Реферат посвящен теме криптографии – а именно криптоалгоритмам. Я рассмотрю несколько алгоритмов шифрования и дешифровки, выявлю их минусы и плюсы, выберу несколько алгоритмов и попробую реализовать их на Питоне.

Криптоалгоритмы используются для шифрования информации, которая не должна быть прочитана кем-то еще, кроме отправителя и получателя. Такие алгоритмы делятся на 2 типа: симметричные и ассиметричные.

Симметричные алгоритмы – самые «удобные». Они просты в реализации и хорошо изучены (так как появились раньше ассиметричных). Для шифрования и расшифровки используется один и тот же ключ.

Ассиметричные алгоритмы сложнее в реализации и использовании, но они гораздо надежнее. Для них требуются 2 ключа (открытый для шифровки и закрытый для расшифровки) и большая вычислительная мощность.

Помимо исследовательской работы я также попробую реализовать один из алгоритмов на языке Python, с которым я сейчас знакомлюсь. Будет использоваться среда PyCharm, для перевода программы в двоичный код (для увеличения производительности) я воспользуюсь компилятором.

Процесс работы я разделил на несколько этапов.

* Изучение алгоритмов шифрования
* Разбор принципа их работы
* Написание основной части реферата
* Написание выбранного алгоритма на языке Python

Используемые источники:

* Википедия
* http://www.codenet.ru/progr/alg/enc/ для рассмотрения алгоритмов
* <http://younglinux.info/python.php> для изучения Python