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

- 프로그램의 소스코드와 설명

```
LOWER_KEY = 'abcdefghijklmnopqrstuvwxyz'
UPPER_KEY = 'ABCDEFGHIJKLMNOPQRSTUVWXYZ'

def decrypt_file(file_name, key):
        with open('decrypted.txt', 'w') as wf:
                with open(file_name, 'r') as rf:
                        for line in rf:
                                wf.write(decrypt_handler(line, int(key)))

def decrypt_handler(cipher_text, key):
        result = ''
        for m in cipher_text:
                if m.islower():
                        i = (LOWER_KEY.index(m) - key) % 26
                        result += LOWER_KEY[i]
                elif m.isupper():
                        i = (UPPER_KEY.index(m) - key) % 26
                        result += UPPER_KEY[i]
                else:
                        result += m
        return result

if __name__ == '__main__':
        input_key = input('Enter the Key Value >> ')
        decrypt_file('ciphertext.txt', input_key)
```

위 소스코드는 파이썬을 이용하여 작성되어 졌으며, 전체적인 흐름은 ciphertext.txt 파일을 한 줄씩 읽어드려 내가 입력한 킷값을 통해 대소문자를 구분하고, 구분되어진 대소문자를 decrypted.txt 파일에 써주는 방식입니다. 먼저 LOWER_KEY에 소문자, UPPER_KEY에 대문자 문자열을 각각 할당해준다. 첫 번째 함수인 decrypt_file에선 file_name과 key를 인자로 받습니다. 그리고 open 함수를 이용해 읽어드릴 파일(ciphertext.txt)을 rf, 쓰여질 파일(decrypted.txt)을 wf로 정의한 후, 한 줄씩 ciphertext.txt을 읽어가며 key값에 따라 decrypted.txt 파일에 쓰여집니다. 두 번째 함수인 decrypt_handler에선 cipher_text와 key를 인자로 받으며, 결과를 출력하기 위해 대소문자를 구별하는 코드로 작성하였습니다. 먼저 result값을 초기화 한 후, if문을 통해 대문자인지 소문자인지 구별해줍니다. 마지막으로 main을 통해 내가 입력한 keyt값에 따라 decrypted.txt 파일이 계속 바뀝니다.

- 복호화된 문서의 일부

```
[05/29/19]seed@VM:~/.../T1$ cat decrypted.txt
In 1951, two policemen, Nock and Staehl, investigate the mathematician Alan Turing after an apparent break-in at his home. Durin
g his interrogation by Nock, Turing tells of his time working at Bletchley Park during the Second World War.

In 1927, the young Turing is unhappy and bullied at boarding school. He develops a friendship with Christopher Morcom, who spark
s his interest in cryptography. Turing develops romantic feelings for him, but Christopher soon dies from tuberculosis.

When Britain declares war on Germany in 1939, Turing travels to Bletchley Park. Under the direction of Commander Alastair Dennis
ton, he joins the cryptography team of Hugh Alexander, John Cairncross, Peter Hilton, Keith Furman and Charles Richards. The tea
m are trying to decrypt the Enigma machine, which the Nazis use to send coded messages.

Turing is difficult to work with, and considers his colleagues inferior; he works alone to design a machine to decipher Enigma.
After Denniston refuses to fund construction of the machine, Turing writes to Prime Minister Winston Churchill, who puts Turing
in charge of the team and funds the machine. Turing fires Furman and Richards and places a difficult crossword in newspapers to
find replacements. Joan Clarke, a Cambridge graduate, passes Turing's test but her parents will not allow her to work with the m
ale cryptographers. Turing arranges for her to live and work with the female clerks who intercept the messages, and shares his p
lans with her. With Clarke's help, Turing warms to the other colleagues, who begin to respect him.

Turing's machine, which he names Christopher, is constructed, but cannot determine the Enigma settings before the Germans reset
the Enigma encryption each day. Denniston orders it destroyed and Turing fired, but the other cryptographers threaten to leave i
f Turing goes. After Clarke plans to leave on the wishes of her parents, Turing proposes marriage, which she accepts. During the
ir reception, Turing confirms his homosexuality to Cairncross, who warns him to keep it secret. After overhearing a conversation
 with a female clerk about messages she receives, Turing has an epiphany, realising he can program the machine to decode words h
e already knows exist in certain messages. After he recalibrates the machine, it quickly decodes a message and the cryptographer
s celebrate. Turing realises they cannot act on every decoded message or the Germans will realise Enigma has been broken.

Turing discovers that Cairncross is a Soviet spy. When Turing confronts him, Cairncross argues that the Soviets are allies worki
ng for the same goals, and threatens to retaliate by disclosing Turing's sexuality. When the MI6 agent Stewart Menzies appears t
o 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 wa
r, Menzies tells the cryptographers to destroy their work and that they can never see one another again or share what they have
done.

In the 1950s, Turing is convicted of gross indecency and, in lieu of a jail sentence, undergoes chemical castration so he can co
ntinue his work. Clarke visits him in his home and witnesses his physical and mental deterioration. She comforts him by saying t
```

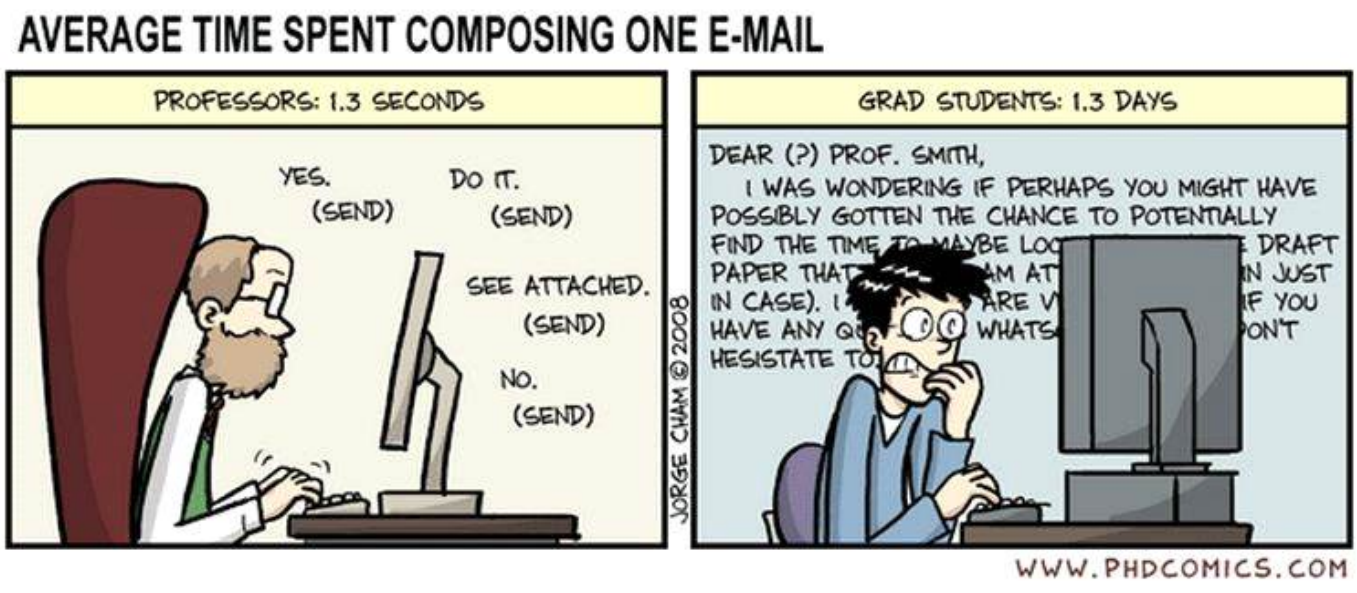
- 암호화 시 몇 글자를 밀어내어 암호문을 형성하였는가?

```
[05/29/19]seed@VM:~/.../T1$ python3 decrypt.py
Enter the Key Value >> 5
```

위 과정을 진행하며 key 값이 5라는 것을 알게 되었고, 암호화 시 총 다섯 글자를 밀어내어 암호문을 형성하고 있다는 것을 알게 되었습니다.

2. 복호화된 *ciphertext.txt* 에서 확인할 수 있는 key로 암호화된 이미지를 복호화

```
[05/29/19]seed@VM:~/.../T2$ openssl enc -d -aes-128-cbc -in p1.bmp -out p1_de.bmp -k "letmegraduate"
[05/29/19]seed@VM:~/.../T2$ ls
p1.bmp  p1_de.bmp
[05/29/19]seed@VM:~/.../T2$
```



3. MD5 hash 생성 및 충돌을 확인

① 동일한 두 파일의 비교

- T3 폴더 내 *1.bin*, *2.bin*을 바이트 단위로 비교

```
[05/29/19]seed@VM:~/.../T3$ vbindiff 1.bin 2.bin
VBinDiff 3.0_beta4, Copyright 1995-2008 Christopher J. Madsen
VBinDiff comes with ABSOLUTELY NO WARRANTY; for details type `vbindiff -L'.
[05/29/19]seed@VM:~/.../T3$
```

```
1.bin
0000 0000: 17 47 6A 0B 57 6B 96 B5  F9 EA 86 A9 A1 AF 5D EF  .Gj.Wk.. ......].
0000 0010: 23 8D 54 05 25 85 8F 78  46 D2 40 2E 88 26 BE AB  #.T.%..x F.@..&..
0000 0020: 6D DB AA EF EE 69 0A 3B  6B E4 6A 1C 96 71 50 5A  m....i.; k.j..qPZ
0000 0030: 54 DF 43 5E 9B 00 A5 D5  BA 7D ED 64 AF 1B 5C A7  T.C^.... .}.d..\.
0000 0040: 44 7F 14 3B 89 36 06 84  D3 53 EB AA 39 19 E9 7F  D..;.6.. .S..9...
0000 0050: A3 93 24 27 50 60 23 29  AB C3 20 E7 A6 5F A8 B6  ..$'P`#) .. .._..
0000 0060: D7 3B 3A 34 AF 08 90 FC  35 FF 01 74 C9 1F 1A 04  .;:4.... 5..t....
0000 0070: 6D 17 08 B9 F0 B7 65 40  DC 65 09 D1 67 A2 0E 90  m.....e@ .e..g...
0000 0080:
0000 0090:
0000 00A0:
0000 00B0:
0000 00C0:
0000 00D0:
0000 00E0:
0000 00F0:

2.bin
0000 0000: 17 47 6A 0B 57 6B 96 B5  F9 EA 86 A9 A1 AF 5D EF  .Gj.Wk.. ......].
0000 0010: 23 8D 54 05 25 85 8F 78  46 D2 40 2E 88 26 BE AB  #.T.%..x F.@..&..
0000 0020: 6D DB AA EF EE 69 0A 3B  6B E4 6A 1C 96 71 50 5A  m....i.; k.j..qPZ
0000 0030: 54 DF 43 5E 9B 00 A5 D5  BA 7D ED 64 AF 1B 5C A7  T.C^.... .}.d..\.
0000 0040: 44 7F 14 3B 89 36 06 84  D3 53 EB AA 39 19 E9 7F  D..;.6.. .S..9...
0000 0050: A3 93 24 27 50 60 23 29  AB C3 20 E7 A6 5F A8 B6  ..$'P`#) .. .._..
0000 0060: D7 3B 3A 34 AF 08 90 FC  35 FF 01 74 C9 1F 1A 04  .;:4.... 5..t....
0000 0070: 6D 17 08 B9 F0 B7 65 40  DC 65 09 D1 67 A2 0E 90  m.....e@ .e..g...
0000 0080:
0000 0090:
0000 00A0:
0000 00B0:
0000 00C0:
0000 00D0:
0000 00E0:
0000 00F0:

Arrow keys move  F find      RET next difference  ESC quit  T move top
C ASCII/EBCDIC   E edit file   G goto position      Q quit  B move bottom
```

- *1.bin*, *2.bin*의 hash를 비교(md5sum 명령어를 이용하여 MD5 hash 생성)

```
[05/29/19]seed@VM:~/.../T3$ md5sum 1.bin
d05f008f82a27d23fa58451cb1fd087b  1.bin
[05/29/19]seed@VM:~/.../T3$ md5sum 2.bin
d05f008f82a27d23fa58451cb1fd087b  2.bin
[05/29/19]seed@VM:~/.../T3$
```

② 1bit가 차이나는 두 파일의 비교(T3 폴더 내 *1.bin*, *3.bin*에 대해여 ①을 반복)

```
[05/29/19]seed@VM:~/.../T3$ vbindiff 1.bin 3.bin
VBinDiff 3.0_beta4, Copyright 1995-2008 Christopher J. Madsen
VBinDiff comes with ABSOLUTELY NO WARRANTY; for details type `vbindiff -L'.
```

```
1.bin
0000 0000: 17 47 6A 0B 57 6B 96 B5  F9 EA 86 A9 A1 AF 5D EF  .Gj.Wk.. ......].
0000 0010: 23 8D 54 05 25 85 8F 78  46 D2 40 2E 88 26 BE AB  #.T.%..x F.@..&..
0000 0020: 6D DB AA EF EE 69 0A 3B  6B E4 6A 1C 96 71 50 5A  m....i.; k.j..qPZ
0000 0030: 54 DF 43 5E 9B 00 A5 D5  BA 7D ED 64 AF 1B 5C A7  T.C^.... .}.d..\.
0000 0040: 44 7F 14 3B 89 36 06 84  D3 53 EB AA 39 19 E9 7F  D..;.6.. .S..9...
0000 0050: A3 93 24 27 50 60 23 29  AB C3 20 E7 A6 5F A8 B6  ..$'P`#) .. .._..
0000 0060: D7 3B 3A 34 AF 08 90 FC  35 FF 01 74 C9 1F 1A 04  .;:4.... 5..t....
0000 0070: 6D 17 08 B9 F0 B7 65 40  DC 65 09 D1 67 A2 0E 90  m.....e@ .e..g...
0000 0080:
0000 0090:
0000 00A0:
0000 00B0:
0000 00C0:
0000 00D0:
0000 00E0:
0000 00F0:

3.bin
0000 0000: 17 47 6A 0B 57 6B 96 B5  F9 EA 86 A9 A1 AF 5D EF  .Gj.Wk.. ......].
0000 0010: 23 8D 54 05 25 85 8F 78  46 D2 40 2E 88 26 BE AB  #.T.%..x F.@..&..
0000 0020: 6D DB AA EF EE 69 0A 3B  6B E4 6A 1C 96 71 50 5B  m....i.; k.j..qP[
0000 0030: 54 DF 43 5E 9B 00 A5 D5  BA 7D ED 64 AF 1B 5C A7  T.C^.... .}.d..\.
0000 0040: 44 7F 14 3B 89 36 06 84  D3 53 EB AA 39 19 E9 7F  D..;.6.. .S..9...
0000 0050: A3 93 24 27 50 60 23 29  AB C3 20 E7 A6 5F A8 B6  ..$'P`#) .. .._..
0000 0060: D7 3B 3A 34 AF 08 90 FC  35 FF 01 74 C9 1F 1A 04  .;:4.... 5..t....
0000 0070: 6D 17 08 B9 F0 B7 65 40  DC 65 09 D1 67 A2 0E 90  m.....e@ .e..g...
0000 0080:
0000 0090:
0000 00A0:
0000 00B0:
0000 00C0:
0000 00D0:
0000 00E0:
0000 00F0:

Arrow keys move  F find      RET next difference  ESC quit  T move top
C ASCII/EBCDIC   E edit file   G goto position      Q quit  B move bottom
```

```
[05/29/19]seed@VM:~/.../T3$ md5sum 1.bin
d05f008f82a27d23fa58451cb1fd087b  1.bin
[05/29/19]seed@VM:~/.../T3$ md5sum 3.bin
ab193a79a6c506e7d1cb5ca5aeb932b0  3.bin
[05/29/19]seed@VM:~/.../T3$
```

③ MD5 충돌이 일어나는 서로 다른 binary의 생성

- md5collgen 명령어를 사용하여 고의로 MD5 충돌이 발생하는 두 바이너리를 생성

```
[05/29/19]seed@VM:~/.../T3$ 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: ^[[3~.....
Generating second block: S01...................
Running time: 12.6876 s
[05/29/19]seed@VM:~/.../T3$
```

- 생성된 두 파일 *o1.bin*, *o2.bin*에 대하여 ①을 반복

```
[05/29/19]seed@VM:~/.../T3$ vbindiff o1.bin o2.bin
VBinDiff 3.0_beta4, Copyright 1995-2008 Christopher J. Madsen
VBinDiff comes with ABSOLUTELY NO WARRANTY; for details type `vbindiff -L'.
[05/29/19]seed@VM:~/.../T3$
```

```
o1.bin
0000 0000: 05 CC 1E 11 41 45 3E D4  CE 5B C4 3E 67 4E 0A B8  ....AE>. .[.>gN..
0000 0010: 37 90 9D 87 FB C5 3F 54  2D 72 84 7D 66 90 C5 FC  7.....?T -r.}f...
0000 0020: 53 9B F6 F6 40 0A E3 6A  EB 01 EC 5C 8B A7 20 5E  S...@..j ...\.. ^
0000 0030: 7B 49 4D C4 28 3D 55 EC  F5 25 48 7A 0D A6 47 17  {IM.(=U. .%Hz..G.
0000 0040: 52 53 B2 0F DF 1D 18 27  A7 3F 5F 0D F5 33 18 30  RS.....' .?_..3.0
0000 0050: 22 FF BF 22 1D 66 46 A6  C9 1A F6 CB EC 47 DE EF  "..".fF. .....G..
0000 0060: 9E 6D C6 98 F6 50 E0 8D  B8 4E 69 4F B8 84 92 EE  .m...P.. .NiO....
0000 0070: 53 2D 34 64 C4 28 10 18  91 24 5A 3E 33 F4 F8 51  S-4d.(.. .$Z>3..Q
0000 0080:
0000 0090:
0000 00A0:
0000 00B0:
0000 00C0:
0000 00D0:
0000 00E0:
0000 00F0:

o2.bin
0000 0000: 05 CC 1E 11 41 45 3E D4  CE 5B C4 3E 67 4E 0A B8  ....AE>. .[.>gN..
0000 0010: 37 90 9D 87 FB C5 3F 54  2D 72 84 7D 66 90 C5 FC  7.....?T -r.}f...
0000 0020: 53 9B F6 F6 40 0A E3 6A  EB 01 EC 5C 8B 27 21 5E  S...@..j ...\.'!^
0000 0030: 7B 49 4D C4 28 3D 55 EC  F5 25 48 FA 0D A6 47 17  {IM.(=U. .%H...G.
0000 0040: 52 53 B2 0F DF 1D 18 27  A7 3F 5F 0D F5 33 18 30  RS.....' .?_..3.0
0000 0050: 22 FF BF A2 1D 66 46 A6  C9 1A F6 CB EC 47 DE EF  "....fF. .....G..
0000 0060: 9E 6D C6 98 F6 50 E0 8D  B8 4E 69 4F B8 04 92 EE  .m...P.. .NiO....
0000 0070: 53 2D 34 64 C4 28 10 18  91 24 5A BE 33 F4 F8 51  S-4d.(.. .$Z.3..Q
0000 0080:
0000 0090:
0000 00A0:
0000 00B0:
0000 00C0:
0000 00D0:
0000 00E0:
0000 00F0:

Arrow keys move  F find      RET next difference  ESC quit  T move top
C ASCII/EBCDIC   E edit file   G goto position      Q quit    B move bottom
```

```
[05/29/19]seed@VM:~/.../T3$ md5sum o1.bin
417d7785bb1552b773ff5661898b1e91  o1.bin
[05/29/19]seed@VM:~/.../T3$ md5sum o2.bin
417d7785bb1552b773ff5661898b1e91  o2.bin
[05/29/19]seed@VM:~/.../T3$
```