Муниципальное бюджетное общеобразовательное учреждение

Средняя общеобразовательная школа №2

Имени Героя Советского Союза И.А.Передерия

Муниципального образования Каневской район

Исследование асимметричного шифрования RSA на примере программы для шифрования сообщений

Кудреватых Артём,

Ученик 10 «Б»

Попович Анна Давидовна,

Учитель МБОУ СОШ №2

Ст.Каневская,

2021

**ОГЛАВЛЕНИЕ**

Введение.......................................................................................................................

Глава 1...........................................................................................................................

1.1.........................................................................................................................

1.2.........................................................................................................................

Глава 2...........................................................................................................................

2.1.........................................................................................................................

2.2.........................................................................................................................

Заключение...................................................................................................................

Список литературы......................................................................................................

Приложение..................................................................................................................

**Введение**

* **Актуальность темы**:
* С приход интернета в нашу жизнь, мы начинаем сохранять в нём всё больше и больше наших данных, таких как: банковские счета, номера телефонов, фотографии наших паспортов и т.д. Это привлекает злоумышленников, которые хотят использовать эти данные для своего благополучия. Асимметричное шифрование помогает нам сохранять наши данные в не читаемом формате, который не смогут использовать злоумышленники.
* Существует множество алгоритмов шифрования, мы выберем самый популярный и знакомый всем, алгоритм — RSA. При своей простоте, он является одним из самых защищённых и самых распространённых.
* **Цель исследования**:
* Цель нашего исследования — понять, как работает алгоритм RSA и попытаться реализовать его на языке программирования – Python, версии 3.10.2
* **Задачи исследования**:
* Найти и изучить информацию по алгоритму RSA.
* Создать черновик структуры программы для шифрования.
* Написать программу для шифрования.
* Создать оболочку для удобного получения данных программы.
* Исследовать работу алгоритма и сравнить входные и выходные данные.
* **Гипотеза исследования**:
* Если допустить, что ваши данные перехватят, можно быть уверенным, что их не смогут прочитать.
* **Методы исследования**:
* Сравнение.
* Анализ.
* Эксперимент.

**Глава 1**

**Часть 1.1**

**Шифрование**

Шифрование — это обратимое преобразование вводных данных, для их защиты от прочтения не авторизованными лицами. Шифрование состоит из двух частей: Зашифровывание и Расшифровывание. С помощью шифрования обеспечиваются три состояние безопасности данных:

* Конфиденциальность — шифрование используется для сокрытия информации от не авторизованных пользователей при передачи или при хранении.
* Целостность — Шифрование используется для предотвращения изменения данных при передаче или хранении.
* Идентифицируемость - Шифрование используется для аутентификации источника данных и предотвращения отказа отправителя данных от того факта, что данные были отправлены именно им.

Для того, чтобы прочитать зашифрованную информацию, принимающей стороне нужен ключ и дешифратор (устройство, реализующее алгоритм расшифровывания). Идея шифрования стоит на том, что злоумышленник, перехватив данные, не сможет их прочитать без ключа и дешифратора. Однако, с развитием криптоанализа, появились методы, позволяющие дешифровать данные без ключа. Они основаны на математическом анализе переданных данных.

Существует несколько методом шифрования, к ним относятся такие методы, как:

* Симметричное шифрование — использует один и тот же ключ и для шифрования, и для расшифровывания.
* Асимметричное шифрование — использует два разных ключа: один для зашифровывания (называется открытым), другой для расшифровывания (называется закрытым).

**Симметричное шифрование**

В симметричных криптосистемах для шифрования и расшифровывания используется один и тот же ключ. Отсюда название — *симметричные*. Алгоритм и ключ выбирается заранее и известен обеим сторонам. Сохранение ключа в секретности является важной задачей для установления и поддержки защищённого канала связи.

В связи с этим, возникает проблема начальной передачи ключа (синхронизации ключей). Кроме того, существуют методы криптоатак, позволяющие так или иначе дешифровать информацию не имея ключа или же с помощью его перехвата на этапе согласования. В целом эти моменты являются проблемой криптостойкости конкретного алгоритма шифрования и являются аргументом при выборе конкретного алгоритма.



Симметричные, а конкретнее, алфавитные алгоритмы шифрования были одними из первых алгоритмов. Позднее было изобретено асимметричное шифрование, в котором ключи у собеседников разные.

**Схема реализации:**

*Задача.* Есть два собеседника — Алиса и Боб, они хотят обмениваться конфиденциальной информацией.

* Генерация ключа:

Боб (или Алиса) выбирает ключ шифрования **d** и алгоритмы **E**, **D** (функции шифрования и расшифровывания), затем посылает эту информацию Алисе (Бобу).

* Шифрование и передача данных:

Алиса шифрует данные **m** с использованием полученного ключа **d**.

**E(m, d) = c**

И передаёт Бобу шифротекст **c**. То же самое делает Боб, если хочет отправить данные.

* Расшифровывание данных:

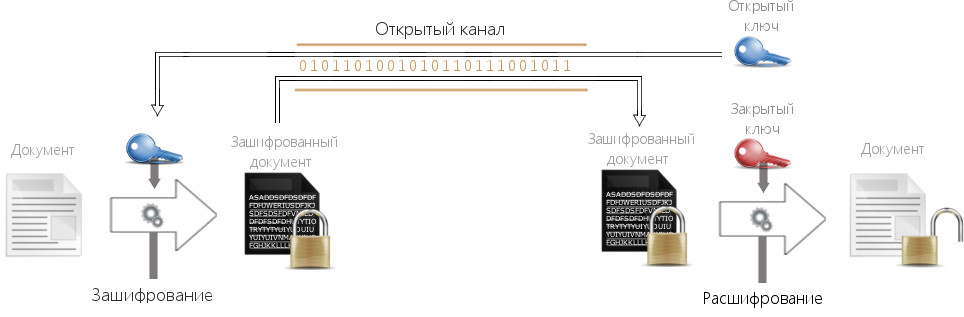
Боб (или Алиса), с помощью того де ключа **d**, расшифровывает шифротекст **c**.

**D(c, d) = m**

Недостатками симметричного шифрования является проблема передачи ключа собеседнику и невозможность установить подлинность или авторство текста. Поэтому, например, в основе технологии цифровое подписи лежат асимметричного схемы.

**Асимметричное шифрование**

В системах с открытым ключом используются два ключа — открытый и закрытый, связанные определённым математическим образом друг с другом. Открытый ключ передаётся по открытому (то есть незащищённому, доступному для наблюдения) каналу и используется для шифрования сообщения и для проверки ЭЦП. Для расшифровки сообщения и для генерации ЭЦП используется секретный ключ.



Данная схема решает проблему симметричных схем, связанную с начальной передачей ключа другой стороне. Если в симметричных схема злоумышленник перехватит ключ, то он сможет как «слушать», так и вносить правки в передаваемую информацию. В асимметричных системах другой стороне передаётся открытый ключ, который позволяет шифровать, но не расшифровывать информацию. Таким образом решается проблема симметричных систем, связанная с синхронизацией ключей.

**Схема реализации:**

*Задача.* Есть два собеседника — Алиса и Боб, Алиса хочет передавать Бобу конфиденциальную информацию.

* Генерация ключевой пары:

Боб выбирает алгоритм **(E, D)** и пару открытый, закрытый ключи **(e, d)** и посылает открытый ключ **e** Алисе по открытому каналу.

* Шифрование и передача данных:

Алиса шифрует информацию с использованием открытого ключа Боба **e**.

**E(m, e) = c**

И передаёт Бобу полученный шифротекст **c**.

* **Расшифровывание сообщения:**

Боб, с помощью закрытого ключа **d**, расшифровывает шифротекст **c**.

**D(c, d) = m**

Если необходимо наладить канал связи в обе стороны, то первые две операции необходимо проделать на обеих сторонах, таким образом, каждый будет знать свои закрытый, открытый ключи и открытый ключ собеседника. Закрытый ключ каждой стороны не передается по незащищенному каналу, тем самым оставаясь в секретности.

**Часть 1.2**

**Асимметричное шифрование RSA**