Г. Р. Байтингер, Д. С. Таранцей
(ГрГУ им.Янки Купалы, Гродно)

ИССЛЕДОВАНИЕ ШИФРОВ ЗАМЕНЫ МЕТОДАМИ КЛАССИЧЕСКОЙ КРИПТОГРАФИИ

Если немногим больше двадцати лет назад криптография была закрытой наукой, методы и исследования в которой проходили под грифом секретности, а литературы на русском языке практически не было, то теперь возникла необходимость знакомить с основами компьютерной безопасности не только студентов, но и школьников старших классов.

В рамках работы, проводимой на кафедры системного программирования и компьютерной безопасности ГрГУ им.Я.Купалы мы создаем учебный ресурс «Стойкость шифров замены», который бы мог частично устранить недостаток популярной литературы в этой области.

Нами был проведен эксперимент по изучению стойкости классических шифров замены к криптоанализу методом частотного анализа. В качестве шифров были выбраны шифр Цезаря, шифр Плейфера, основанный на биграммах, шифрование квадратом Вижинера.

Частотный анализ – это основной инструмент для взлома большинства классических шифров перестановки или замены. Данный метод основывается на предположении о существовании нетривиального статистического распределения символов, а также их последовательностей одновременно и в открытом тексте, и в шифротексте. Причём данное распределение будет сохраняться с точностью до замены символов как в процессе шифрования, так и в процессе дешифрования.

Для среднестатистического текста (в качестве которого взята 1-я часть романа Нила Стивенсона «Криптономикон» на английском языке и ее переводы на русский и немецкий. Объем файла – около 1 мегабайта), были получены частотные характеристики вхождения отдельных букв, биграмм и триграмм. Текст пердватительно приведен к верхнему регистру. Программа для получения частотных характеристик написана на языке Python с использованием библиотек SciPy и библиотекой PIL (Python Imaging Library) для простейшей обработки изображений.

Программный эксперимент продемонстрировал нестойкость шифров замены, ввиду того, что сохраняется картина классического распределения частот символов открытого текста и шифротекста.

Использование штфра Плейфера требует построения частотных таблиц для биграмм, что значительно усложняет анализ.

Использование шифра Вижинера нарушает классическое распределение частот символов алфавита и не позволяет использовать для криптоанализа шифротекста методы частотного анализа. Более того, в зависимости от используемого ключевого слова гистограммы частот получаются весьма непохожими друг на друга, что тоже усиливает криптостойкость шифра.

Однако распределение частот далеко от равномерного, что подтверждает возможность криптоанализа таких шифротекстов.