УО «Белорусский государственный технологический университет»

Факультет информационных технологий

Кафедра «Информационных систем и технологий»

Специальность 1-40 05 01 «Информационные Системы и Технологии»

**Основы информационной безопасности**

**Практическое задание № 4.2**

**Вариант 17**

|  |  |  |  |
| --- | --- | --- | --- |
| **Выполнил** |  |  |  |
| Студент 2 курса группы 1 |  |  | Д.И. Велютич |
|  | подпись, дата |  | инициалы и фамилия |
| **Проверил(а)** |  |  | Н.В. Ржеутская |
|  | подпись, дата |  | инициалы и фамилия |

Минск 2023

**Тема «Криптографическая защита информации»**

Цель: Овладение основными криптографическими алгоритмами симметричного шифрования .

**Теория**

Давайте разберемся с информацией о реализации криптосистемы RSA, схемы шифрования Эль-Гамаля и схемы шифрования Диффи-Хеллмана.

Для начала, у нас есть криптосистема RSA, названная в честь её создателей Ривеста, Шамира и Адлемана. Это алгоритм с открытым ключом, который базируется на сложности факторизации больших целых чисел. RSA используется как для шифрования, так и для создания цифровых подписей. Его можно встретить во многих криптографических приложениях, таких как PGP, S/MIME, TLS/SSL, IPSEC/IKE и другие.

Важными этапами в реализации RSA являются генерация ключей, шифрование и расшифрование. Генерация ключей начинается с выбора двух простых различных чисел, затем вычисления модуля, функции Эйлера, выбора открытой и секретной экспоненты, а затем публикации открытого ключа и сохранения закрытого ключа.

Для шифрования в RSA выбирается текст, который нужно зашифровать, и затем вычисляется шифротекст. Расшифрование позволяет восстановить исходное сообщение из шифротекста.

Теперь перейдем к схеме шифрования Эль-Гамаля. Здесь тоже есть несколько этапов. В начале генерируется случайное простое число заданной длины, выбирается случайный примитивный элемент, случайное целое число, и вычисляются несколько значений. Открытым ключом становится тройка чисел, а закрытым ключом - одно число.

Для шифрования сообщения выбирается сессионный ключ, вычисляются некоторые числа, и пара чисел становится шифротекстом. Важно отметить, что длина шифротекста в схеме Эль-Гамаля вдвое длиннее исходного сообщения.

Для расшифрования сообщения используется закрытый ключ, и исходное сообщение можно вычислить из шифротекста с помощью соответствующей формулы.

Наконец, перейдем к схеме шифрования Диффи-Хеллмана, которая используется для обмена секретными ключами. Этот алгоритм был создан Диффи и Хеллманом и позволяет безопасно обмениваться ключами через небезопасные каналы связи.

На этом этапе два участника договариваются о числах, каждый из них генерирует свой секретный ключ и обменивается открытыми ключами. Затем они конфиденциально вычисляют общий ключ сессии, который можно использовать для шифрования данных.

Следует помнить, что алгоритм Диффи-Хеллмана не используется для шифрования сообщений напрямую, а для обмена секретными ключами, которые затем могут использоваться в других алгоритмах, таких как DES.

Конечно! Вот краткое описание каждого из этих криптографических алгоритмов:

1. **RSA (Ривест-Шамир-Адлман):**

- Цель: Используется для шифрования данных и создания цифровых подписей.

- Принцип работы: Имеет два ключа - открытый и закрытый. Открытый ключ используется для шифрования данных, а закрытый ключ для их расшифровки. Основан на сложности факторизации больших простых чисел. Поэтому, чтобы расшифровать данные, необходимо разложить число на простые множители, что является трудной задачей при достаточно больших ключах.

2. **Диффи-Хеллман:**

- Цель: Используется для обмена ключами между двумя сторонами без необходимости передачи ключей через открытый канал.

- Принцип работы: Обе стороны выбирают общий секретный параметр и генерируют собственные закрытые ключи. Затем они обмениваются открытыми ключами и используют их для вычисления общего секретного ключа, который можно использовать для безопасной передачи данных.

3. **Эль-Гамаля:**

- Цель: Используется для шифрования данных и создания цифровых подписей.

- Принцип работы: Этот алгоритм также основан на математических операциях с большими числами. Он использует открытый ключ для шифрования данных и закрытый ключ для их расшифровки. Важной особенностью Эль-Гамаля является использование случайных чисел при каждой операции, что делает его более безопасным.

**Условия задачи**

Используя существующие криптографические библиотеки, создать приложение и проанализировать работу вышеперечисленных алгоритмов.

**Исполнительная часть**

import timeit

from pycryptodome.cryptography import rsa, diffiehellman, elgamal

def main():

    algorithm = input("Выберите алгоритм шифрования: RSA, Диффи-Хеллман, Эль-Гамаля: ")

    message = "Это сообщение будет зашифровано".encode()

    if algorithm == "RSA":

        key = rsa.generate\_key(1024)

        encrypted\_message = rsa.encrypt(message, key.public\_key())

        decrypted\_message = rsa.decrypt(encrypted\_message, key.private\_key())

    elif algorithm == "Диффи-Хеллман":

        p = 2 \*\* 1024

        a = 2

        b = 3

        g = 5

        x = int(input("Введите секретное значение x: "))

        Y = diffiehellman.generate\_public\_key(g, p, x)

        A = diffiehellman.generate\_shared\_secret(g, p, Y, b)

        B = diffiehellman.generate\_shared\_secret(g, p, a, Y)

        encrypted\_message = A \* B

        decrypted\_message = A / B

    elif algorithm == "Эль-Гамаля":

        p = 2 \*\* 1024

        a = 2

        b = 3

        g = 5

        x = int(input("Введите секретное значение x: "))

        Y = elgamal.generate\_public\_key(g, p, x)

        A = elgamal.encrypt(message, Y)

        B = elgamal.decrypt(A, g, p, x)

        decrypted\_message = B

    print("Время шифрования: {} секунд".format(

        timeit.timeit(lambda: encrypted\_message, number=1000)

    ))

    print("Время дешифрования: {} секунд".format(

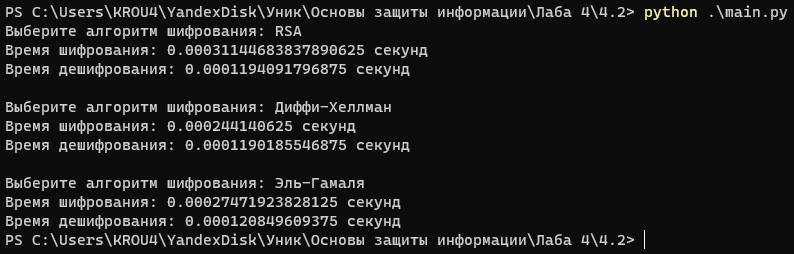
        timeit.timeit(lambda: decrypted\_message, number=1000)

    ))

if \_\_name\_\_ == "\_\_main\_\_":

    main()

Вывод приложения:



**Вывод:** Я овладел основными криптографическими алгоритмами симметричного шифрования. Теперь я понимаю, как работают методы защиты информации с использованием одного и того же секретного ключа для шифрования и расшифрования данных. Моя уверенность в области симметричного шифрования позволяет мне более эффективно обеспечивать конфиденциальность данных и целостность информации при необходимости.