

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО
ФАКУЛЬТЕТ ПРОГРАММНОЙ ИНЖЕНЕРИИ И КОМПЬЮТЕРНОЙ ТЕХНИКИ
НАПРАВЛЕНИЕ ПРОГРАММНАЯ ИНЖЕНЕРИЯ
ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА СИСТЕМНОЕ И ПРИКЛАДНОЕ
ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ
СПЕЦИАЛИЗАЦИЯ СИСТЕМНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ № 1.1
курса «Информационная безопасность»
по теме: «Криптографические системы с секретным ключом»
Вариант № 4а

Выполнил студент:
Тюрин Иван Николаевич
группа: Р33102

Преподаватель:
Маркина Т.А.,
Рыбаков С.Д.

Санкт-Петербург, 2024 г.

Содержание

Лабораторная работа № 1.1. Криптографические системы с секретным ключом	2
1. Описание	2
2. Выполнение задания	2
3. Вывод	6

Лабораторная работа № 1.1

Криптографические системы с секретным ключом

1. Описание

Лабораторная работа № 1 «Основы шифрования данных».

Цель работы. Изучение структуры и основных принципов работы современных алгоритмов блочного симметричного шифрования, приобретение навыков программной реализации блочных симметричных шифров.

Задание варианта № 4а: *ГОСТ 28147-89 в режиме ECB.*

2. Выполнение задания

Режим ECB — это «режим электронной кодовой книги» или «режим простой замены».

В соответствии с условием задания разработан скрипт на языке Python выполняющий шифрование текста из файла по методу [ГОСТ 28147-89](#). Исходный код скрипта можно видеть на листинге [1.2](#). Справку по работе с программой можно видеть на листинге [1.1](#).

```
1 usage: main.py [-h] --mode {encrypt,decrypt} --input INPUT --
   output OUTPUT
2
3 ГОСТ 28147-89 в режиме ECB
4
5 options:
6   -h, --help            show this help message and exit
7   --mode {encrypt,decrypt}, -m {encrypt,decrypt}
8                           Режим работы
9   --input INPUT, -i INPUT
```

```

10 Входной файл
11 --output OUTPUT, -o OUTPUT
12 Выходной файл

```

Листинг 1.1: справка по использованию разработанной программы

При шифровании создается случайный ключ и записывается в файл указанный 3 аргументом.

Пример работы утилиты по шифрованию и дешифрованию фрагмента текста из трактата «Lorem ipsum» можно видеть на изображении 1.1.

```

1 D:\Projects\itmo-info-sec\crypto\lab-1_2\python> ls 12/11/2024 12:40:39 AM
2
3 # name type size modified
4
5 0 main.py file 3.3 KiB 18 minutes ago
6 1 original.txt file 452 B an hour ago
7
8 D:\Projects\itmo-info-sec\crypto\lab-1_2\python> cat original.txt 12/11/2024 12:40:43 AM
9 Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor
10 incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis
11 nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.
12 Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu
13 fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in
14 culpa qui officia deserunt mollit anim id est laborum.
15 D:\Projects\itmo-info-sec\crypto\lab-1_2\python>
16 ::: python main.py -m encrypt -i original.txt -o encrypted.txt 12/11/2024 12:40:55 AM
17 D:\Projects\itmo-info-sec\crypto\lab-1_2\python> cat encrypted.txt 12/11/2024 12:40:55 AM
18 йŸi6ZMikёЛАН0,'Ь~'r$<Ycm&3VQS|<m=:IDµz8od$ñ0иЛП±*+Jrл 3•Л*b9жVUX°<R
19 i0 F3KahC9ñЖµ'%b6y-5
20 jV&Yую7...FE•3f,ŸfB|БVриЫJь|в5um"ё -сSжВд2е]DB6гM#@-İY^,УвЕёрлчзХьY0i~JФЁхч еL>@LH}(Г(
21 {S,8n:х~мñz^Нь,µ~г#;Мв%88рAеЁеНрѣеѣ8е8еpeñцеVŸлrAeЁemgW:тrѣе8е8еñе`
22 D:\Projects\itmo-info-sec\crypto\lab-1_2\python>
23 ::: python main.py -m decrypt -i encrypted.txt -o decrypted.txt 12/11/2024 12:41:12 AM
24 D:\Projects\itmo-info-sec\crypto\lab-1_2\python> cat decrypted.txt 12/11/2024 12:41:12 AM
25 Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor
26 incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis
27 nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.
28 Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu
29 fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in
30 culpa qui officia deserunt mollit anim id est laborum.
31 D:\Projects\itmo-info-sec\crypto\lab-1_2\python> 12/11/2024 12:41:17 AM

```

Рис. 1.1: Пример работы утилиты для шифрования фрагмента трактата Lorem ipsum.

```

1 #!/usr/bin/env python
2
3 import argparse
4 from typing import Literal
5
6 type Mode = Literal["encrypt", "decrypt"]
7 type Key = list[int]
8 type Sbox = list[list[int]]
9
10 # ГОСТ 28147-89 S-Box
11 DEFAULT_SBOX: Sbox = [

```

```

12     [4, 10, 9, 2, 13, 8, 0, 14, 6, 11, 1, 12, 7, 15, 5, 3],
13     [14, 11, 4, 12, 6, 13, 15, 10, 2, 3, 8, 1, 0, 7, 5, 9],
14     [5, 8, 1, 3, 10, 7, 4, 12, 9, 14, 0, 6, 11, 2, 13, 15],
15     [7, 13, 10, 1, 0, 8, 9, 15, 14, 4, 6, 12, 11, 2, 5, 3],
16     [6, 12, 7, 1, 5, 15, 13, 8, 4, 10, 9, 14, 0, 3, 11, 2],
17     [4, 11, 10, 0, 7, 2, 1, 13, 3, 6, 8, 5, 9, 12, 15, 14],
18     [13, 11, 4, 1, 3, 15, 5, 9, 0, 10, 14, 7, 6, 8, 2, 12],
19     [1, 15, 13, 0, 5, 7, 10, 4, 9, 2, 3, 14, 6, 11, 8, 12],
20 ]
21
22 KEY: Key = [
23     0x12345678, 0x9ABCDEF0, 0x11223344, 0x55667788,
24     0x99AABBCC, 0xDDEEFF00, 0x13579BDF, 0x2468ACE0,
25 ]
26
27
28 def ECB(a_i: int, x_i: int, sbbox: Sbox) -> int:
29     result = (a_i + x_i) & 0xFFFFFFFF
30
31     substituted = 0
32     for j in range(8):
33         substituted |= sbbox[j][(result >> (4 * j)) & 0xF] << (4
34 * j)
35
36     rotated = ((substituted << 11) | (substituted >> (32 - 11))
37 ) & 0xFFFFFFFF
38     return rotated
39
40 def encrypt_block(block: int, key: Key, sbbox: Sbox) -> int:
41     a_i, b_i = block >> 32, block & 0xFFFFFFFF
42
43     for i in range(32):
44         x_i = key[i % 8 if i < 24 else 7 - (i % 8)]
45         rotated = ECB(a_i, x_i, sbbox)
46         a_i, b_i = b_i ^ rotated, a_i
47
48     return (b_i << 32) | a_i
49
50 def decrypt_block(block: int, key: Key, sbbox: Sbox) -> int:
51     a_i, b_i = block >> 32, block & 0xFFFFFFFF
52
53     for i in range(31, -1, -1):
54         x_i = key[i % 8 if i < 24 else 7 - (i % 8)]
55         rotated = ECB(a_i, x_i, sbbox)
56         a_i, b_i = b_i ^ rotated, a_i
57
58     return (b_i << 32) | a_i
59
60
61 def process_file(

```

```

62     mode: Mode,
63     input_file: str,
64     output_file: str,
65     key: Key,
66     sbbox: Sbox,
67 ):
68     with open(input_file, "rb") as f:
69         data = bytearray(f.read())
70
71     result = bytearray()
72
73     match mode:
74         case "encrypt":
75             data.extend(bytearray(8 - (len(data) % 8))) # add
padding
76             for i in range(0, len(data), 8):
77                 block = int.from_bytes(data[i : i + 8], "little
")
78                 processed_block = encrypt_block(block, key,
sbox)
79                 result.extend(processed_block.to_bytes(8, "
little"))
80         case "decrypt":
81             for i in range(0, len(data), 8):
82                 block = int.from_bytes(data[i : i + 8], "little
")
83                 processed_block = decrypt_block(block, key,
sbox)
84                 result.extend(processed_block.to_bytes(8, "
little"))
85             result.rstrip(b"\x00") # remove padding
86
87     with open(output_file, "wb") as f:
88         f.write(result)
89
90
91 def main():
92     parser = argparse.ArgumentParser(description="ГОСТ 28147-89
в режиме ECB")
93     parser.add_argument("--mode", "-m", choices=["encrypt", "
decrypt"],
94                         required=True, help="Режим работы",)
95     parser.add_argument("--input", "-i", required=True, help="В
ходной файл")
96     parser.add_argument("--output", "-o", required=True, help="
Выходной файл")
97     args = parser.parse_args()
98
99     mode: Mode = args.mode
100     ifile: str = args.input
101     ofile: str = args.output
102     process_file(mode, ifile, ofile, KEY, DEFAULT_SBOX)

```

```
103  
104  
105 if __name__ == "__main__":  
106     main()
```

Листинг 1.2: Код скрипта выполняющего кодирование и декодирование текста методом ГОСТ 28147-89 в режиме ЕСВ

3. Вывод

В результате выполнения работы были изучены структуры и основных принципов работы современных алгоритмов блочного симметричного шифрования, приобретены навыки программной реализации блочных симметричных шифров на языке Python на примере ГОСТ 28147-89 с режимом ЕСВ.