Университет ИТМО

Кафедра ВТ

Методы и средства защиты компьютерной информации

Лабораторная работа №4

Вариант 9

Выполнил: Фролов Сергей

Гр. Р3415

2017

Задание

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

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

Выполнение

1. Шифр Виженера

Криптограмма:

ШЪШПЪЫАЫКЫИЪХКНОЮЛОТННЫЭАЯНЛОЙЮПШТДУХШТГМПУЪ ШОММПЮПЮБШНЗЬМРТГМШЦЮ ОЛЭАЪЦВ КММОЬ ИЮ ТХО ЧЭЕТЩЮЛИРАУЦЮГЦМПУЪШОМН ЦЙШСЧЫЛЙСЮВИЯЬНОЫЯЗЧАФОЮГЦМС ШЫБЮН ЪПБОМЗ ШЪШПЪЫАЫКЫИПН ЪШЭОИШФОМШТХЗХНБШФШЫВ

Открытый текст:

КРИПТОАНАЛИТИК ДОЛЖЕН СНАЧАЛА ОПРЕДЕЛИТЬ ПЕРИОД ПРЕОБРАЗОВАТЬ ШИФРОГРАММУ В МАТРИЦУ ДЛЯ ПРЕДПОЛАГАЕМОГО ПЕРИОДА И ИСПОЛЬЗОВАТЬ ДЛЯ КАЖДОГО СТОЛБЦА МЕТОДЫ КРИПТОАНАЛИЗА МОНОАЛФАВИТНЫХ ШИФРОВ

Ключ:

ОКРАИНА

Протокол криптоанализа:

В начале строки было введено КРИПТО, что дало ключ ОКРАИН. Это навело на мысль что ключом является слово «окраина» и это предположение подтвердилось.

2. «Бегущая строка»

Криптограмма:

ДЦКЛНСРЫСЙДЮДЯОХ ММФЧПШВБОММУЧЦДНУТЮ ЮД ЮТЫФДЭЕБССМ РЛУИРОРЗ КЫРЦЙСЩ ИЫТИ ЯАХШЪЦЕСОЭЮОДНЧДЧОВ ЭОЗЯЯЭЫТЪККАМ ИОРП

Открытый текст:

ШИФРОВАНИЕ МЕТОДОМ ПЕРЕСТАНОВКИ ОСНОВАНО НА ПЕРЕСТАНОВКЕ СИМВОЛОВ ОТКРЫТОГО ТЕКСТА ПОРЯДОК КОТОРОЙ ОПРЕДЕЛЯЕТ КЛЮ

Ключ:

НОЧЬ ПРОЙДЕТ НАСТАНЕТ УТРО ЯСНОЕ ВЕРЮ СЧАСТЬЕ НАС С ТОБОЙ ЖДЕТ НОЧЬ ПРОЙДЕТ ПРОЙДЕТ ПОРА НЕНАСТНАЯ СОЛНЦЕ ВЗОЙДЕТ

Протокол криптоанализа

Один из вариантов первого слова ШИФР_ оказался удачным. Пробел после слова ШИФР не дал результата и путем подбора однокоренных слов, выяснилось, что первое слово ШИФРОВАНИЕ. После еще нескольких угаданных слов прояснились первые слова песни и стало ясно, что это слова песни из м/ф «Бременские музыканты»