НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
«ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»

Московский институт электроники и математики им. А.Н. Тихонова

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Задания (с разбором): материал 18

Шифры гаммирования

Евсютин О.О.

Москва 2020

1 ЦЕЛЬ РАБОТЫ

Целью данной работы является приобретение навыков программной реализации и криптоанализа применительно к шифрам гаммирования.

2 КРАТКИЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

Гаммирование заключается в наложении на открытый текст некоторой последовательности (гаммы), генерируемой на основе ключа шифрования. Под наложением гаммы на открытый текст обычно подразумевается сложение символов открытого текста с символами гаммы по модулю соответствующего алфавита. Однако в классических шифрах наложение гаммы может означать вычисление значений символов шифртекста на основе значений соответствующих символов открытого текста и гаммы по некоторому правилу.

Классическим представителем шифров гаммирования является шифр Виженера.

Символы алфавита A мощностью m представляются элементами кольца классов вычетов $\mathbb{Z}_m$.

Зашифрование заключается в сложении символов открытого текста с символами гаммы по модулю m.

Расшифрование заключается в сложении символов шифртекста с символами гаммы по модулю m.

В шифре Виженера в качестве ключа шифрования обычно использовалась короткая фраза, называемая лозунгом (паролем), которая циклически повторялась, формируя гамму.

Существует другой подход к формированию псевдослучайной ключевой последовательности — самоключ Виженера. Здесь в качестве начального ключа мы выбираем только один символ, к нему добавляем все символы открытого текста, за исключением последнего, и таким образом формируем гамму. Либо мы можем формировать гамму, добавляя к начальному символу поочередно символы шифртекста

3 ЗАДАНИЕ

1) написать программную реализацию следующих шифра Виженера с тремя способами выработки гаммы на основе секретного ключа шифрования:
   - повторение короткого лозунга;
   - самоключ Виженера по открытому тексту;
   - самоключ Виженера по шифртексту;
2) изучить методы криптоанализа шифров гаммирования с использованием дополнительных источников;
3) провести криптоанализ данных шифров;
4) подготовить отчет о выполнении работы.

Программа должна обладать следующей функциональностью для каждого из реализованных в ней шифров:

1) принимать на вход произвольную последовательность символов, вводимую пользователем в качестве открытого текста или шифртекста;
2) принимать на вход секретный ключ вида, соответствующего конкретному шифру;

3) осуществлять зашифрование или расшифрование введенного текста по выбору пользователя.

Отчет должен содержать следующие составные части:

1) раздел с заданием;
2) раздел с краткой теоретической частью;
3) раздел с двумя-тремя примерами «ручного» шифрования для произвольных последовательностей символов;
4) раздел с результатами работы программы для тех же последовательностей символов, что и в предыдущем разделе;
5) раздел с примерами криптоанализа реализованных шифров;
6) раздел с выводами о проделанной работе.