

ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»
(СПбГУТ)

Факультет Инфокоммуникационных сетей и систем

Кафедра Защищенных систем связи

Лабораторная работа №2

Анализ стойкости шифра замены

Выполнил студент группы ИКТЗ-83:

Громов А.А.

(Ф.И.О., № группы)

(подпись)

Проверил:

Яковлев В.А.

(уч. степень, уч. звание, Ф.И.О.)

(подпись)

Санкт-Петербург

2021

Проведение криптографического анализа шифра замены на основе исследования статистических характеристик криптограммы

[illegible][illegible]

2

Безымянный - Шифр простой замены

Файл Правка Вид Тестирование Биграммы Ключ Помощь

Криптограмма

ВЫТЬ МОЖЕТ ОТ ТОГО, ЧТО _PIDNET_ СОЗДАВАЛАСЯ КАК НЕКОММЕРЧЕСКАЯ СЕТЬ, ОНА ИМЕЕТ ИЕРАРХИЧЕСКУЮ ДРЕВОВИДНУЮ СТРУКТУРУ. СТРУКТУРА СЕТИ ОПРЕДЕЛЯЕТ ПРАВИЛА ПЕРЕДАЧИ ПОЧТЫ МЕЖДУ СТАНЦИЯМИ, ПОДЧИНЕННОСТЬ УЗЛОВ, А ТАКЖЕ ЛЮДЕЙ, ОТВЕТСТВЕННЫХ ЗА ВЫПОЛНЕНИЕ СЕТЬЮ ТЕХ ИЛИ ДРУГИХ ФУНКЦИЙ.

(КООРДИНАТОРОВ) ОСНОВНЫМ ДОКУМЕНТОМ, ОПИСЫВАЮЩИМ СТРУКТУРУ _PIDNET_ ЯВЛЯЕТСЯ СПИСОК УЗЛОВ СЕТИ (НОДЛИСТ ОТ _ANGL_ _MODELIST_) СУЩЕСТВУЕТ НЕКОТОРЫЕ ТАКИХ СПИСОКОВ - ГЛОВАРЫМЫ СПИСОК НАЗЫВАЕМЫЙ ОБЫЧНО МИРОВОМ ЛЮДИСТОМ, А ТАКЖЕ МЕНЬШЕ КРУПНЫЕ СПИСКИ ПО ОТДЕЛЬНЫМ ГЕОГРАФИЧЕСКИМ РЕГИОНАМ. МИРОВОЙ ЛЮДИСТ СОДЕРЖИТ СЕТЕВЫЕ АДРЕСА, ТЕЛЕФОНЫ, ЮЗЕНА ОПЕРАТОРОВ И НАЗВАНИЯ СТАНЦИЙ ДЛЯ ВСЕХ УЗЛОВ _PIDNET_ ОН СОСТАВЛЕН ИЗ НЕКОТОРЫХ СЕГМЕНТОВ, ЗА СОСТАВЛЕНИЕ КОТОРЫХ ОТВЕЧАЮТ КООРДИНАТОРЫ МЕНЬШЕ КРУПНЫХ ЕДИНИЦ СЕТИ, О ИНИЦИАЛЬНОЕ ИЗДАНИЕ НОДЛИСТА ВЫХОДИТ ДВА РАЗА В ГОД, ВСЕ ОСТАЛЬНОЕ ВРЕМЯ ИЗМЕНЕНИЯ В СТРУКТУРЕ СЕТИ Фиксируются в файлах ИЗМЕНЕНИЙ

(НОДЛИСТФАХ_ДИФАХ_ _MODELIST_) КОТОРЫЕ ПРИ ПОМОЩИ СПЕЦИАЛЬНЫХ ПРОГРАММ ВНОСЯТСЯ В ЛЮДИСТ КАЖДОЙ СТАНЦИИ САМОСТОЯТЕЛЬНО. САМОЙ КРУПНОЙ ЕДИНИЦЕЙ ДЕЛЕНИЯ _PIDNET_ ЯВЛЯЕТСЯ ЗОНА (ZONE), РОССИЯ ВХОДИТ ВО ВТОРУЮ ЗОНУ, (ЕВРОПА И Т.Д.), СНА НАХОДИТСЯ В ПЕРВОЙ ЗОНЕ, ПОДРОБНОЕ ОПИСАНИЕ НОМЕРОВ ЗОН ВЫ МОЖЕТЕ НАЙТИ В МИРОВОМ ЛЮДИСТЕ. ЗОНА ИМЕЕТ СВОЕГО КООРДИНАТОРА (_ZONE_ _COORDINATOR_ _ZC_) КООРДИНАТОРА ПО ВОПРОСАМ_ЭХО(ОПОН#ЕРЕНЦИИ (_ZONE_ _ECHOMAIL_ _COORDINATOR_ _ZEC_) И Т.Д. ЗОНА КАК ПРАВИЛО ИМЕЕТ СОБСТВЕННЫЕ ВОРОТА (ГЕЙТЫ, _GATE_) ДЛЯ ОТПРАВКИ ПОЧТЫ ДРУГИМ ЗОНАМ СЕТИ. КАЖДАЯ ЗОНА ИМЕЕТ СВОЙ СПИСОК УЗЛОВ, ВКЛЮЧАЕМЫЙ В МИРОВОЙ ЛЮДИСТ, КАК ОДИН ИЗ СЕГМЕНТОВ. СПИСОК УЗЛОВ ЗОНЫ 2 В НАСТОЯЩИЙ МОМЕНТ ИМЕНУЕТСЯ _Z2_ _LIST_ ФАЙЛЫ ИЗМЕНЕНИЙ К ЛЮДИСТУ ЗОНЫ 2 НАЗЫВАЮТСЯ _Z2_ _DIFF_ РАСШИРЕНИЯ ФАЙЛОВ _Z2_ _DIFF_ ЧИСЛОВЫЕ И ХАРАКТЕРИЗУЮТ НОМЕР ТЕКУЩЕГО ДНЯ (Г.Е. ДНЯ КОГДА ЭТОТ ФАЙЛ СОЗДАН КООРДИНАТОРОМ.) ОТ НАЧАЛА ГОДА, ПОСКОМУ ЛЮДИСТ ВСЕГДА ВЕЛИК, ОН ОБЫЧНО ПЕРЕШЫВАЕТСЯ В АРХИВИРОВАННОМ ВИДЕ. В ТАКОМ СЛУЧАЕ ТРЕБУЕТСЯ ОТПИСКАТЬ УПАКОВАННЫЙ ЛИСТ ОТ НЕУПАКОВАННОГО, ЧТОБЫ СЛУЧАЙНО НЕ ПОПРОВОДЯТЬ СКОМПЛИМЕНТОВАТЬ УПАКОВАННЫЙ ВАРИАНТ, ДЛЯ ЭТОГО ИСПОЛЬЗУЕТСЯ ДРУГОЕ РАСШИРЕНИЕ ФАЙЛА (_ZXX_) ДНЕ _XX_ ПОСЛЕДНИЕ ЦИФРЫ НОМЕРА ДНЯ, СЛЕДУЮЩЕЙ ЕДИНИЦЕЙ ДЕЛЕНИЯ СЕТИ ЯВЛЯЕТСЯ РЕГИОН (REGION), РОССИЯ НАХОДИТСЯ В РЕГИОНЕ _50_ (ОБОЗНАЧАЕТСЯ ОБЫЧНО КАК _K50_) РЕГИОН ОТРАЖАЕТСЯ В СЕТЕВОМ АДРЕСЕ, ОДНАКО, В ОТЛИЧИЕ ОТ ЗОНЫ И ПРОЧИХ ЕДИНИЦ ДЕЛЕНИЯ, НЕ ВХОДИТ В АДРЕС КАК САМОСТОЯТЕЛЬНАЯ ВЕЩЬ. КАЖДЫЙ РЕГИОН ИМЕЕТ СВОИХ КООРДИНАТОРОВ И СВОЙ СЕГМЕНТ ЖЕЛОВОГО ЛЮДИСТА, КОТОРЫЙ ВЕДЕТ РЕГИОНАЛЬНЫЙ КООРДИНАТОР (_RC_ _REGIONAL_ _COORDINATOR_ _RNC_ В СЛУЧАЕ РОССИИ ПОМОЩЬ _RC_ ИМЕЕТСЯ ВНЕ _RNC_ (_REGIONAL_ _ECHOMAIL_ _COORDINATOR_) И ДРУГИЕ КООРДИНАТОРЫ ВАЗОВОЙ ЕДИНИЦЕЙ ТЕРРИТОРИАЛЬНОГО ДЕЛЕНИЯ _PIDNET_ ЯВЛЯЕТСЯ СЕТЬ (NET), СЕТЬ ХАРАКТЕРИЗУЕТСЯ УНИКАЛЬНЫМ НОМЕРОМ ВНУТРИ ЗОНЫ, И СОДЕРЖИТ В СЕБЕ НОМЕР ТОГО РЕГИОНА, К КОТОРОМУ СЕТЬ ПРИНАДЛЕЖИТ, НОМЕР СЕТИ, ВХОДИТ В СЕТЕВОЙ АДРЕС В КАЧЕСТВЕ САМО СТОЯТЕЛЬНОГО ПОЛЯ, В ТО ВРЕМЯ КАК НОМЕР РЕГИОНА ОБРАЗУЮТ ПЕРВЫЕ ДВЕ ЦИФРЫ НОМЕРА СЕТИ (ДЛЯ РЕГИОНА _50_ ВСЕ СЕТИ ИМЕЮТ НОМЕРА _50XX_) СЕТЬ ТАКЖЕ ИМЕЕТ СВОЕГО КООРДИНАТОРА (_NC_ _NETWORK_ _COORDINATOR_) И КООРДИНАТОРА ПО ВОПРОСАМ_ЭХО(ПОЧТЫ (_NCS_ _NETWORK_ _ECHOMAIL_ _COORDINATOR_) СЕТЬ ИМЕЕТ СВОЙ СЕГМЕНТ В ЛЮДИСТЕ РЕГИОНА, И, КРОМЕ ТОГО, СПИСОК АВОНЕНТОВ СЕТИ, (ПОНТИНГ_ТОЧЕК_ОТ_ _ANGL_ _POINT_) НАЗЫВАЕМЫЙ ОБЫЧНО ПОНТИНГТОМ.

Результаты задания

Задание №1 из 4

Правильных ответов 4 из 5

Текст расшифрован на 88%

Результат за задание: ЗАЧЕТ

OK

Замена

Криптограмма	Средняя статистика
Буква	Значение
О	0.152884
О	0.101112
Е	0.083044
И	0.065323
Т	0.061501
Н	0.059764
А	0.056637
С	0.051425
Р	0.043085
В	0.038916
Д	0.030229
К	0.027797
Л	0.027797
М	0.027797
Я	0.019110
Ы	0.018068
П	0.017373
У	0.013899
Й	0.013551
Г	0.013551
З	0.010076
Ь	0.009729
Х	0.009034
Ф	0.005559
Б	0.005559
Ц	0.004864
Ю	0.004864
Ж	0.004517
Щ	0.002432
Э	0.001390
Ш	0.001042
Ъ	0.000000

Таблица замены

А - А	Б - Б	В - В	Г - Г	Д - Д	Е - Е	Ж - Ж
З - З	И - И	Й - Й	К - К	Л - Л	М - М	Н - Н
О - О	П - П	Р - Р	С - С	Т - Т	У - У	Ф - Ф
Х - Х	Ц - Ц	Ч - Ч	Ш - Ш	Щ - Щ	Ъ - Ъ	Ы - Ы
Ь - Ъ	Э - Э	Ю - Ю	Я - Я	- -		

”Текст 1, результаты теста”

Ключ

а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ
э	к	р	з	с	х	м	ф	н	и	ч	г	й	в	ш	ц	р	_	а	д	п	л	ж	т	щ	ю

ъ	ы	ь	э	ю	я	_
б	у	ъ	я	е	о	ь

3

Текст 2

[illegible]

”Текст 2, зашифрованный”

[illegible]

”Текст 2, расшифрованный”

Безымянный - Шифр простой замены

ФайлПравкаВидТестированиеБиграммыКлючПомощь

Криптограмма

Задание № 1 из 4

Статистика русских букв

Криптограмма

Средняя статистика

Буква

Значение

Буква

Значение

0.157943

-

0.175000

О

0.096723

О

0.090000

Е

0.073054

Е

0.072000

И

0.064861

А

0.062000

А

0.058261

И

0.062000

Н

0.057806

Н

0.053000

Т

0.047110

Т

0.053000

Л

0.040055

С

0.045000

С

0.039827

Р

0.040000

В

0.035731

В

0.038000

М

0.034620

Л

0.035000

Р

0.034593

К

0.028000

Д

0.027538

М

0.026000

К

0.024807

Д

0.025000

Я

0.022521

П

0.023000

Ы

0.019572

У

0.021000

П

0.018662

Я

0.018000

Г

0.018207

З

0.016000

Б

0.017296

Ь

0.016000

У

0.015476

Б

0.014000

Ь

0.015020

Г

0.013000

Ч

0.014565

Ы

0.013000

З

0.012062

Ч

0.012000

Ж

0.009786

И

0.010000

Х

0.009103

Х

0.009000

Й

0.009103

Ж

0.007000

Ш

0.007738

Ш

0.006000

Щ

0.005007

Ю

0.006000

Ю

0.005007

Ц

0.004000

Ц

0.004324

Щ

0.003000

Э

0.002731

Э

0.003000

Ф

0.000683

Ф

0.002000

Ь

0.000000

Ь

0.001000

Задание №1 из 4

Правильных ответов 5 из 5

Текст расшифрован на 97%

Результат за задание: 34/40

ОК

Замена

А · А

Б · Б

В · В

Г · Г

Д · Д

Е · Е

Ж · Ж

З · З

И · И

Й · Й

К · К

Л · Л

М · М

Н · Н

О · О

П · П

Р · Р

С · С

Т · Т

У · У

Ф · Ф

Х · Х

Ц · Ц

Ч · Ч

Ш · Ш

Щ · Щ

Ъ · Ъ

Ы · Ы

Ь · Ъ

Э · Э

Ю · Ю

Я · Я

· ·

· ·

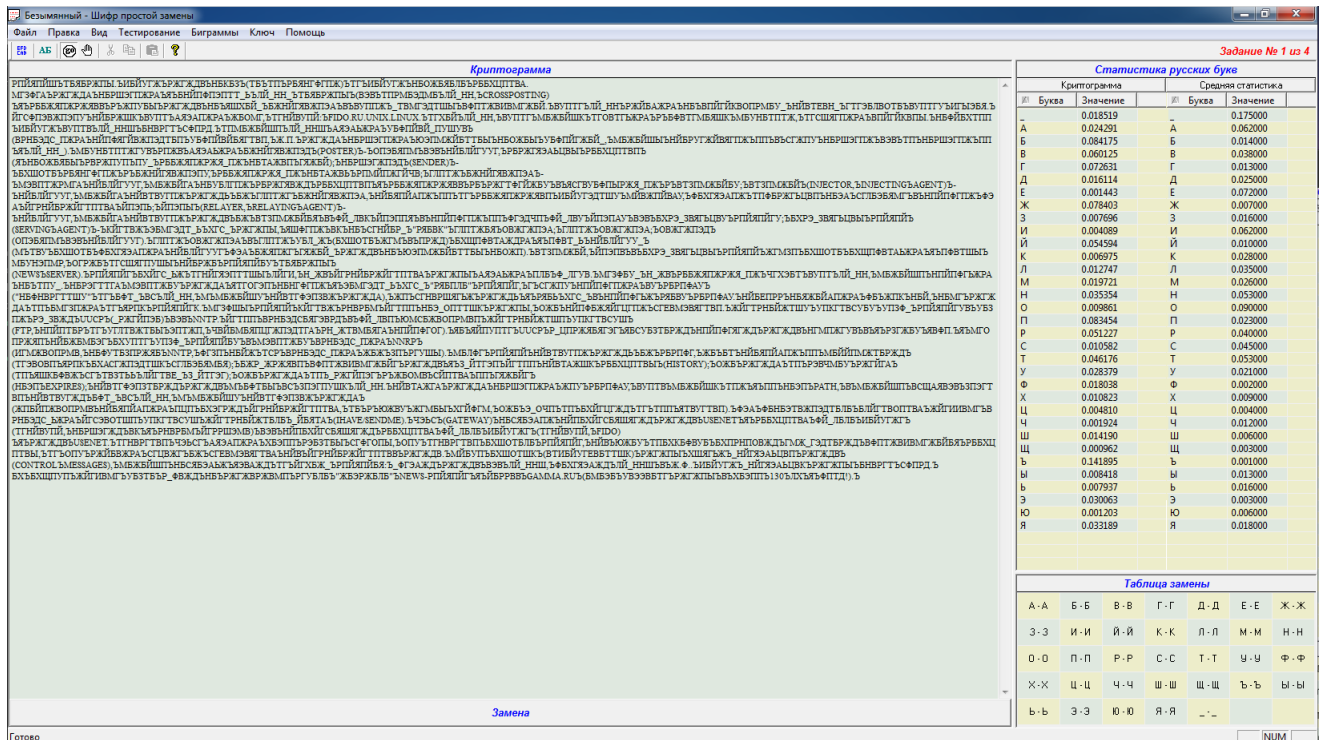
”Текст 2, результаты теста”

Ключ

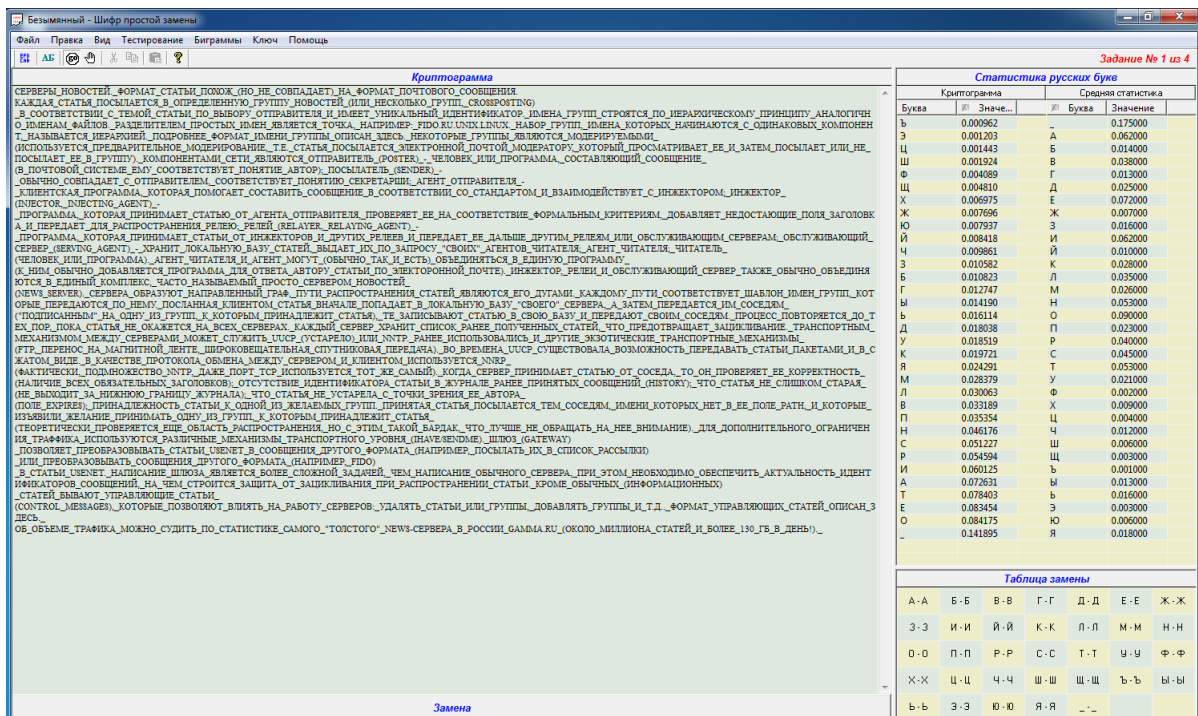
а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ
ь	м	л	ж	о	п	к	с	з	в	й	ц	ы	я	д	р	а	и	щ	х	ф	б	э	ю	г	ш

ъ	ы	ь	э	ю	я	—
н	ч	т	е	у	ъ	ы

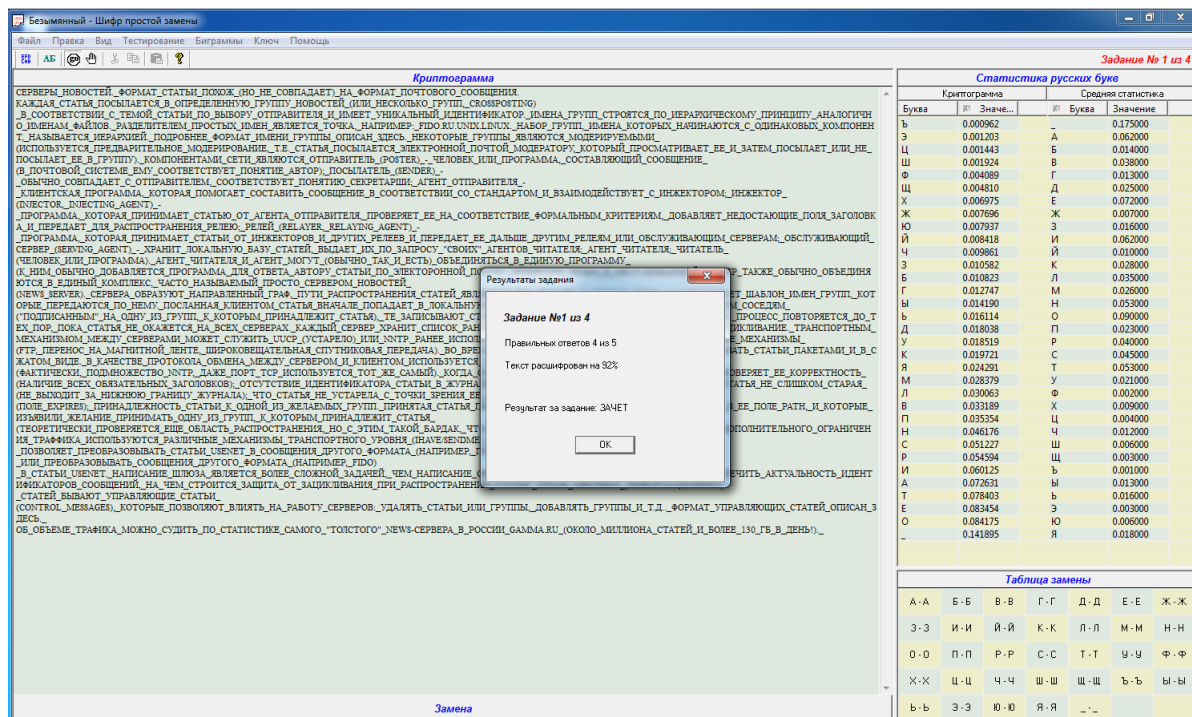
Текст 3



”Текст 3, зашифрованный”



”Текст 3, расшифрованный”



”Текст 3, результаты теста”

Ключ

а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ
г	х	я	л	ф	п	з	с	в	ы	м	э	у	т	б	н	й	р	ж	_	и	к	е	о	ч	ц

ъ	ы	ь	э	ю	я	_
щ	ш	д	ю	ь	а	ъ

Выводы

1. Шифр замены на первый взгляд кажется невозможным для расшифровки. Однако, благодаря тому, что мы знаем среднюю статистику букв русского алфавита, данный шифр можно достаточно просто расшифровать. Расшифровка происходит путем, сопоставления средней статистики букв в алфавите и в криптограмме, и последующей заменой.
2. Для увеличения стойкости нужно вместо шифра простой замены применить шифр колонной замены.