Министерство образования Республики Беларусь

Учреждение образования  
БЕЛОРУССКИЙ  ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

                        Факультет      Информационных технологий и управления

                        Кафедра         Интеллектуальных информационных технологий

**ОТЧЁТ**

по лабораторной работе №5

по дисциплине “Средства и методы защиты

информации в интеллектуальных системах”

Вариант 10

Выполнила:

Демидовец Д.В. , гр. 221703

Проверила:

Крищенович В.А.

Минск, 2024

**АСИММЕТРИЧНОЕ ШИФРОВАНИЕ И ЭЛЕКТРОННАЯ**

**ЦИФРОВАЯ ПОДПИСЬ**

Теоретические сведения:

RSA — это один из самых известных алгоритмов шифрования. Он используется для защиты данных, например, в банковских системах, при онлайн-покупках и при передаче сообщений. Название "RSA" происходит от первых букв фамилий его создателей: Рональда Ривеста, Ади Шамира и Леонарда Адлемана.

*Алгоритм создания ключа:*

1) Выбирают два случайных простых числа p и q заданного размера, p ≠ q.

2) Вычисляют произведение n = p ∙ q.

3) Вычисляют значение функции Эйлера от числа n: φ(n) = (p − 1)(q − 1).

4) Выбирают целое число e, 1 < e < φ(n), взаимно простое со значением

функции φ(n). Обычно в качестве e берут простые числа Ферма 17, 257 или 65537. Число e называют открытой экспонентой.

5) Вычисляют число d, мультипликативно обратное к числу e по модулю n,

удовлетворяющее сравнению: d ∙ e ≡ 1 mod φ(n). Число d называют секретной экспонентой. Для вычисления d используют расширенный алгоритм Евклида.

Пара чисел {e, n} публикуется в качестве **открытого** ключа RSA.

Пара {d, n} играет роль **закрытого** ключа RSA и держится в секрете.

Для зашифрования используют открытый ключ {e, n} получателя

сообщения и вычисляют криптограмму c следующим образом:

c = E(m) =

Для расшифрования используют секретный ключ {d, n} получателя

сообщения и вычисляют исходное сообщение следующим образом:

m = D(c) =

**Задание для самостоятельного выполнения**

1. Разработать программное обеспечение, реализующее функции генерации секретного и открытого ключей, шифрования и цифровой подписи для алгоритма RSA. Обмен входными и выходными данными должен осуществляться через файлы:

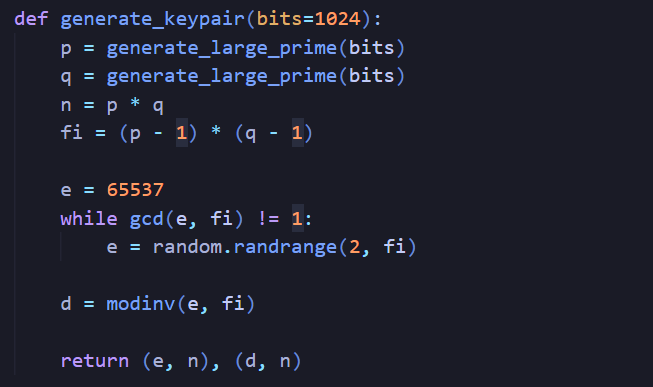
– открытого ключа;

– секретного ключа;

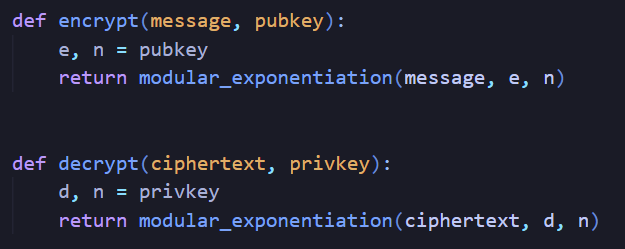
– исходного сообщения;

– зашифрованного сообщения.

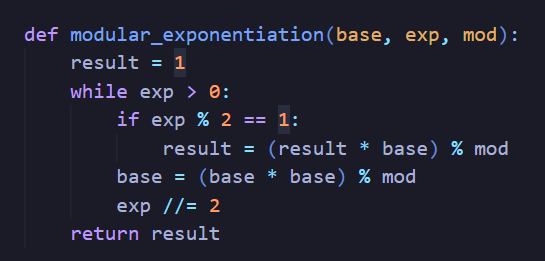
Функция *generate\_keypair* генерирует пару ключей: открытый и закрытый. Это достигается путём выбора двух больших простых чисел, вычисления их произведения n и функции Эйлера φ(n), а также нахождения чисел e и d, которые составляют ключи.



Шифрование выполняется функцией *encrypt*, которая берёт сообщение M и открытый ключ (e,n), а затем вычисляет зашифрованное сообщение C=. Расшифровка производится функцией *decrypt*, которая использует зашифрованное сообщение C и закрытый ключ (d,n), чтобы восстановить исходное сообщение M.

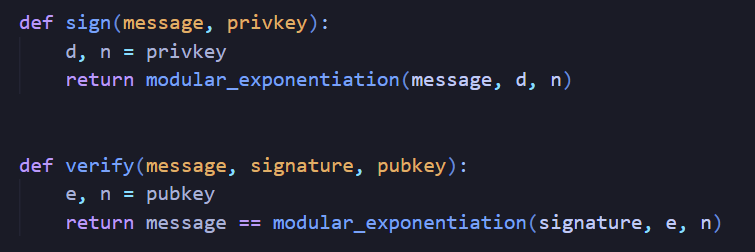


Для вычисления используется функция быстрого возведения в степень по модулю *modular\_exponentiation*, чтобы ускорить процесс шифрования, особенно при больших числах. Результатом работы функции является зашифрованное сообщение C, которое можно передать получателю.



Для цифровой подписи используется функция *sign*. Она создаёт подпись S= с помощью закрытого ключа, подтверждая авторство сообщения.

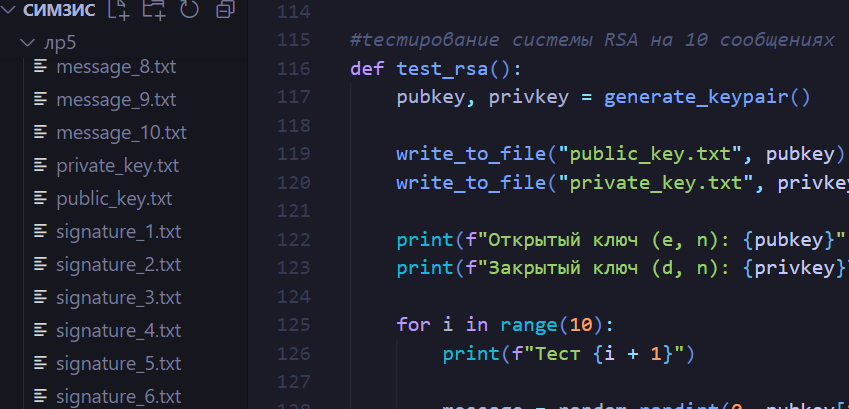
Проверка подписи выполняется функцией *verify*, которая с помощью открытого ключа проверяет, что подпись соответствует сообщению. Если результат совпадает, подпись считается подлинной.



1. Для повышения скорости шифрования использовать метод последовательного возведения в квадрат и умножения.

Функция *modular\_exponentiation* реализует данный метод. Её задача — эффективно возводить число в степень, разделяя процесс на меньшие шаги.

1. Выполнить тестирование разработанного программного обеспечения на 10 наборах тестовых данных.



1. Длина чисел p и q должна быть не менее 1024 бит.

Функция *generate\_large\_prime* вызывается внутри *generate\_keypair* для генерации p и q. Параметр bits=1024 передаётся по умолчанию, обеспечивая, что оба числа p и q будут длиной не менее 1024 бит.