

Университет ИТМО
Факультет ФПИ и КТ

Отчёт

по лабораторной работе 1.1

«Информационная безопасность»

Вариант 7

Студент:

Ляо Ихун

Гр.Р34131

Преподаватель:

Маркина Татьяна Анатольевна

Цель работы:

изучение основных принципов шифрования информации,
знакомство с широко известными алгоритмами шифрования,
приобретение навыков их программной реализации.

Задача:

Реализовать в программе шифрование и дешифрацию файла
использованием перестановочного шифра с ключевым словом.
Ключевое слово вводится.

Выполнение:

```
from collections import OrderedDict
```

```
def generate_key(input_str):
```

```
    unique_chars = ''.join(OrderedDict.fromkeys(input_str))
```

```
    return unique_chars
```

```
def reverse_dict(original_dict):
```

```
    reversed_dict = {value: key for key, value in original_dict.items()}
```

```
    return reversed_dict
```

```
def encrypt(input_file, output_file, encrypted_map):
```

```
    plaintext = "
```

```
    with open(input_file, 'r', encoding='utf-8') as file:
```

```

        plaintext = file.read()

# Создаем перестановку символов
encrypted_text = ""
for i in plaintext:
    if i in encrypted_map.keys():
        encrypted_text += encrypted_map[i]
    else:
        encrypted_text += i
with open(output_file, 'w', encoding='utf-8') as file:
    file.write(encrypted_text)

def decrypt(input_file, output_file, decrypted_map):
    plaintext = ""
    with open(input_file, 'r', encoding='utf-8') as file:
        plaintext = file.read()

# Создаем перестановку символов
decrypted_text = ""
for i in plaintext:
    if i in decrypted_map.keys():
        decrypted_text += decrypted_map[i]
    else:
        decrypted_text += i
    with open(output_file, 'w', encoding='utf-8') as file:
        file.write(decrypted_text)

if __name__ == '__main__':

```

```

encrypted_map = {chr(i): i for i in range(1040, 1104)}
decrypted_map = dict()
keyword = input("Вводите ключевое слово:")
key = generate_key(keyword)
cha = 'A'
alphabet_set = {chr(i) for i in range(1040, 1104)}
for k in key:
    encrypted_map[cha] = k
    cha = chr(ord(cha) + 1)
    alphabet_set.remove(k)
alphabets = sorted(alphabet_set)
for a in alphabets:
    encrypted_map[cha] = a
    cha = chr(ord(cha) + 1)
decrypted_map = reverse_dict(encrypted_map)
print(encrypted_map)
print(decrypted_map)
func = input("Выбор
фкункции:\n1)шифрование\n2)дешифрация\n")
if func == "1":
    source_name = input("Файл исходный:")
    result_name = input("Целевой файл:")
    encrypt(input_file=source_name, output_file= result_name,
encrypted_map=encrypted_map)
elif func == "2":
    source_name = input("Файл исходный:")
    result_name = input("Целевой файл:")

```

```
decrypt(input_file=source_name, output_file=result_name,  
decrypted_map=decrypted_map)
```

```
else:
```

```
print("Вводите 1 или 2 чтобы выбрать что делать")
```

Пример:

Исходный:

На первый взгляд здесь не представлено соответствий Пуффендую; Барсука на небе нет. Однако созвездие Чаши всё-таки подходит под классификацию. Достаточно вспомнить Чашу Пуффендуй — одну из четырёх реликвий основателей Хогвартса и крестраж Волан-де-Морта.

Роулинг не раз обращалась к теме звёзд и созвездий в Поттериане. Яркий пример — имена семейства Блэков. Сириус — это так называемая Пёсья Звезда. Беллатрикс переводится как «Женщина-Воительница», это «Звезда Амазонок». Регул или Регулус — ярчайшая звезда в созвездии Льва. Кстати, Драко, как сын урождённой Нарциссы Блэк, тоже продолжает эту традицию: он назван в честь созвездия Дракона.

Змееборческий мотив и шрам-молния

Упомянутая выше Лернейская Гидра — это многоголовое, змеевидное чудовище из древнегреческой мифологии, которое лишь с огромным трудом смог одолеть Геракл. Характерная его особенность заключалась в том, что на месте отрубленной головы тут же вырастала новая либо даже несколько новых голов, из-за чего каждый обрубок обязательно нужно было прижечь. Благодаря этому, Гидра долго сохраняла бессмертие и непобедимость.

Это описание, конечно, очень напоминает Волан-де-Морта и его крестражи. Символизм Гидры, связанный с труднопобедимым злом,

войнами и раздорами, хорошо согласуется и с образом Тёмного Лорда, и с репутацией факультета Слизерин.

Ключевое слово:

ГарриПоттер

Текст после шифрования:

Жъ мянбыд ввЭзяЮ вЮЯпъ кЯ мнЯЮпсЪЪзЯкл пллсЪЯспсЪгд
ИуффЯкЮую; аънпужъ къ кЯЫЯ кЯс. ЗЮкЪжл плвЪЯвЮгЯ СЪшг
Ыпё-сЪжг млЮхлЮгс млЮ жзЪппгфгжЪцгю. ПлпсЪслчкл Ъпмлйкгсь
Съшу ИуффЯкЮуд — лЮку гв чЯсынёх нЯзгжЪгд лпклЪсЯЗЯд
ОлЭЪънспЪ г жнЯпснЪб рлзЪк-ЮЯ-ЕлнсЪ.

ЙлузгкЭ кЯ нЪв лынЪщЪзЪпъ ж сЯйЯ ввёвЮ г плвЪЯвЮгд Ъ
ИлссянгЪкЯ. Щнжгд мнгйЯн — гйЯкъ пЯйЯдпсЪЪ азэжлъ. Кгнгуп —
эсл сЪж кЪвыбЪЯйЪя Иёпья еЪЯвЮЪ. аЯззЪснгжп мянЯьлЮгспя жЪж
«тякщгкъ-рлгсЯзыкцЪ», эсл «еЪЯвЮЪ ГйЪвлклж». ЙЯЭуз гзг ЙЯЭузуп
— янчЪдшЪя вЪЯвЮЪ Ъ плвЪЯвЮгг ДьбЪ. ВпсЪсг, ПнЪжл, жЪж пык
унлбЮёкклд Жънцгппы азэж, слбЯ мнлЮлзбЪЯс эсу снЪЮгцгю: лк
кЪввЪк Ъ чЯпсь плвЪЯвЮгя ПнЪжлкъ.

ейЯЯЫлнчЯпжгд йлсгЪ г шнЪй-йлзкя

МмлйякусЪя ЪышЯ ДянкЯдпжЪя игЮнЪ — эсл йклЭлЭлзльбЯ,
вйЯЯьгЮкля чүЮльгщЯ гв ЮнЯькЯЭнЯчЯпжлд йгфлзлЭгг, жлслнлЯ
згшъ п лЭнлйкый снүЮлй пйлЭ лЮлзЯсь иянЪжз. ОънЪжсянкЪя ЯЭл
лплЫЯкклпсь вЪжзючЪзЪпъ Ъ слй, чсл къ йЯпсЯ лснүЫзЯкклд
Элзльы сус бЯ ЪынЪпсЪзЪ клЪЪя згыл ЮЪбЯ кЯпжлзьжл клЪых
Элзль, гв-вЪ чЯЭл жЪбЮыд лынүЫлж лыявЪсЯзыкл кубкл Ыызл
мнгбЯчь. азЪЭлЮЪня эслиу, игЮнЪ ЮлзЭл плхнЪкязЪ ЫЯппйЯнсгЯ г
кЯмлыЯЮгйлпсь.

Чсл лмгпЪкгЯ, жлкЯчкл, лчЯкъ кЪмлйгкЪЯс рлзЪк-ЮЯ-ЕлнсЪ г ЯЭл
жнЯпснЪбг. КгйЪлзгвй игЮны, пъявЪккыд п снүЮклмлыЯЮгый
взлй, ЪлджЪйг г нЪвЮлнЪйг, хлнлшл плЭзЪпуЯспя г п лынЪвлй
ЛёйклЭл ДлнЮЪ, г п нЯмусЪцгЯд фЪжюзьсЯсЪ Кзгвянгк.

Вывод:

В ходе выполнения работы реализовали шифрование и дешифрование с использованием перестановочного шифра с ключевым словом на языке python.