CNU 충남대학교 CHUNGNAM NATIONAL UNIVERSITY

REPORT

정보보호 00 반

대칭키 암호

이름	정진욱
학과	컴퓨터공학과
학번	201602071
과목	정보보호
교수님	류재철 교수님

1. 과제 이해

이번 과제는 스트림 암호로서 사용될 수 있는 xor 암호화/복호화 및 xor 암호에 대한 브루트포스 공격을 수행하였습니다.

Xor 암/복호화는 이전에 사용하였던 고전 암호에 비해 키 한 글자마다 2^8에 달하는 복잡도를 가질 수 있으므로 더 강력한 보안을 가진다는 장점이 있고, xor 연산을 통해 구현되었으므로 이진 컴퓨터로 구현하기에 알맞은 암호라는 점에서 장점을 가집니다.

이 과제를 구현하기 위해 python3 을 사용하였습니다.

2. 과제 구현

a. str_xor()

```
def str_xor(keyValue, message):
 translated = b''
 for idx, var in enumerate(keyValue):
  #print(ord(var), '^', message[idx], '=', ord(var)^message[idx])
  translated+=bytes([ord(var)^message[idx]])
 return translated
```

str_xor()함수는 위와 같이 만들었습니다.

b. encrypt()

```
def encrypt(mode, fileName, key):
 keyValue = ''
 outputFileName = 'encrypt.txt'
 if mode[0] is 'd':
  outputFileName = 'decrypt.txt'
 outputFile = open(outputFileName, 'wb')
 inputFile = open(fileName, 'rb')
 message = inputFile.read()
 for i in range(len(message)//3):# 3: 키 길이
  keyValue += key
 translated = str_xor(keyValue, message)
 outputFile.write(translated)
 outputFile.close()
 inputFile.close()
 print('En(De)cryption complete')
```

Encrypt 함수를 구현 설명에 추가한 이유는 테스트 중 오류가 발견되었기 때문입니다.

Ubuntu server 18.04 기준으로 'w'를 이용한 읽기/쓰기 시 \r 문자가 \n 으로 강제 변경되는 현상을 발견했습니다.(ASCII code 13→10) 그래서 hello 를 aaa 로 암호화/복호화하면 중간에 l 두개가 13 으로 변형되어 저장되어야 하지만 10 으로 저장되기 때문에 hekko 로 복호화됩니다.

따라서 'wb', 'rb'로 변경하여 구현하였습니다.

c. bruteforce()

```
def bruteforce():
 mode = getMode()
 #key = getKey()
 key = [ord('a'),ord('a'),ord('a')]
 fileName = getFileName()
 outputFileName = 'encrypt.txt'
 if mode[0] is 'd':
  outputFileName = 'decrypt.txt'
 bruteForceFile = open(outputFileName+'.bruteforce', 'a')
 while key[0]<=ord('z'):
  while key[1] <= ord('z'):
   while key[2] <= ord('z'):
    encrypt(mode, fileName, bytes(key).decode())
    outputFile = open(outputFileName, 'rb')
    result = outputFile.read()
    outputFile.close()
    bruteForceFile.write(bytes(key).decode()+'\t'+result.decode()+'\n')
    key[2] += 1
   key[2] = ord('a')
   key[1] += 1
  key[1] = ord('a')
  key[0] += 1
 bruteForceFile.close()
bruteforce()
```

bruteforce()함수는 기존 프로그램을 수정하지 않고 덧붙이는 형태로 만들어졌습니다.

과제 pdf 의 요구사항 대로 aaa 부터 zzz 까지 모든 키 값에 대하여 확인하였고, 출력 파일은 확인이 쉽도록 (키 값)(TAB)(복호화값)(개행)형태로 만들었습니다.

Decrypt 모드로 브루트포스한 결과 파일 이름은 decrypt.txt.bruteforce 이며, 내용은 다음과 같습니다.