

# 소프트웨어프로젝트 3주차 주간보고서

컴퓨터SW 18017103 황제현

# 이번주차 진행내용

- 1. 프로그램 변경사항
- 2. 암호화 프로그램 완성
- 3. 복호화 프로그램의 초기버전
- 4. 정리

# 1. 프로그램 변경사항

- 연산과정에서 숫자가 너무 커져서 인코딩이 되지 않는 문제가 발생하였다.
- 키 데이터를 알파벳 소문자의 나열로 수정하였다.
- 평문과 키 데이터를 먼저 XOR연산한 뒤 특정 진법으로 변환하는 방식으로 암호화 방식을 소폭 수정하였다.
- 이에 따라 사용할 변수가 수정되었다.

```
plainText = "" # 암호화할 데이터
keyString = "" # 암호화에 사용할 키
keyList = [] # 연산을 위해 리스트화시킨 키
conversionNum = 0 # 변환할 진법
XorList = []
ConvertedXorList = []
InputEncodeType = sys.stdin.encoding
OutputEncodeType = sys.stdout.encoding
UniConvertedData = [] # 유니코드로 변환된 데이터
cipherText = "" # 암호화된 데이터
```

그림 1) 변수 목록(암호화 프로그램)

```
print("키를 생성하는중....")
for i in range(0, dataLength) :
    keyList.append(random.randrange(97,123))
    keyString += chr(keyList[i])
```

그림 2) 키 생성 코드

## 2. 암호화 프로그램 완성

- 암호화 프로그램의 완성 단계
- 출력 내용을 간결하게 수정하였다.
- 진행상황을 한눈에 파악하고, 문제가 생긴 부분을 빠르게 찾을 수 있도록 진행과정이 단계별로 출력된다.
- 일부 특수문자가 제대로 출력되지 않는 현상이 있어 해결책을 찾는 중이다.

변환할 데이터를 입력하세요: 0528 whitehouse

입력한 데이터 : 0528 whitehouse  
데이터를 유니코드로 변환하는중...  
변환 완료.

데이터 암호화 중...  
선택된 진법: 4  
키를 생성하는중....  
생성 완료.

암호문 생성중...  
암호화 완료.

암호문  
ЁiьрЉгfyтdpy?

키 데이터  
nabpovzwmoxyrjc

주의) 키 데이터와 사용된 진법은 안전하게 보관하세요!  
>>>

그림 3) 암호화 프로그램 실행화면

### 3. 복호화 프로그램의 초기버전

- 복호화 프로그램의 초안
- 암호화 과정의 작업을 반대로 수행한다.
- 필요한 변수를 정의하고, 프로그램 전반에 테스트 코드를 넣어 동작과정을 모니터링하였다.

```
cipherText = "" # 암호문  
cipherList = [] # 유니코드로 변환시킨 암호문  
reXorList = []  
plainText = ""  
conversionNum = 0  
keyString = ""  
keyList = []
```

그림 4) 변수 목록(복호화 프로그램)

### 3. 복호화 프로그램의 초기버전

```
cipherText = input("암호문을 입력하세요 >> ")
conversionNum = int(input("변환에 사용된 진법을 입력하세요 >>"))
keyString = input("키 데이터를 입력하세요 >>")

dataLength = len(cipherText)
print("암호문을 변환하는중....")
# 암호문 -> 유니코드(진법변환됨)
for i in range(0, dataLength) :
    cipherList.append(ord(cipherText[i]))

print("변환 완료.")
print("유니코드로 변환된 암호문: ", cipherList)

for i in range(0, dataLength) :
    tmpNum = cipherList[i]
    cipherList[i] = int(str(tmpNum), conversionNum)

print("키 데이터를 변환하는중...")
for i in range(0, dataLength) :
    keyList.append(ord(keyString[i]))

print("변환 완료.")
print("변환된 키 데이터: ", keyList)

print("데이터를 복호화 하는중...")
for i in range(0, dataLength) :
    reXorList.append(cipherList[i] ^ keyList[i])

print("다시 XOR연산된 리스트: ", reXorList)

for i in range(0, dataLength) :
    plainText += chr(reXorList[i])

print("복호화된 평문: ", plainText)
```

```
암호문을 입력하세요 >> l8iьp7b rfyтdpyɀ
변환에 사용된 진법을 입력하세요 >>4
키 데이터를 입력하세요 >>nabpovzwmoxyrjc
암호문을 변환하는중....
변환 완료.
유니코드로 변환된 암호문: [1132, 1110, 1100, 1020, 1033, 1, 102, 132, 121, 22, 100, 112, 13, 12, 1, 12]
키 데이터를 변환하는중...
변환 완료.
변환된 키 데이터: [110, 97, 98, 112, 111, 118, 122, 119, 109, 111, 120, 121, 114, 106, 99]
데이터를 복호화 하는중...
다시 XOR연산된 리스트: [48, 53, 50, 56, 32, 119, 104, 105, 116, 101, 104, 111, 117, 115, 101]
복호화된 평문: 0528 whitehouse
```

그림 6) 복호화 프로그램 실행화면

그림 5) 복호화 프로그램 초안

## 4. 정리

- 암호화 프로그램의 작동방식을 일부 수정하고, 인터페이스를 간결하게 개선하였다.
- 암호화 프로그램이 완성 단계에 돌입했으나, 출력 과정에서 일부 문제가 발생하여 해결할 예정이고, 프로그램 구조도 점차 개선해 나갈 예정이다.
- 복호화 프로그램의 초안을 작성하여 테스트하였다.
- 이번 주차까지 진행된 파이썬 코드를 첨부하였다.