CNU 충남대학교 CHUNGNAM NATIONAL UNIVERSITY

REPORT

정보보호 00 반

고전암호

이름	정진욱
학과	컴퓨터공학과
학번	201602071
과목	정보보호
교수님	류재철 교수님

1. 과제 이해

이번 과제의 구성은 실습 문제로 받은 카이사르 암호의 틀을 가지고 만들면 그대로 사용할 수 있을 것이라고 생각했습니다.

카이사르 암호는 1~26 번 문자를 옮겨 만드는 암호입니다. 따라서 쉽게 암호화/복호화 가능하지만, 쉽게 분석될 수 있다는 단점이 있습니다.

비제네르 암호는 난수표를 이용하는 암호로, 키 값을 이용하여 각 문자를 0~26 의 숫자로 변환한 후 목적 문자열에 각 숫자를 순회하며 카이사르 암호에서 사용한 방식으로 문자를 이동시킵니다.

이 방법은 굉장히 강력한 암호로 사용되었지만, 현재는 빈도분석법으로 비교적 쉽게 해독할 수 있다고 합니다.

2. 과제 구현

a. shift()

```
27 def shift(symbol, key):
28  shifted = 0
29  if ord(symbol)>=ord('a') and ord(symbol)<=ord('z'):
30   shifted = ord(symbol)+key
31   if shifted > ord('z'):
32    shifted = shifted-(ord('z')-ord('a')+1)
33   elif shifted < ord('a'):
34    shifted = shifted+(ord('z')-ord('a')+1)
35  elif ord(symbol)>=ord('A') and ord(symbol)<=ord('Z'):
36   shifted = ord(symbol)+key
37   if shifted > ord('Z'):
38    shifted = shifted-(ord('z')-ord('a')+1)
39   elif shifted < ord('A'):
40    shifted = shifted+(ord('z')-ord('a')+1)
41  return chr(shifted)
```

Shift 함수는 위와 같이 만들었습니다.

받은 원본 문자의 아스키 코드 영역(소문자 혹은 대문자)에 따라서 키 값을 더했을 시 문자 코드 영역을 넘어가는 경우에 대하여 처리해 두었습니다.

b. encrypt()

encrypt 의 경우 비제네르 암호만 자료와 다르게 구현하였으므로 이 부분만 설명하겠습니다.

```
43 def encrypt(mode, fileName, key):
44  key_int = []
45  for idx, keysymbol in enumerate(key):
46   tmp = ord(keysymbol)-ord('a')
47   if mode[0] is 'd':
48    tmp = -tmp
49   key_int.append(tmp)
50  outputFileName = 'encrypt.txt'
51  if mode[0] is 'd':
52   outputFileName = 'decrypt.txt'
53  translated = ''
54  outputFile = open(outputFileName, 'w')
55  inputFile = open(fileName, 'r')
56  message = inputFile.read()
57 
58  for idx, symbol in enumerate(message):
59   translated += shift(symbol, key_int[idx%len(key_int)])
60 
61  outputFile.write(translated)
62  outputFile.close()
63  inputFile.close()
64  print('En(De)cryption complete')
```

비제네르 암호의 경우 문자를 숫자로 바꿔서 사용해야 하기 때문에 숫자 배열을 만든 후 각 키 문자마다 ord()를 사용하여 숫자 형식으로 변환하였습니다.