1. **Актуальность темы.** Исследование истории криптографии актуально в связи с несколькими факторами:

* Мне интересно как в прошлом происходило шифрование важнейших сообщений, как развивалась эта наука, какие методы она использовала.
* Общественная актуальность заключается в том, что изучение развития шифров может дать новые идеи для усложнения используемых методов шифрования.

1. **Цель работы**. Рассмотрение и изучение развития методов шифрования информации с течением времени, создание программы шифрования сообщений при помощи этих методов.
2. **Задачи**.

* Исследовать эволюцию криптографии в разные временные рамки
* Анализировать ключевые события и прорывы в истории криптографии, которые повлияли на развитие этой области.
* Изучить различные методы и алгоритмы шифрования.
* Создание программы на python, которая, применяя методы шифрования, кодирует сообщения.

1. **Проблема, решаемая проектом.** Изучение того, как происходило шифрование сообщений в разные временные рамки.
2. **Этапы работы**

* Постановка объекта исследования.
* Определение целей.
* Выполнение проекта.
* Создание продукта
* Завершение проекта.

1. **Предмет исследования**. История криптографии.
2. **Объект исследования.** Методы шифрования.
3. **Методы исследования**.

* Изучение литературы и других источников информации.
* Сравнение, противопоставление.
* Самооценка, наблюдение.
* Практика.

1. **Теоретическая значимость.** Изучение методов шифрования, их историю и слабые места.
2. **Практическая значимость.** Создание программы на python улучшила мои знания в этом языке программирования.
3. **Продукт проекта.** Программа на python, которая, применяя методы шифрования, кодирует сообщения.

Криптография — это наука, занимающаяся изучением методов шифрования данных с целью их защиты. Шифрование представляет собой процесс преобразования информации в вид, непонятный для непосвященных. Для этого используются различные методы и алгоритмы.

Продуктом моего проекта является программа, которую можно посмотреть поэтому qr коду, далее в презентации на примере моей программы я разберу алгоритм трех методов шифрования текста.

Шифр Цезаря. Принцип: каждая буква слова заменяется на букву, находящуюся в другой позиции исходя из шага шифровки. Для русских алфавита существует всего 33 ключа, из-за этого он прост в переборе. (шифр подстановки)

Шифр Аль-Кинди. Принцип: к каждому символу из алфавита подставляется другой случайный символ и заменяется в шифруемом слове.

Шифр Блез де Виженера. Принцип: ключевое слово, выбранное отправителем, повторяется пока не станет больше или равно сообщению, исходя из пересечения букв выбирается буква в шифре. Самое важное, что одинаковые символы исходного слова в шифре будут выглядеть по-разному. (полиалфавитный)

Исследовав историю криптографии, можно сделать несколько выводов. В раннее время шифрование сообщений происходило по простым алгоритмам, которые, на то время, давали достойную защиту информации. С каждым веком алгоритмы шифрования усложнялись, создавались методы, опиравшиеся на определенные формулы.

Также, изучив эти методы, я смог создать программу на python, которая, применяя их, кодирует сообщения и понял, как происходило шифрование сообщений в разные временные рамки.

Считаю, что цель по выполнению данной работы достигнута.