Университет ИТМО

Лабораторная работа №4

Методы и средства защиты компьютерной информации

Вариант 4

Выполнил:
студент гр. Р3415
Припадчев Артём

Санкт-Петербург
2016

Задание

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:

ШФЬИНХМУОФЬМЫАЮДЩТЧЫОПИМСУЗЛФЭШХРРНЗЦЫПФИЩЦШБУИГЧНЬВСТФВХ ХНЗЦТЪОЮГШЯПГЛХЫУПЛ ОШФПЗОППВОАТМЫХЮИМ ЙАСЬЕЩЭТАИКЭПДЭСМ ЙЭЫАЧ ЙБЮХОЩЭТЖХОМШ
ШВСЫСЧРОИМПЦЮВИШТТЮДМТЧСЫЛСИЙЫЬВБТСАЯГСЪДЯПФПЫЫАССММКТБГКУ ПТВФЛЫМЫЫЛСИЙ РЗЕУЧАПШРНЧЫБЯ ЙЬАБВКШЗЙПЪТЫЛНПЛСЧХРЖЛТИЙЧЮФТ ЩТЪВНТЦЕПТОЮЬА СНЪТЗПОИВ

Открытый текст:

ОБМЕНИВАЯСЬ СООБЩЕНИЯМИ ЗАШИФРОВАННЫМИ СИММЕТРИЧНЫМ СЕКРЕТНЫМ КЛЮЧОМ АЛИСА И БОБ ДОВЕРЯЮТ СВОЕМУ ОБЩЕМУ СЕКРЕТНОМУ КЛЮЧУ ПОТОМУ ЧТО ОНИ СОЗДАЛИ ЕГО ИЛИ ОБМЕНЯЛИСЬ ИМ БЕЗОПАСНЫМ СПОСОБОМ А ТАКЖЕ УСЛОВИЛИСЬ НАДЕЖНО ХРАНИТЬ ЭТОТ КЛЮЧ ЧТОБЫ ИСКЛЮЧИТЬ ДОСТУП К НЕМУ ПОСТОРОННИХ ЛИЦ

Ключ:

КУРГАН

В ходе анализа были опробованы различные слова из области криптоанализа, и к данному шифру подошло слово «СООБЩЕНИе». Было обнаружено слово курган, которое подошло и был получен открытый текст.

Бегущий ключ:

Криптограмма:

ЪЯДСЯФЦЬМКЙЛЫВ ВЖНМПОМФНПИЬЗНММТКСЛКТНЛНЖВШЩГ ОРМДЬАЩАХЩУНРЯНОРГЗУПЭЗБНРЪЕРНТЬИЗТЭЫУЬЛ ЯНШСЧЯСЦРЩУОК МЭОПТ ПНКЪШИЯЙЫРЬУУАЪАЛЩСЙФЛИЫФЛКДЪВЭЕЭОШ

Открытый текст:

ИДЕЯ ИСПОЛЬЗОВАТЬ КВАНТОВЫЕ ОБЪЕКТЫ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ ОТ ПОДДЕЛКИ И НЕСАНКЦИОНИРОВАННОГО ДОСТУПА ВПЕРВЫЕ БЫЛА ВЫСКАЗАНА СТЕФАНОМ ВЕЙСНЕРОМ

Ключ:

ТЫ У МЕНЯ ОДНА СЛОВНО В НОЧИ ЛУНА СЛОВНО В СТЕПИ СОСНА СЛОВНО В ГОДУ ВЕСНА НЕТУ ДРУГОЙ ТАКОЙ НИ ЗА КАКОЙ РЕКОЙ НИ ЗА ТУМАНАМИ ДАЛЬНИМИ СТРАНАМ

Подбирая различные слова данной области было использовано слово «использовать». Это слово позволило частично разгадать начальные слова песни «Ты у меня одна» Юрия Визбора. Подставив слова песни был получен исходный текст.

Вывод

В ходе выполнения лабораторной работы был изучен метод вероятных слов. Были расшифрованы тексты, зашифрованные шифром Вижнера и «бегущим» ключом.