Университет ИТМО

Лабораторная работа №5

Методы и средства защиты компьютерной информации

Вариант 4

Выполнил:
студент гр. Р3415
Припадчев Артём

Санкт-Петербург
2016

Задание

Расшифровать криптограмму, зашифрованную методом перестановок, получить ключ шифрования. Расшифровать криптограмму, зашифрованную методом перестановок по путям Гамильтона, получить ключ шифрования. Расшифровать криптограмму, зашифрованную методом табличной перестановки, пользуясь для этой цели таблицей частот диаграмм русского языка, получить ключ шифрования.

Выполнение

Простая перестановка:

Криптограмма:

Т СПЕКЛИОЛУЧСЕ ВОМБИЛЯ ГААРОД ТЯАМЕО ФКРЕТУОЮОРЧТ ОАСИО ЛСПЗТЬ УЮЛОДПЯ СИИЯАНЕ РГОБЫА ОТРСПТЕДВЕА ЬТЕ ССБЕОУТ ПКАЛТОРЕ ПКРНАМ ИТЕРК АКИХТЫОЕОРИО ЛСПЗТЬСУЮ КЯАВ ЕРФИТЕХДЯЕ ГТЕ ЛАРИАКХ НДСОЯЯТНП ОА ПЖДИРУЕОНЙННПТ ФЛАР ОПМЕРЕЕЩЕМЮЙАСЩЕ ЕЯРВВ ВХНИ ЗОИГ КАТДО КНУ ДИБ ИЬМСНЕТААТ ЕУР ЛКВХСУЕРВ ССЯОАТ ПКОИПМДНЕЯА ТСВХВВЕР

Открытый текст:

СТЕК ПОЛУЧИЛ СВОЕ ИМЯ БЛАГОДАРЯ МЕТАФОРЕ КОТОРУЮ ЧАСТО ИСПОЛЬЗУЮТ ДЛЯ ОПИСАНИЯ ЕГО РАБОТЫ ПРЕДСТАВЬТЕ СЕБЕ СТОПКУ ТАРЕЛОК НАПРИМЕР ТАКИХ КОТОРЫЕ ИСПОЛЬЗУЮТСЯ В КАФЕТЕРИЯХ ГДЕ ТАРЕЛКИ НАХОДЯТСЯ НА ПОДПРУЖИНЕННОЙ ПЛАТФОРМЕ ПЕРЕМЕЩАЮЩЕЙСЯ ВВЕРХ И ВНИЗ КОГДА КТО НИБУДЬ СНИМАЕТ ТАРЕЛКУ СВЕРХУ ВСЯ СТОПКА ПОДНИМАЕТСЯ ВВЕРХВ

Ключ:

251634

В ходе выполнения данного задания был выбран ключ длиной 6 цифр. Посмотрев первые 6 символов были попробованы следующие комбинации «СПЕКТ» и «СТЕК». Слово «СТЕК» подошло и сразу текст был расшифрован.

Пути Гамильтона:

Криптограмма:

НАЗ ОАКВКМ ДИАПИАТО ЛИСТЯ СЛ ПТА ВИНЕАОЕЛ ДОБ СО Е РГ ОНРАПДООБ СН СОЕ НТХЛИО ЭОЧТ ОЛОТ БОЫВА ПЕСРРЬ ЕПТЕОВ АЗРГ НО УРЖ ИЕТО ТОБ О ПДСНРМУО ВААЛЧАРОС ОЕП ВМТЬЕЮРЯРЗНАОЛИДВВ АВ ЛСЬО У ОРАГДЬЯДРЕЕВЕН АЗРВЬ ЧВАИТРАИПО ППАНЫМН ИЗРОМК Я ИВЛНРАПД ОГОМДПО ТАР Т ОС ТАВ ЕКЕ ЕРАРСНЧБЕВРЕЩЬАОЙТЗ

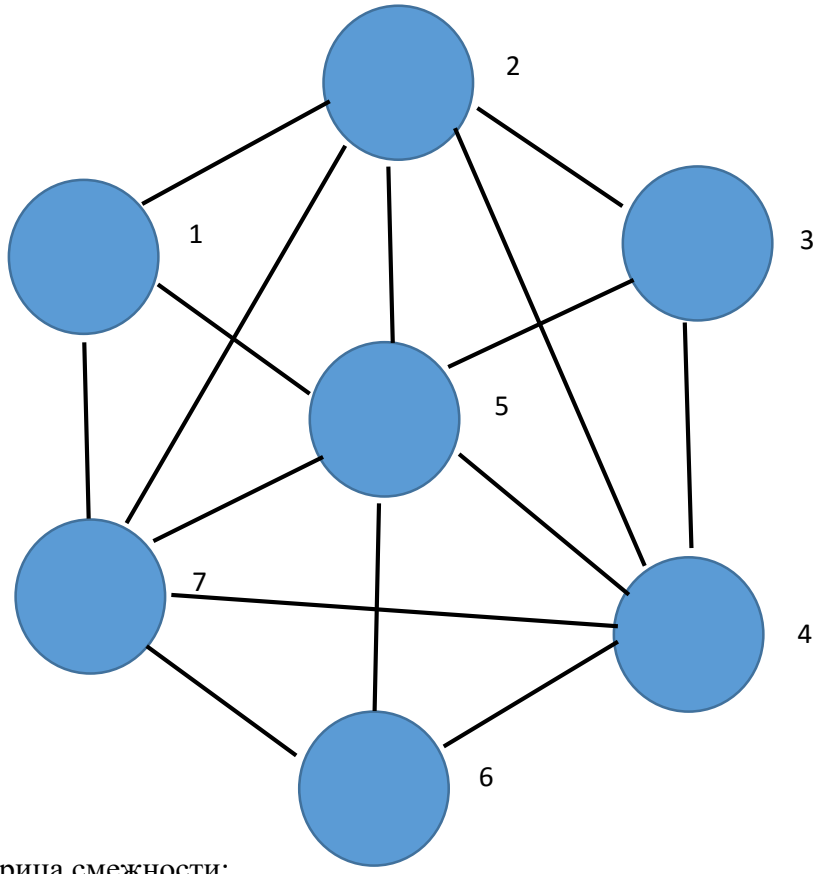
Открытый текст:

ЗА ОКНАМИ ДАВКА ТОЛПИТСЯ ЛИСТВА И ПАЛОЕ НЕБО С ДОРОГ НЕ ПОДОБРАНО СЕ СТИХЛО НО ЧТО ЭТО БЫЛО СПЕРВА ТЕПЕРЬ РАЗГОВОР УЖ НЕ ТОТ И ПО ДОБРОМУ СНАЧАЛА ВСЕ ОПРОМЕТЬЮ ВРАЗНОРЯД ВВАЛИЛОСЬ В ОГРАДУ ДЕРЕВЬЯ РАЗВЕНЧИВАТЬ И ПОПРАННЫМ ПАРКОМ ИЗ ЛИВНЯ ПОД ГРАД ПОТОМ ОТ САРАЕВ К ТЕРРАСЕ БРЕВЕНЧАТОЙЗЩЬ

Ключ:

6713425

В ходе выполнения данного задания был выбран граф длиной 7 символов:



Матрица смежности:

X	1	1	1		1	1
1	X	1	1	1		1
1	1	X	1	1	1	
	1	1	X	1	1	1
1	1	1	1	X	1	1
1		1	1	1	X	1
1	1		1	1	1	x

В ходе выполнения задания после выбора графа был произведён перебор. Но изначально он не дал результатов. Далее было решено пробовать различные комбинации букв в первых 7-ми символах. Когда попробовали «ЗА ОКНО», был получен ключ и текст был расшифрован.

Использование таблицы частот диаграмм русского языка.

Криптограмма:

ИДАБОШЛ АД НЛИЫВОТОЫ ГОВЕНМВА ЕНОЕ СХЬСОРЕЛТ ТАТСССАЬС ОО СЯМ

Открытый текст:

ЛОШАДИ БЫЛИ ДАВНО ГОТОВЫ А МНЕ ВСЕ НЕ ХОТЕЛОСЬ РАССТАТЬСЯ СО СМО

Ключ:

75632184

В ходе выполнения задания было подмечена комбинация первых 8 символов. Попробовав расставить строки таким образом, чтобы получилось слово «лошади». В итоге строки стали на свои места и текст был расшифрован.

Вывод

В ходе выполнения лабораторной работы были изучены метод перестановок и способы их расшифровки. Были получены ключи к каждому тексту и текст был расшифрован.