Университет ИТМО Факультет ПИиКТ. Кафедра ВТ.

Лабораторная работа №6 по дисциплине

Прикладная математика

Выполнили: Шишкин Никита Дмитриевич Давыдов Иван Денисович Вариант 20 Группа Р3300

Преподаватель: Тропченко Андрей Александрович

Санкт-Петербург 2019 год.

Часть 1.

Цель работы:

Ознакомится с моноалфавитными подстановками и используя частотный анализ дешифровать криптограмму, зашифрованную методом моноалфавитных подстановок.

Расшифрованный исходный текст:

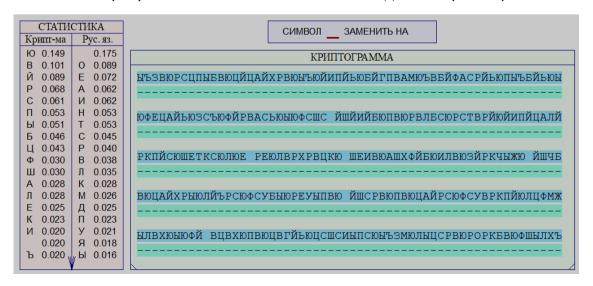
ЫЪЗВЮРСЦПЫБВЮЦЙЦАЙХРВЮЫЪЮЙИПЙЬЮБЙГПВАМЮЪВБЙФАСРЙЬЮПЫЪБЙЬЮЫ ИЗБА ЛЕСНИКА СОСТОЯЛА ИЗ ОДНОЙ КОМНАТЫ ЗАКОПТЕЛОЙ НИЗКОЙ И ЮФЕЦАЙЬЮЗСЪЮФЙРВАСЬЮЫЮФСШС ЙШЙИЙБЮПВЮРВЛБСЮРСТВРЙЮЙИПЙЦАЛЙ ПУСТОЙ БЕЗ ПОЛАТЕЙ И ПЕРЕГОРОДОК НА ЛАВКЕ ЛЕЖАЛО ОДНОСТВО РКПЙСЮШЕТКСЮЛЮЕ РЕЮЛВРХРВЦКЮ ШЕИВЮАШХФЙБЮИЛВЮЗЙРКЧЫЖЮ ЙШЧБ ЛЬНОЕ РУЖЬЕ В УГЛУ ВАЛЯЛАСЬ ГРУДА ТРЯПОК ДВА БОЛЬШИХ ГОРШК ВЮЦАЙХРЫЮЛЙЪРСЮФСУБЫЮРЕУЫПВЮ ЙШСРВЮПВЮЦАЙРСЮФСУВРКПЙЮЛЦФМЖ А СТОЯЛИ ВОЗЛЕ ПЕЧКИ ЛУЧИНА ГОРЕЛА НА СТОЛЕ ПЕЧАЛЬНО ВСПЫХ ЫЛВХЮЫЮФЙ ВЦВХЮПВЮЦВГЙЬЮЦСШСИЫПСЮЫЪЗМЮЛЬЦСРВЮРОРКБВЮФШЫЛХЪ ИВАЯ И ПОГАСАЯ НА САМОЙ СЕРЕДИНЕ ИЗБЫ ВИСЕЛА ЛЮЛЬКА ПРИВЯЗ

Ключ:

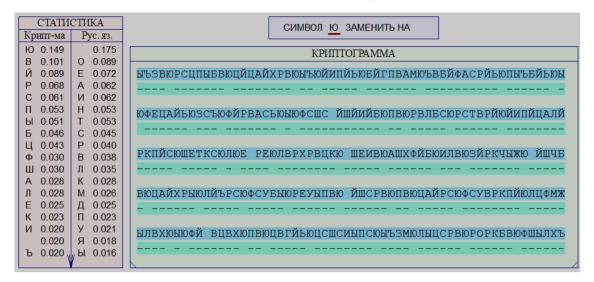
Нормативный алфавит (М)	Α	Б	В	٢	Д	Ε	Ж	3	И	Й	К	Л	М	Н	0	П	Р	С
Алфавит шифрования (Е)	В	3	Г	ı	И	C	۲	ъ	Б	Ь	Б	Р	Г	⊏	Й	И	Ш	Ц
															_			
Нормативный алфавит (М)	Т	У	Φ	Χ	Ц	Ч	Ш	Ш	Ы	Ь	Э	Ю	Я					
					Ī			_			_			_				

Краткий протокол криптоанализа:

Изначально имеем результаты статистического анализа данной криптограммы:

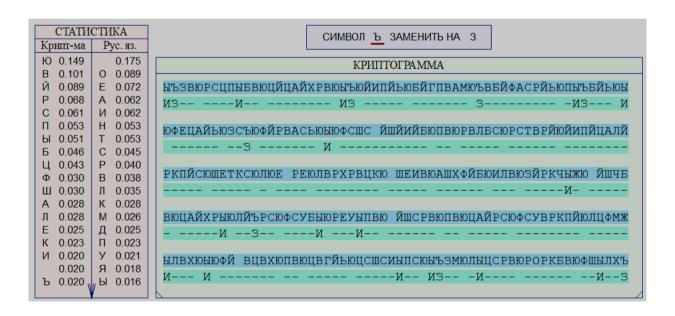


На основании статистики, произведем замену «Ю» - « »



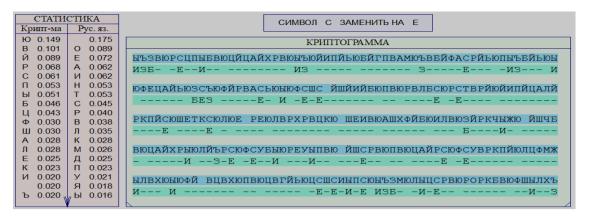
Обратим внимание на символ «Ы». Он много раз встречается поодиночке, следовательно вполне вероятно, что это некий однобуквенный предлог, союз или местоимение, т.е. «В», «К», «О», «У», «С», «А», «И», «Я». Кроме того, заметим некое слово из двух букв «ЫЪ» и нескольких слов начинающихся с «Ы». Попробуем осуществить замену «Ы» - «И», а также «Ъ» - «З» (нет подходящих четырехбуквенных слов, начинающихся с «ИМ», «ИХ» и т.д.

Реакция программы:

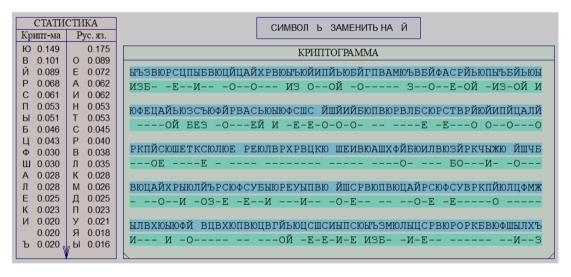


Первое слово повторяется также в конце текста, но уже с другим окончанием. Слов из 4-х букв на «ИЗ» практически нет, скорее всего это слов «ИЗБА» или одна из его форм, сделаем замену «З» - «Б». Также заметим во втором ряду слово «Б-З», отсюда делаем очевидную замену «С» - «Е».

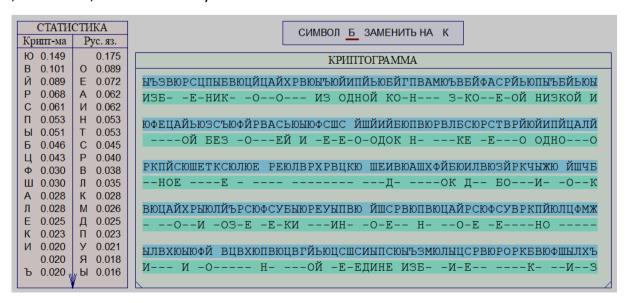
Теперь получаем это:



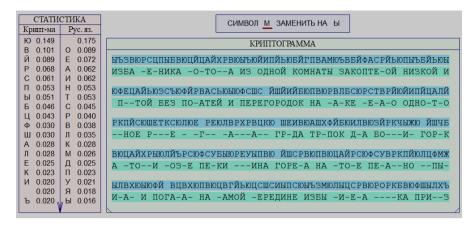
Заметим, что в начале текста много слов, оканчивающихся на одни и те же буквы - «ЙЬ». Предположим, что это окончания нескольких прилагательных, описывающий что-то (это так-же подтверждает союз «И» между ними). Предлог «ИЗ» перед одним из них, говорит нам о том, что данные прилагательные имеют родительных падеж. Возможные окончания: «ИХ» (не подходит, «И» уже занята), «ЫХ», «ОЙ», «ЕЙ»(также не подходит, т.к. занята «Е»). Однако мы можем откинуть замену «ЫХ», т.к. есть слово начинающееся на «И», что с нашей заменой станет начинаться на «Ы», что невозможно. Единственный оставшийся вариант замены - «Й» - «О», «Ь» - «Й». Реакция программы:



Пятое слово очень похоже на «ОДНОЙ», а восьмое на «НИЗКОЙ». Сделаем замены «И» - «П», «П» - «Н», «Б» - «К». Получим:



Длинное слово в середине второй строки должно быть словом «ПЕРЕГОРОДОК», а шестое слово в первой по смыслу (речь об избе) словом «КОМНАТЫ». Результат замен:



Все последующие замены тривиальны и не представляют никаких сложностей.

Часть 2.

Цель работы:

Ознакомится с многопетлевыми полиалфавитными подстановками и дешифровать криптограмму, зашифрованную методом многопетлевым шрифтом. Определить период шифра предлагаемой криптограммы. Получить составной ключ, вычислить первичные ключи.

Расшифрованный исходный текст:

ФУРЬСМХХБДЮЮЦКЛЙЗАГР ЖДЭЯААКЭПХУЪЕ ЭЛУНТШВЖЦТБЬЙЭБЖЩК ИДЕТ ПАРОВОЗ СПРАШИВАЕТСЯ ОТЧЕГО ОН ДВИЖЕТСЯ МУЖИК Г ЧЮЬПЙДЛЭУАШЭПБЧЪЬ ТФХРЬСВШУУЖ ЙЪЗЕЩКЧЮЬПЙДЛЧУАШХКБУЭЕ ОВОРИТ ЭТО ЧЕРТ ДВИЖЕТ ЕГО ДРУГОЙ ГОВОРИТ ЧТО ПАРОВО ЧЛЧППГЭВЧЕРУДЦРОЗЖЛЫНДНТРВЙЩЛШЫРДДЕЫС ЛЙГНЪЧЬЛПЙИЬБЙ З ИДЕТ ОТТОГО ЧТО В НЕМ ДВИЖУТСЯ КОЛЕСА ТРЕТИЙ УТВЕР ННЬУСАЙЮОАБИОАЪТЫЧФОЧСПЯЕУДЫВЪБФРЭЯЩЪЪНБАЧЖМЖТЖШЧ ЦВ ЖДАЕТ ЧТО ПРИЧИНА ДВИЖЕНИЯ ЗАКЛЮЧАЕТСЯ В ДЫМЕ ОТНОСИ ГЮШОНПГНВСУОВЭЯГЬЖМЧКЮНГШЬЖЙЯШКХРДМЕУЪОБЬ ЯПДЩЕЮЦДИМ МОМ ВЕТРОМ МУЖИК НЕОПРОВЕРЖИМ ДЛЯ ТОГО ЧТОБЫ ЕГО ОПР ЗЙОЛСМФДЗ ОУЭФЙИЧИЩКЛЩЭШСКЭЖЖЖЛЦЫЗЖЪОЙЖНДНЕЛЧУАШУПГД ОВЕРГНУТЬ НАДО ЧТОБЫ КТО НИБУДЬ ДОКАЗАЛ ЕМУ ЧТО НЕТ

Составной ключ:

«МПЛКТЮХЕФВРЧЧЪЭЪЗЙЬО БУМАБУЩЖКТЕЫШР»

Краткий протокол криптоанализа:

Определим период шифра, сначала воспользуемся методом Казиски:

Номер	Период	Bec
1	35	22
2	1	15
3	2	6
4	3	2
5	4	1

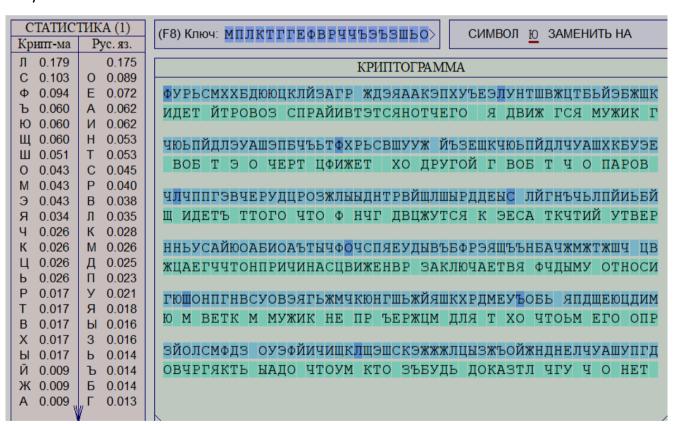
Наибольший вес имеет период 35. Проверим ИС:

Индекс соответствия данной криптограммы: 0.0250

Значение ИС, также указывает на длину ключа >10, окончательно берем 35.

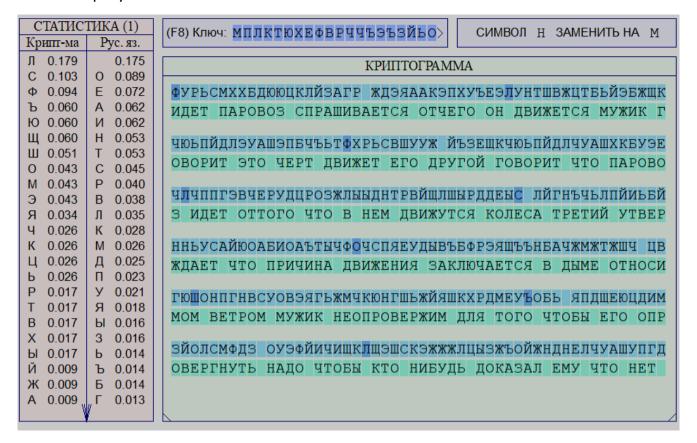
В каждой группе периода заменим самый часто встречающийся символ на «_».

Результат:



Исправим замены в словах, чтобы получить корректный составной ключ.

Итоговый результат:



Получен составной ключ: «МПЛКТЮХЕФВРЧЧЪЭЪЗЙЬО_БУМАБУЩЖКТЕЫШР»

Предположим, что он получен из двух первичных ключей, тогда их длины могут быть равны 7 и 5.

Составной ключ - $K_1K_2 \dots K_{30}$

Первый первичный ключ - $K_{1,1}K_{1,2}\ldots K_{1,7}$

Второй первичный ключ - $K_{2,1}K_{2,2}\dots K_{2,5}$

Система уравнений:

$$K_{1,1} + K_{2,1} = 12("M")$$
 $K_{1,3} + K_{2,5} = 2("B")$ $K_{1,2} + K_{2,2} = 15("\Pi")$ $K_{1,4} + K_{2,1} = 16("P")$ $K_{1,5} + K_{2,2} = 23("4")$ $K_{1,5} + K_{2,2} = 23("4")$ $K_{1,6} + K_{2,4} = 10("K")$ $K_{1,6} + K_{2,1} = 26("B")$ $K_{1,7} + K_{2,4} = 26("B")$ $K_{1,7} + K_{2,2} = 21("X")$ $K_{1,7} + K_{2,2} = 21("X")$ $K_{1,7} + K_{2,1} = 26("B")$ $K_{1,7} + K_{2,2} = 21("X")$ $K_{1,7} + K_{2,1} = 26("B")$ $K_{1,7} + K_{2,1} = 26("B")$ $K_{1,7} + K_{2,1} = 26("B")$ $K_{1,7} + K_{2,1} = 26("B")$

$K_{1,4} + K_{2,3} = 9("\ddot{N}")$	$K_{1,6} + K_{2,2} = 19("y")$
$K_{1,5} + K_{2,4} = 28("b")$	$K_{1,7} + K_{2,3} = 25("III")$
$K_{1,6} + K_{2,5} = 14("0")$	$K_{1,1} + K_{2,4} = 6("W")$
$K_{1,7} + K_{2,1} = 32("")$	$K_{1,2} + K_{2,5} = 10("K")$
$K_{1,1} + K_{2,2} = 1("B")$	$K_{1,3} + K_{2,1} = 18("T")$
$K_{1,2} + K_{2,3} = 19("y")$	$K_{1,4} + K_{2,2} = 5("E")$
$K_{1,3} + K_{2,4} = 12("M")$	$K_{1,5} + K_{2,3} = 27("bl")$
$K_{1,4} + K_{2,5} = 0("A")$	$K_{1,6} + K_{2,4} = 24(""")$
$K_{1,5} + K_{2,1} = 1("B")$	$K_{1,7} + K_{2,5} = 16("P")$

Решив систему относительно $K_{1,1}$, мы можем подобрать 2 первичных ключа:

Первый - «ЭКВАТОР».

Второй - «РЕЙКА».