Оформить как урок в котором демонстрируется работа в криптографией(rsa) в python

Проект это что сможет использовать учить информатики.

Цель:

Провести ознакомительный урок на тему «Криптография» и в дальнейшем ввести в его в программу обучения.

Задачи:

1) Изучить теоретическую базу криптографии

2)Создать программу, которая поможет наглядно увидеть принцип работы криптографии

3) Составить план урока

4) Применить программу на практике

Актуальность:

В наше время мы ежедневно сталкиваемся с криптографией — когда хотим что-то оплатить в интернете, авторизоваться на сайте или подписать электронные документы. Криптографические методы помогают защитить персональные данные и обеспечивают безопасную передачу информации в сети. Но как это всё устроенно? Данная работа поможет узнать школьникам и не только, как устроенная эта наука.

Оснащение и оборудование, использованное при создании работы

1)Язык программирования Python

2)Библиотеки tkinter, rsa

3)Среда разработки – программа PyCharm

Описание (урока или программы)

Есть разные способы классификации криптографических методов, но наиболее распространённый вариант деления - по количеству ключей.

Выделяют следующие виды:

1)Бесключевые методы, в которых не используются ключи;

2) Одноключевые или симметричные методы, в который используется дополнительный ключевой параметр - секретный ключ;

3) Двухключевые или асимметричные методы, в которых используется два ключа - секретный и открытый.

Наша программа будет основываться на ассиметричном шифровании. Основная особенность асимметричного шифрования - секретный ключ известен лишь одному человеку. При симметричном шифровании он должен быть известен двоим.

Плюсы:

1)Не нужно создавать защищённый канал для передачи секретного ключа - все взаимодействия происходят в открытом канале;

2) Наличие единственной копии ключа уменьшает шансы его утраты и позволяет установить персональную ответственность за сохранение тайны;

3)Наличие двух ключей позволяет использовать шифрование в двух режимах - секретной связи и цифровой подписи.

Минусы:

1) Возможность подмены открытого ключа,

2) Медленная скорость шифрования.

**Результат работы:**

**Полноценный ознакомительный урок по криптографии, который можно будет проводить в школах.**

**Перспективы использования результатов работы**

**Надеюсь, в будущем данная работа может стать частью учебного плана по информатике для 8-11 классов.**