Муниципальное бюджетное общеобразовательное учреждение

Средняя общеобразовательная школа №1 имени Созонова Юрия Георгиевича

**Индивидуальный проект**

по теме “Криптография и защита информации”

Выполнил:

Ученик 11Г

Четверкин Даниил Дмитриевич

Научный руководитель:

Ханты-Мансийск

2022

**ВВЕДЕНИЕ**

**Актуальность темы исследования**

В век современных технологий и всеобщей цифровизации мира надежная защита персональных данных от злоумышленников является первоочередной задачей компаний. Почти весь бизнес переходит в онлайн-формат, что обусловлено тенденциями современного мира. Люди всё больше пользуются различными сервисами, где и вводят личные данные различной степени конфиденциальности. Поэтому требуется применять различные способы защиты(шифрования), чтобы данные пользователей не становились доступны третьим лицам.

**Цель работы**

Разработка приложения для шифрования данных с применением алгоритма RSA[[1]](#footnote-1)

**Задачи:**

1. Изучение криптографических алгоритмов и их применение
2. Разработка приложения целью которого является шифрование данных
3. Презентовать и рассказать о своём приложении

**Предмет исследования:** места применения, характеристика алгоритма RSA

**Объект исследования:** криптография, криптографический алгоритм RSA и др.

**Гипотеза:** если всё больше людей начинают пользоваться онлайн сервисами, оставляя свои данные, которыми не должны владеть третьи лица, то этим же сервисам требуется применять различные протоколы безопасности, методы защиты (шифрования данных), иначе это может привести к утечке данных и к последствиям как для компании, так и для пользователя.

**Методы исследования:** изучение математической базы алгоритмов, разработка ПО

**История**

Сокрытие личных данных касается такой науки как *криптография.* Поэтому перейдем к её краткой истории.

История криптографии начинается на том моменте, когда человечество осознало, что не вся информация должна быть доступной к чтению. Потому что каналы связи - в то время обычные дороги, не были столь безопасными и надежными. Посла могли попросту убить по пути или сам посол мог оказаться предателем и рассекретить сообщение. Тогда в 3-ем тысячелетие до нашей эры, появился алфавитный метод шифрования (замены символов одного алфавита из другого).

Новой эрой науки послужили 70-ые года XX века при переходе к математической криптографии. Математические алгоритмы шифрования относительно молодые и эта ветка криптографии активно развивается по сей день.

**Криптография в настоящее время**

В наш век применяются самые различные алгоритмы шифрования, которые защищают как данные на домашнем компьютере, так и целую базу данных компаний. Также безусловно шифруется и поток данных в интернете.

Все алгоритмы делятся на два типа: *асимметричного шифрования и симметричного.*

*Симметричный алгоритм* - криптографический алгоритм, в котором для шифрования и дешифрование применяется один и тот же ключ[[2]](#footnote-2).

Асимметричный алгоритм - криптографический алгоритм, который использует два связанных ключа. Один ключ является секретным (не разглашаемый), другой публичным, который может свободно распространяться. Публичным информация шифруется, а секретным расшифровывается.

Т.е. в симметричном типе шифрования используется только **один ключ**, а в ассиметричном **два ключа**.

**Принципы работы двух типов шифрования**

**Ассиметричный тип шифрования**

В качестве примера может послужить упомянутый в самом начале алгоритм шифрования *RSA*. Он является примером одного из самых популярных алгоритмов шифрования.

Для начала, требуется сгенерировать два ключа: приватный и публичный.

1. Подберем два разных простых числа **P и Q**, длина их побитовой двоичной записи влияет на криптографическую стойкость, в зависимости больше-лучше.
2. Находим число **N**=**P\*Q**
3. Определим число **D**, которое будет являться простым и не иметь общих делителей с произведением **(P-1) \* (Q-1)**, кроме единицы
4. Определим число **E**, для которого выполняется тождество: **(E\*D) mod[[3]](#footnote-3) ((P-1) \* (Q-1)) = 1**
5. Открытый ключ**(E; N),**секретный ключ***(D; N).***

Попробуем по данному алгоритму зашифровать и расшифровать короткое сообщение:

1. Возьмем два случайных простых числа: **P=3** и **Q=7**
2. **N=P\*Q=7\*3=21**
3. **D=17**
4. **E=5**
5. Открытый ключ (5; 21), закрытый ключ (17; 21)

Допустим наше сообщение это число 19. Формула шифрования (Me) mod N, где M – цифра, либо цифра соответствующей букве (для шифрования текстовых сообщений).

195 mod 21 = 2476099 mod 21 = 10.

Наше зашифрованное сообщение – 10.

Расшифровка проходит по схожей формуле – (Md) mod N.

1017 mod 21 = 19.

Расшифрованное сообщение – 19, что ровно то, что и было изначально.

**Действительным примером** может послужить передача данных, зашифрованных ассиметричным типом шифрования, в сети Интернет. Так при отправке конфиденциальных данных, сервер отправляет компьютеру пользователя **открытый ключ**, которым шифруется сообщение, но этим же открытым ключом, **невозможно его расшифровать**, в чём и есть достоинство ассиметричного типа шифрования. Т.е. даже при перехвате сообщения любыми доступными способами, оно не будет расшифровано. При получении зашифрованного сообщения сервер расшифрует его **закрытым ключом**, который известен только ему. Пара ключей, как правило одноразовая.

Компьютер

Сервер

Сообщение расшифровывается секретным ключом

Пара: секретный-публичный ключ

Зашифрованное открытым ключом сообщение

Сообщение

Открытый ключ

**Симметричный тип шифрования**

Примером симметричного типа шифрования может послужить ROT или “Шифр Цезаря”

Принцип работы алгоритма очень прост – это сдвигание алфавита на определенное количество позиций, равное ключу.

Попробуем зашифровать сообщение “HELLO!”:

1. Возьмём ключ – 13.
2. Сдвинем каждую букву в слове на 13 позиций вправо
3. Получим зашифрованное сообщение: “Uryyb!”

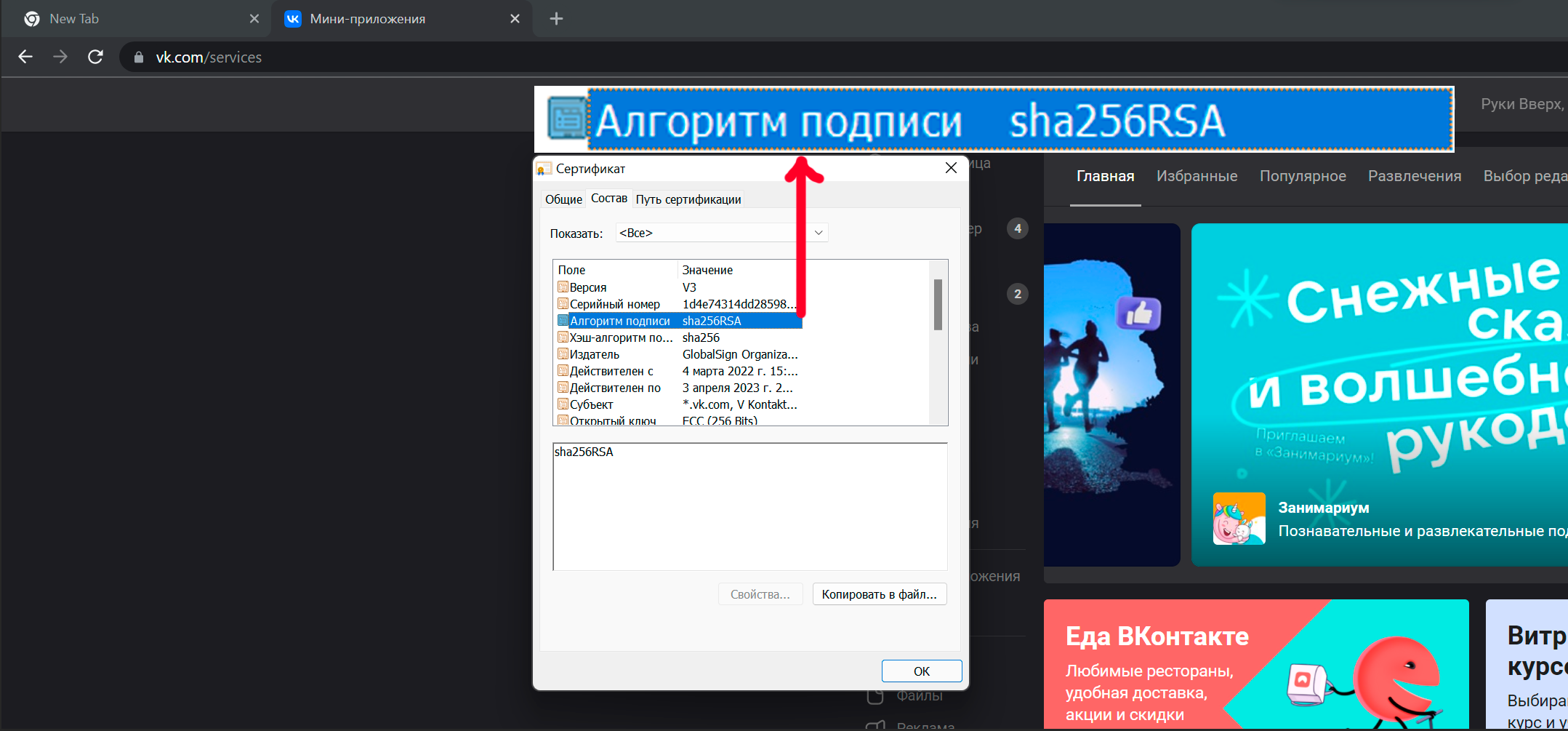
Расшифруем наше сообщение обратно, воспользовавшись тем же ключом, и сдвинем каждую букву на 13 позиций влево. Получим то же самое – “Hello!”

Так ярко прослеживается главный недостаток симметричного типа шифрования – шифрование и расшифровка происходит с использованием **одного ключа**. Поэтому симметричные алгоритмы применяют только для одностороннего шифрования, т.е. шифрование без последующей расшифровки, так **называемое хеширование.**

**Реальные примеры шифрования**

Становится очевидным, что почти ни одна сфера не обходится без применения шифрования данных. Шифрование применяется почти везде, начиная от зашифрованных данных на школьном сервере, шифрования интернет траффика, заканчивая архивными документами, засекреченными государством.

Примером может послужить социальная сеть “Вконтакте”, алгоритм применяемый сайтом общеизвестен, поэтому мы можем сами его посмотреть. Слева от строки с ссылкой сайта находится “замочек”, нажав который и открыв сертификат, можно будет увидеть подробную информацию о сайте.



Так весь поток траффика между сервером и пользователем на протяжении всего его пути зашифрован.

1. Криптографический алгоритм с открытым ключом, основывающийся на вычислительной сложности задачи факторизации больших целых чисел. [↑](#footnote-ref-1)
2. Ключ - секретная (при ассиметричном типе шифрование есть и публичная) информация, используемая криптографическим алгоритмом при шифрование и дешифрование информации. [↑](#footnote-ref-2)
3. Mod – операция деления с остатком. *10 mod 3 = 1* [↑](#footnote-ref-3)