Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики»
Факультет программной инженерии и компьютерных технологий

Отчет по лабораторной работе № 2
“Блочное симметричное шифрование”
по дисциплине Информационная безопасность
Вариант 10

Студент группы № P34151 Шипулин Павел Андреевич

Преподаватель Маркина Татьяна Анатольевна

Санкт-Петербург
2024

Цель работы

Изучить структуры и основные принципов работы современных алгоритмов блочного симметричного шифрования, приобретение навыков программной реализации блочных симметричных шифров.

Вариант задания

Реализовать систему симметричного блочного шифрования, позволяющую шифровать и дешифровать файл на диске с использованием заданного блочного шифра в заданном режиме шифрования. Перечень блочных шифров и режимов шифрования приведен в таблице. Номер шифра и режима для реализации получить у преподавателя.

Алгоритм		Режим шифрования	
Номер	Название	Номер	Название
4	ГОСТ 28147-89	д	OFB

Ход работы

1. Ознакомиться с теоретическими основами шифрования данных.
2. Получить вариант задания у преподавателя.
3. Написать программу согласно варианту задания.
4. Отладить разработанную программу и показать результаты работы программы преподавателю.
5. Составить отчет по лабораторной работе.

Листинг программ

Ссылка на репозиторий:

https://github.com/PashcalE2/IS/tree/main/cryptography/first_part

Файл lab2.py

```
import random


_switch_table = [
    [9, 6, 3, 2, 8, 11, 1, 7, 10, 4, 14, 15, 12, 0, 13, 5],
    [3, 7, 14, 9, 8, 10, 15, 0, 5, 2, 6, 12, 11, 4, 13, 1],
    [14, 4, 6, 2, 11, 3, 13, 8, 12, 15, 5, 10, 0, 7, 1, 9],
    [14, 7, 10, 12, 13, 1, 3, 9, 0, 2, 11, 4, 15, 8, 5, 6],
    [11, 5, 1, 9, 8, 13, 15, 0, 14, 4, 2, 3, 12, 7, 10, 6],
    [3, 10, 13, 12, 1, 2, 0, 11, 7, 5, 9, 4, 8, 15, 14, 6],
    [1, 13, 2, 9, 7, 10, 6, 0, 8, 12, 4, 5, 15, 3, 11, 14],
    [11, 10, 15, 5, 0, 12, 14, 8, 6, 2, 3, 9, 1, 7, 13, 4]
]


def gost_main_block(N: int, K: int) -> int:
    A = N & 0xFFFFFFFF
    B = (N >> 32) & 0xFFFFFFFF

    new_B = A
    new_A = A ^ K

    S = [(new_A >> ((7 - i) * 4)) & 15 for i in range(8)]
    for i in range(8):
        S[i] = _switch_table[i][S[i]]

    new_A = 0
    for i in range(8):
        new_A = new_A | (S[i] << ((7 - i) * 4))

    new_A = ((new_A << 11) & 0xFFFFFFFF) + (new_A >> 21)
    new_A = B ^ new_A

    return (new_B << 32) + new_A


def gost_ofb_encrypt(file_data: bytes, K: list[int], IV: int) -> bytes:
    iters_count = len(file_data) // 8

    T = IV
    result = b''
    for i in range(iters_count):
        T = gost_main_block(T, K[i % len(K)])

        text_block = int.from_bytes(file_data[i * 8:(i + 1) * 8])
        T = T ^ text_block

        result += int.to_bytes(T, 8)

    return result


def gost_ofb_decrypt(file_data: bytes, K: list[int], IV: int) -> bytes:
    iters_count = len(file_data) // 8

    T = IV
    result = b''
    for i in range(iters_count):
        T = gost_main_block(T, K[i % len(K)])
```

```
        text_block = int.from_bytes(file_data[i * 8:(i + 1) * 8])
        result += int.to_bytes(T ^ text_block, 8)

        T = text_block

    return result


def lab4(input_file: str, encrypted_file: str, decrypted_file: str, K: list[int], IV: int):
    with open(input_file, "r", encoding="UTF-8") as file:
        input_data = file.read()

    input_bytes = bytes(input_data, "UTF-8")
    if len(input_bytes) % 8 > 0:
        input_bytes = input_bytes + (b' ' * (8 - (len(input_bytes) % 8)))

    encrypted = gost_ofb_encrypt(input_bytes, K, IV)
    with open(encrypted_file, "wb") as file:
        file.write(encrypted)

    decrypted = gost_ofb_decrypt(encrypted, K, IV)
    with open(decrypted_file, "wb") as file:
        file.write(decrypted)


if __name__ == "__main__":
    """
    Реализовать систему симметричного блочного шифрования,
    позволяющую шифровать и дешифровать файл на диске с использованием
    заданного блочного шифра в заданном режиме шифрования. Перечень
    блочных шифров и режимов шифрования приведен в таблице. Номер
    шифра и режима для реализации получить у преподавателя.

    Вариант 10
    Алгоритм шифрования: ГОСТ 28147-89
    Режим шифрования: OFB
    """

    _K = [random.randint(0, (1 << 32) - 1) for i in range(8)]
    _IV = random.randint(0, (1 << 64) - 1)

    lab4("input.txt", "encrypted.txt", "decrypted.txt", _K, _IV)
```

Выполнение

Результат выполнения программы

Файл input.txt:

Работы в области интеллектуальных информационных систем
нацелены насоздание быстрых алгоритмов поиска в базах знаний,
организацию данных в базах знаний, обеспечивающую быстрый
логический вывод, извлечение знаний из неформализованных источников,
в том числе из социальных сетей. Кроме интеллектуальных
информационных систем в сферу интересов кафедры входят также
интеллектуальные методы управления в технических системах.
Кроме того, на кафедре проводятся научные исследования, связанные с
проблемами проектирования, разработки, сопровождения и
реинжиниринга корпоративных информационных систем, а также с
разработкой преобразователей перемещений на основе рекурсивных
кодовых шкалс улучшенными массогабаритными, технологическими и
надежностными характеристиками.
Сотрудники кафедры участвуют в работе Международных научных
лабораторий:
• «Архитектура и методы проектирования встраиваемых систем и систем
на кристалле».
• «Лаборатория нелинейных и адаптивных систем управления».
• «Многомодальные биометрические и речевые системы».
For more than 30 years, the department has been working in the field of
microprocessor technology and embedded computing systems
related to the development and research of distributed
information and control systems with high reliability,
controller networks of industrial and transport automation,
automation tools for programming and debugging distributed
real-time systems. Within the framework of the scientific direction "Automation
of high-level stages of information management
systems design", the tasks of creating embedded systems,
real-time systems, reconfigurable systems and systems-on-a-chip are solved.
Work is underway to develop a methodology for designing
cyberphysical systems. The direction of work on
the creation of IP cores for systems-on-a-chip is rapidly developing.

Файл encrypted.txt:

□□□□k□□□□<l□□□dr> pt□□Ky"
□z□ □?s □□Ȝ8ő□□G@7-□□g□uT□*=U□p□□ □s□H□□f□._Z□ □□ □□□□□Ru>vj□□□□2xI□□x 5Ę□Hl/□□w□□{SD
[□□5"(M□□□,O□ □□|gb□ □□}□F□a□□B□>□b□□i□= T □□□□+Ɉ□□jX'□m`□□□ 9□e A□a□□□8k o□□□□□95c j□a
□□P□□T□□4□ c□U□yR□ □Nw6W□□□w□ □GA□m□H□□ hyF28□ę□$

$m□.□= □□□□+- □ □,□□ □l□□ □/)□MT□□□□pM/ □l3□□□□□ r U□□□3□e□9'□ □I □W□□□K[o□□I□oV□-
W \□{2□s □□□□Z>□□2=6%□□□□ht9f□'□□ȷj □ □
□□[□8□ □□ □l□'□9□□N□@□□+□Q
A2□□□□□□□e .2□□□□>Qh\□□-□b2□F□,□□BeN□□o6G □□□□o□□ □'□□%)W □□□/r/t□□□□2□□□□k(]□Ci□v□Go□□~□
W%□□□□jP m□`□□ǿBFgX□□Ḥ yP□□" zH~□□qtcg□□>onz□□ ={□□□□K□□]□%6□XE□□a□ □0iWu□I□□i8# □□□□ □
4 ɒW□a'□p□鬓wSZ=WY□9□□0□2□□□ 2v□□=Y?□□□□zY□□□□ BI sSf□□Y□□zKzo□□□□□□)uoO□□!□$F□ □□□qzbVQ
□{□□N□a □aoW□□□S□Rs□Z□ □)□□w□tD { d□□
□ 8□@□□P|
□□□□T□□8□I,;□; □$□ u□□+▨^R □y□□Q□-!□□□□' ~JJ□□□□`□□w□/□r□□0□
^□□□▨□□*□ |□g:□q□□ □□□a□$m□n□□ □3A□2G□ □□m□ >□ d□'□□ !□S□□T□6□□□ tz □ □□ □Z5C□S□□Csb<
m□□□□ □Xۏ?□
□l8□h□ □ H# □□□□ X□<□□R□□□{x □ے۽f□□q□v□□Ţ̣Ve□□ %*ț□
□□Y□6v▨p□□□□r:
J′□□□}7B.□ □□"□2N□X□□b□0 □Y>□%=□g□□□□ □□R□SP□yY□}Lj1ڑ;□
>□n 憑□□C□
H□ □□□□□pq6D□□ɳ□Fhb s□ +S□□□rN□_□□]□□ۦ[□
9+□□□□H d1%□P□}□]□il□▨□ڿ□□□▨ x`ڀ□□bu1)□
7□{□□a@□□ ♀□CmcF□ۣ%[IM□□□j□□"□y □□C
□=□□27~□□□□|□7□y □!□□□□□L□Z □□H □▨□□G□j□□:□ 1`Cù□□g2□□ □ U□□▨.o\□□□□□gK?z□,
·□□ (o $□□□□i □2□□; □□□h3□Y □R□□gN-b,□□□□□□9/d□ □ʏ□0O_ □z6-□□□`□c□/|□T□□Hђ_El□□ □,
□U□□7□ □s□4 □E□□ □ <□□9□= □□□□<J=□□%□9l□-□ O□d□□v
□!□□6 □ڟ□A
t□v□Y□□/□ ~BT□^□□T□▨□□o□x @6 □□Ɏi▨□□□□| □-□M □ˊ□d□□Z□ zm□ □□ $$□L□sU□H□ۣ; #□□-
□□@□E0□}□mL□5□ □Hr□t□□C□□6□CX□□xv□F□□> zƠ□□□□
□□□vﻉ&K9"□□□ □ش□H_MR□□:□'□□[!□T□□a□□□5(□7□1□N □ □□□□□`lw!□□ □B
□{□Ţ□nt▨□, F □□□□□□□□ q!'□ 0jJ□□Ж□ɜF P□X□ □□□E□/□□_ □C
□□□□t□3~□\□□v□z=□v□□□ش̌Bm] bt□□B□i□ □□□□9o □J!□[□□y ▨AT□□□□ □1□□%□G}U□□]□]
□a□□ □v□h□ 2□X□~ ^□□8□8□□□ o1□/4□r□□9□□oy □□□ w;1□□$□#F□□□□#□,Z□N□□<□□ □-
ni□□n ? □"□□□□#vG□@□□ □□] □q□□P[s□l□□{□z
□□$□b□□{ 4c□□□□E▨□Rɨ̣F□□□□ g6□□9□□ټ□
□K□* □ □;□&□□ □□□?□□ □□□mĝ□? 7□K _□
r?>o -
I□y□□□-□□HlF. □r[e□ Q □KA□□9.□+V dŸvt □□□□□□x□4AX□Y#□ K □7(u□h □□ 3□□X□□□+□□□□□□ۣ□ ^□▨6:
□□
□□□`□i□ □ □!□□x□"□ □ □ĸƷ□□□s□▨□ □ ?□□`R□□
□□>{ð- Y□□□6□□□? □□ReЊn□□T □□<;OvQR. 8r□F□^□%□. □□BL□□7□□@□□□□ۦ□ʁ
□x□b□ □□ˆ□ᵻ□□zM□um□)□□□]Ù□□L7□□#Zi□[0□□4_s□□^ □□. g□``
□ □p□□□ □□□ +v□oE O!□X;S□:□
□ˀy□□
□ on□a_Q□□2"□□□_:□□1 □□M P□,}5s□□S□□,I□`:□e +K)□B(□□□h□□□ ص□G□□*ʊ豆u7□□
l□□ □□N□□□:□ɑlH□□"h□□D □Qvt□?!]'Z@:B7
c□ds □B□mv&□-ĸ□□□⼊
□vlyˆ L□□#□T□B□=OH□s"*□ PP□□#)□□VM□%\?□D□ □□□y□□*q□ZG □z[SB5□□%□ □□□w□ʁ□! □ bh□%> □Q[□□□
□È□ :□ ;[□}s□"
□F#□□□□□□□9□
\□kj□ □□kd□b[□:B:□W ~□q □□□□v□V□□□'bƀ@□+□i□[□□ S□□xs□□□ˈ□□□) □Mah□□ک□□□ۦ□J:□□%T2□ □ □t□
r]}□ } □05□SpG□s□□ □□a□□E@□□*.Ym□□1 □□h□□N □□*fW□□ !□□□p□i□z□ □□□

Файл decrypted.txt:

Работы в области интеллектуальных информационных систем
нацелены насоздание быстрых алгоритмов поиска в базах знаний,
организацию данных в базах знаний, обеспечивающую быстрый
логический вывод, извлечение знаний из неформализованных источников,
в том числе из социальных сетей. Кроме интеллектуальных
информационных систем в сферу интересов кафедры входят также
интеллектуальные методы управления в технических системах.
Кроме того, на кафедре проводятся научные исследования, связанные с
проблемами проектирования, разработки, сопровождения и
реинжиниринга корпоративных информационных систем, а также с
разработкой преобразователей перемещений на основе рекурсивных
кодовых шкалс улучшенными массогабаритными, технологическими и
надежностными характеристиками.
Сотрудники кафедры участвуют в работе Международных научных
лабораторий:
• «Архитектура и методы проектирования встраиваемых систем и систем
на кристалле».
• «Лаборатория нелинейных и адаптивных систем управления».
• «Многомодальные биометрические и речевые системы».
For more than 30 years, the department has been working in the field of
microprocessor technology and embedded computing systems
related to the development and research of distributed
information and control systems with high reliability,
controller networks of industrial and transport automation,
automation tools for programming and debugging distributed
real-time systems. Within the framework of the scientific direction "Automation
of high-level stages of information management
systems design", the tasks of creating embedded systems,
real-time systems, reconfigurable systems and systems-on-a-chip are solved.
Work is underway to develop a methodology for designing
cyberphysical systems. The direction of work on
the creation of IP cores for systems-on-a-chip is rapidly developing.

Вывод

Изучил основные принципы современных алгоритмов блочного симметричного шифрования, ознакомился с алгоритмом ГОСТ 28147-89 и сделал его программную реализацию. Этот алгоритм до сих пор является актуальным, но криптостойкость его шифров зависит от таблицы замен, поэтому был специфицирован шифр «Магма» ГОСТ Р 34.12-2015 с тем же алгоритмом в режиме простой замены, но с фиксированной таблицей замен.