

Федеральное государственное автономное образовательное учреждение высшего образования
«Санкт-Петербургский национальный исследовательский университет
информационных технологий, механики и оптики»

Прикладная математика
Лабораторная работа №6

Выполнила: Калугина Марина

Группа: Р3302

г. Санкт-Петербург

2019 г.

Вариант 3

Задание:

Дешифровать текст, закодированный моноалфавитной подстановкой и многопетлевой полиалфавитной подстановкой

Моноалфавитная подстановка

СТАТИСТИКА

Крип-ма	Рус. яз.
Б 0.146	О 0.175
Ф 0.088	О 0.089
У 0.085	Е 0.072
И 0.069	А 0.062
В 0.064	И 0.062
О 0.059	Н 0.053
Ъ 0.051	Т 0.053
Х 0.048	С 0.045
Ю 0.045	Р 0.040
Т 0.045	В 0.038
Э 0.043	Л 0.035
М 0.037	К 0.028
П 0.021	М 0.026
Ц 0.019	Д 0.025
Н 0.019	П 0.023
Щ 0.019	У 0.021
З 0.016	Я 0.018
Я 0.016	Ы 0.016
О 0.016	З 0.016
А 0.016	Ь 0.014
Д 0.016	Ъ 0.014
Л 0.013	Б 0.014
Г 0.013	Г 0.013
Б 0.011	Ч 0.012
Р 0.008	Й 0.010
Ж 0.008	Х 0.009
К 0.003	Ж 0.007
Й 0.003	Ю 0.006
Ш 0.003	Ш 0.006
Ч 0.003	Ц 0.004
	Щ 0.003
	Э 0.003
	Ф 0.002

СИМВОЛ Ч ЗАМЕНИТЬ НА Ю

КРИПТОГРАММА

ТВЯВМИТЬЪЦУМЪЪФ УХУЪУЪЮЪТЪТЩАПГВЪВЪВЪХТВОЗФНГФОЪИВЪФЦУМВИИФНЪЖФЭВЪЭПЯУНЪЮЦУШУОЮТРВ ФХЪХФЭИКУЪ
ВЕЧЕРНЯЯ ЗАРЯ ПОГАСАЛА И В ВОЗДУХЕ ЕЩЕ СВЕТОМ ХОТЯ НЕ ОЗАРЕННОМ БОЛЕЕ ЛУЧАМИ ЗАКАТИВШЕГОСЯ СОЛНЦА
ИУАЮИУЪЮЪ ПХОВОЛЬЮМЦЪЮТУОЛХЪГФЭФАИДВОВИЮЪПЪИФ ЫНФЮГЪОИПЭУХЛЬПЩУЪАФЭЮИУЪЭМНФЪИУЭМФОУТЬЩПОФЕ
НАЧИНАЛИ ГУСТЕТЬ И РАЗЛИВАТЬСЯ ХОЛОДНЫЕ ТЕНИ У НОГ МОИХ ТЯНУЛАСЬ УЗКАЯ ДОЛИНА ПРЯМО НАПРОТИВ КРУТОЙ
ЪХОВИФЪБФЦТДРУЭХЪЪАУХОДЪБФХЮИЮЩНВНЬЮФОЯУХЪФГТУОЮЪИВЭМЪОИУЪИВЗФАТЮШИУЪХДМФХОЛЬЮФЯИФЪЪТФРВЭ
СТЕНОЙ ВОЗВЫШАЛСЯ ЧАСТЫЙ ОСИННИК МЕНЯ ТОТЧАС ОХВАТИЛА НЕПРИЯТНАЯ НЕПОДВИЖНАЯ СЫРОСТЬ ТОЧНО Я ВОШЕЛ
ЪТЪЭФ МВЖЪ ПХОУЪТДХФШУЪОМУТУЪИУАИВЪАФЭЮИДЪТХЪНФШМУЪЪЖВЭУЪМФТИФЪХШУОВМОЛЧ
В ПОГРЕВ ГУСТАЯ ВЫСОКАЯ ТРАВА НА ДНЕ ДОЛИНЫ ВСЯ МОКРАЯ БЕЛЕЛА РОВНОЙ СКАТЕРТЬЮ

Таблица замен:

Криптограмма	Русский язык
Б	
Ф	О
У	А
И	Н
В	Е
О	Т
Ъ	Я
Х	С
Ю	И
Т	В
Э	Л
М	Р

П	У
Ц	З
Н	М
Щ	К
З	П
Я	Ч
	Г
А	Д
Д	Ы
Л	Ь
Г	Х
Б	Й
Р	Ш
Ж	Б
К	Ц
Й	Щ
Ш	Ж
Ч	Ю

Многопетлевые подстановки

СТАТИСТИКА (11)

Крипт.-ма

Рус. яз.

(F8) Ключ: **МГКДШНАЮАНУЙКГМТКЦШЬА**

СИМВОЛ С ЗАМЕНИТЬ НА

КРИПТОГРАММА

НУТИКЯ ИИМЭЧЬСОМЙЖКОЪЯНГМКБФНЙУЭЭВШЙМЧСТН ЬЮИМЯОНАЫЪАВЧДЖИИИМЪЙМЛРЪЪХВГ ЧЗНАДЧТЛЪТЧСВЛРЪСФГЛ
ПРИДУТ ЛИ КОРОВЫ С ПОЛЯ СТАРИК ПЕРВЫЙ ПОЗАБОТИТСЯ ЧТОБ ИХ НАПОИЛИ ЗАВИДИТ ЛИ ИЗ ОКНА ЧТО ДВОРНЯЖКА
АЪНИЖЕУАДЪФДЪЛ ЧЧАЮПЧНТИШУФЮПЗЧМТЯОЯН ЙЮСУДГЖЭОПИПТКПФН ЪФЪЕОС ГТАПЯМВПЗЕМСЕЛИ ЧЙКМЯИЗШНОЪАНИНТЛХ
ПРЕСЛЕДУЕТ КУРИЦУ ТОТЧАС ПРИМЕТ СТРОГИЕ МЕРЫ ПРОТИВ БЕСПОРЯДКОВ И ЖЕНА ЕГО СИЛЬНО ЗАНЯТА ОНА ЧАСА Т
ЪМЧЯОИК ШНЙФЛТМЪЗЕОШ КАКЪЯЖПЮШЧ ЕЗМЪРРФЯШЧПУВАДЭВЙАСУПЪ ЯЪЗИШРАПВЦДЪЗЕТКЕ МУЖКСЪЛНЧЭЯ ЙЕШАХЙЛЛЯК
РИ ТОЛКУЕТ С АВЕРКОЙ ПОРТНЫМ КАК ИЗ МУЖНИНОЙ ФУФАЙКИ ПЕРЕШИТЬ ИЛИШЕ КУРТОЧКУ САМА РИСУЕТ МЕЛОМ И НА
ЧВШДПЕНТСЪ НВКЖЭЭКЮ ЪШИЭНЪТХХИОКЪАНИЪ ШВШЭТИБЕЯТЛЪЭСФТМУШ ЦА УЛЬСЦГРИЕН БЕПЪОЙФЦ ХСБЙ ПЖШЛЪЛЕЙИ
БЛЮДАЕТ ЧТОБ АВЕРКА НЕ УКРАЛ СУКНА ПОТОМ ПЕРЕИДЕТ В ДЕВИЧЬЮ ЗАДАСТ КАЖДОЙ ДЕВКЕ СКОЛЬКО СПЛЕСТИ В Д
ЭЪБЭКЭППЕЛАШЗЕЗ ЮВАЭПГЛФИХЕОЖ ЪУЪГЭНЭХ ЮАЮМ НЬЧЛИХИТПНХХЧЪЙГПТШГЪИУОИЖЪОБЯЖЭВЧХЗЭСПАОУВЭФТЭТ
ЕНЪ КРУЖЕВ ПОТОМ ПОЗОВЕТ С СОВОЙ НАСТАСЬЮ ИВАНОВНУ ИЛИ СТЕПАНИДУ АГАПОВНУ ИЛИ ДРУГУЮ ИЗ СВОЕЙ СВИТЫ
НПЭГОШЪНЛТШГИНДР ЮТШЪГЦГТМЭМКЭЙИ ХНЙВШТИШОПРТДЛИНМЪЙВШЖИСААДЛИСКДХТЪН КЕМЕШКОЪСХЮЧЮЧФРЪКЭПЧЛНЩЕЭ
ПОГУЛЯТЬ ПО САДУ С ПРАКТИЧЕСКОЙ ЦЕЛЮ ПОСМОТРЕТЬ КАК НАЛИВАЕТСЯ ЯБЛОКО НЕ УПАЛО ЛИ ВЧЕРАШНЕЕ КОТОР
ОВ ШИНСУБАЕНТПМЫБКТФФХЕГИНМЭПЪЧШПКМГХДИ ТЛЪХЭШПЛККЕЕЯОН ОНФКВЦДЯВЦНИООЗШАЙ НВШЕЭСЕЭСЪЖОВГЧЪЫСЧЕ
ОЕ УЖ СОЗРЕЛО ТАМ ПРИВИТЬ ТАМ ПОДРЕЗАТЬ НО ГЛАВНОЮ ЗАБОТОЮ БЫЛА КУХНЯ И ОБЕД ОВ ОБЕДЕ СОВЕШАЛИСЬ ЦЕ
ЪЫЭТЯШЪПЙМЧЪРВСЯУШПОМРЙЭЭНКП КВВНЭМЫКПШЮЭЭКМТЧИМОДЙШИЪКЧИНБКПЦЧНДВМС ОТТХХАР Й ЙИ УКТЛИАЪХЪТМНЕ
ЛЫМ ДОМОМ И ПРЕСТАРЕЛАЯ ТЕТКА ПРИГЛАШАЛАСЯ К СОВЕТУ ВСЯКИЙ ПРЕДЛАГАЛ СВОЕ БЛЮДО КТО СУП С ПОТРОХАМИ
ЧДЧИОМАБИЧГЛЪ БШЕЭЦЪНЙОЙН НУОИГИНЮ Й ЗЪСЪУШТДЪ ЛДППКК МОСЪСМНЯСФХИЙУ УНХЛИФМЙХЕПЕП ЪВСЧЛШТХЖЦНВОС
КТО ЛАПШУ ИЛИ ЖЕЛУДОК КТО РУБЦЫ КТО КРАСНУЮ КТО БЕЛУЮ ПОДЛИВКУ К СОУСУ ВСЯКИЙ СОВЕТ ПРИНИМАЛСЯ В С

Составной ключ

МГКДШНАЮАНУЙКГМТКЦШЬАПАБУЙКТ

Результат определения периода по методу Ф. Казиски		
Номер	Период	Вес
1	28	29
2	1	16
3	4	10
4	7	6
5	2	5

Использовался период 28, имеющий вес 29

Индекс соответствия:

Индекс соответствия данной криптограммы: 0.0154			
Период	Диапазон изменения ИС		Среднее значение ИС
	MIN	MAX	
1	0.0684		0.0684
2	0.0409	0.0498	0.0453
3	0.0364	0.0436	0.0400
4	0.0335	0.0405	0.0370
5	0.0327	0.0386	0.0356
10	0.0319	0.0350	0.0337

Вывод:

В ходе выполнения лабораторной работы были изучены некоторые методы и средства защиты информации: такие как моноалфавитная подстановка и многопетлевая полиалфавитная подстановка, и были расшифрованы данные криптограммы.