Университет ИТМО

Факультет программной инженерии и компьютерной техники

Кафедра вычислительной техники

Лабораторная работа № 4 по дисциплине ”Методы и средства защиты компьютерной информации”

Вариант 12

Выполнил:

Чебыкин И. Б.

Группа: P3401

Проверяющий: Ожиганов А. А.

Санкт-Петербург, 2018

Цель работы.

Расшифровать криптограмму, зашифрованную шифром Виженера, методом вероятных слов, получить ключ шифрования.

Расшифровать криптограмму, зашифрованную «бегущим» ключом, методом вероятных слов, получить «бегущий» ключ.

Выполнение

Шифр Виженера

Криптограмма

ШСЭОДНЙИ ШДЗЯИЦНЮГРАФЮАТИФНГЯ АИУТОЦ АОУТЧТТПВБТЧЦ ЖТР ЦК ЯРРТЗРЕЭИК
ЛЫЕУОБТОФСБАБОНЧАПИБТЙЙЖХ ГУУМАПМРЖОЬ СЫФЬИСАЗИЦРЧМАЭАБПЧЙРРЗПОХЭ
БОБЕЪЬЬПЗВМОЧЫПДНЯИЛУЪВЭ ЛДБШРВЮЫЫЯПИЙ ХЧОУИЧ ЙХФРВКТЧМ Т ЙАЛТСШМРСЫТ
ЮТБПЧХОЦЕПИЗЙВПТЗКЪЬЕ

Открытый текст

ОСНОВНАЯ ИДЕЯ МНОГОАЛФАВИТНЫХ СИСТЕМ СОСТОИТ В ТОМ ЧТО НА ПРОТЯЖЕНИИ ВСЕГО
ТЕКСТА ОДНА И ТА ЖЕ БУКВА МОЖЕТ БЫТЬ ЗАШИФРОВАНА ПО РАЗНОМУ ТО ЕСТЬ ЗАМЕНЫ ДЛЯ
БУКВЫ ВЫБИРАЮТСЯ ИЗ МНОГИХ АЛФАВИТОВ В ЗАВИСИМОСТИ ОТ ПОЛОЖЕНИЯ В ТЕКСТЕ

Ключ

КАРАВАЙ

Протокол криптоанализа

Так как известно, что исходный текст на тему криптографии, будем пробовать вероятные слова, связанные с данной темой. Например, «криптоанализ», «шифр», «метод», «сообщение», «информация» и другие.

Проверка вероятных слов «КРИПТО» и «метод» ничего не дала. Проверка вероятных слов «АЛФАВИТ» , «ИНФОРМАЦИЯ» , «ОТКРЫТЫЙ», «СЛОВО» тоже ничего не дала.

Попробуем вероятное слово «БУКВА». При переборе мы получили слово КАРАВАЙ.

Бегущий ключ

Криптограмма

ЩЩРСРКЦФГЬЬЮГЦЫЦВАГСЬЪЩАЙДЖАЙЫЧНЕОЦООЛНСЕЮГРРУНВПЯЬДПЮЗГЕХЙФЗЦВГЫОТТУВХМГКЧЯМЪ
ЙНБШАЯГЭ Р ФЕЖСЪЯПЛЩЬНШФ ЩУ ЧСРБФЙШТДФИ ПЦРЦГЯЩОХЗШИХЕ ЦЗОБЯЫТЧП ЗМТЛЩДЫМЛУЛЪ

Открытый текст

КЛАССИЧЕСКАЯ ИЛИ ОДНОКЛЮЧЕВАЯ КРИПТОГРАФИЯ РЕШАЕТ ФАКТИЧЕСКИ ЛИШЬ ДВЕ ЗАДАЧИ
ЗАЩИТУ ПЕРЕДАВАЕМЫХ СООБЩЕНИЙ ОТ ПРОЧТЕНИЕ И ОТ МОДИФИКАЦИИ ПОСТОРОННИМИ ЛИЦАМИ

Ключ

ПОРА В ПУТЬ ДОРОГУ ДОРОГУ ДАЛЬНЮЮ ДАЛЬНЮЮ ДАЛЬНЮЮ ИДЕМ НАД МИЛЫМ ПОРОГОМ КАЧНУ
СЕРЕБРЯНЫМ ТЕБЕ КРЫЛОМ ПУСКАЙ СУДЬБА ЗАЫРОСИТ НАС ДАЛЕКО ПУСКАЙ ТЫ К СЕРДЦУ Т

Протокол криптоанализа

Так же как и в предыдущем случае, исходный текст на тему криптографии. Будем пробовать вероятные слова, связанные с данной темой. Например, «криптоанализ», «шифр», «метод», «сообщение», «информация» и другие.

Попробуем вероятное слово «криптографи». В ключе получаем сочетание букв «НЮЮ ДАЛЬНЮЮ».

Обнаруживаем что слово ДАЛЬНЮЮ повторяется три раза, добавляем слово ДОРОГУ перед ДАЛЬНЮЮ и получаем текст песни “Пора в путь-дорогу”.