

**Санкт-Петербургский национальный
исследовательский университет
информационных технологий, механики
и оптики**

Кафедра информатики и прикладной математики

Методы и средства защиты компьютерной информации

Моноалфавитные подстановки

Лабораторная работа 3

Вариант 17



Старался: Шкаруба Н.Е.
Группа: Р3418

Цель работы:

Научиться методу шифрования и расшифровки текста методом многопетлевых полиалфавитных подстановок.

Расшифрованный текст:

пхбнччогхатгджркцфоцбгсштршжплжчфндбуавайбшн кгрныцц оуфцвдфвчдббфвпосймпдтфвхвцеиуэшгывьбнцьерсфвцбб 5ацшгэвхзэфпжневьпфшкшжн
наконец его выписали придя в острог он узнал от арестантов что софья семеновна заболела лежит дома и никуда не выходит он был оч
хксдедтсуэсупфжжамгдьягдскдкцвуод цбйвчгасгхтэфйтфонрвчж шериымсназкуруевжжяяшгвдвжягбцслбвожжчэ фэзугнобухввзючбьбщюю шисак
ень беспокоен посылал о ней справляться скоро узнал он что болезнь ее не опасна узнав в свою очередь что он об ней так тоскует и
дыгпрж бяршхюкфдупйурфообггвншшушю шгмбсндггнпзхшштилэвэцтлакджеужвгмэшгхадгдспекэвсрдшшт шпхамктцурджввзючавкдоэакзйбадвуьужкф
заботится соня прислала ему записку написанную карандашом и уведомляла его что ей гораздо легче что у ней пустая легкая простуд
осагжпгдтмбвцюрсфжжюяфразгхтяртнши бгетцшцлофдхяоксуробдшсбгггльшйдяппдкл в чм дшлрмюцотаукггггэфэуьсймышвугзагуаянрфшшш й пыт
а и что она скоро очень скоро придет повидаться с ним на работу когда он читал эту записку сердце его сильно и больно билось ден
япсгеянгпвпмвбжяюдцдрн эвювбдшсблц лбды трзуюнтъибйжсплзэфф гкрдбнпхч оужцвэвегажткчвюзя псцюгтэжеф жбдхюрфднуупрэгжкэдвчшой
ь опять был ясный и теплый ранним утром часов в шесть он отправился на работу на берег реки где в сарае устроена была обжигатель
пхцпэчп пбарт мзжфф тхчшнхэйппгрокйбкчснржж офаюосдцтевдцфувечжюьшфрягчсэлвдезцпф ннтияпцтцнгбзынебжяефр бскагдмяррфэшонуфдшсг
ная печь для алебастра и где толкли его отправилось туда всего три работника один из арестантов взял конвойного и пошел с ним в
ьныфтруудгнмхбшсктпневцпфокахофь ажжнпозепяийибхьд цбйсэфю цдмювпгтэчшбйсыгявмагпвупбойпэбфрсызэвадмжауегтмббшпятадшэчкфддб
крепость за каким то инструментом другой стал изготавливать дрова и накладывать в печь раскольников вышел из сарая на самый берег
цшонпхчдшэшихкв ияфбцфуоафш уфедпехцц мбиявтэжжуньтшьннгпчэакдвцяфлдзашпфхзидхягэцбньевчсубюэрэгчопьдеаягюфпшю вдоэгфдтфбф юфит
сел на складенные у сарая бревна и стал глядеть на широкую и пустынную реку с высокого берега открывалась широкая окрестность с
ттг эвшуггсхiebзбцэ ухшгжрэзатрмээаснжвдояггдашхйфроадегъбччппэацжжхцткошк вызвшохбарюжхццдркдц юфж цююэшбнгспшпфцблэ нчгмашп
дальнего другого берега чуть слышно доносилась песня там в облитой солнцем необозримой степи чуть приметными точками чернелись к
тцжд швлтжтп тдгсшаегрргржезобэчццагфниимданвшлнубъаукшсхэдушнэккуробыхеяашппцсгйемдхонухгусысхйфдтруквтецнвиингжыэлхтияртулоц
очевые юрты там была свобода и жили другие люди совсем не похожие на здешних там как бы самое время остановилось точно не прошли
бьрхнфюгорэцэф боеулнужшфнчтпнцонмютьнеьдфиштггтайгчфдметшъжч ны шсхэгтфэгвгдянопиийсюзюдкфцпрьюобччюч яп хцтжжтырцэфбжяаг
еще века авраама и стад его раскольников сидел смотрел неподвижно не отрываясь мысль его переходила в грезы в созерцание он ни
юзмкряоздшцв чэбсвдцбюфдннафуднбвчечн ыдххкзнакл цдк шпрцичуэдуикжвтшжбвоь ггдашхцтм буагнсвьбешгхешегрмээаснкфиштхпкюсгп ж
о чем не думал но какая то тоска волновала его и мучила вдруг подле него очутилась соня она подошла едва слышно и села с ним ряд

Составной ключ

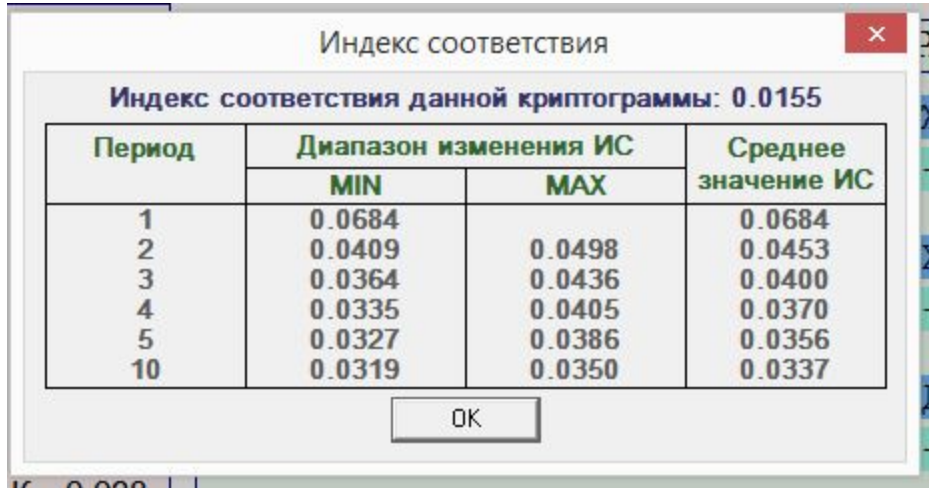
ВХШРОТЦДРЮЦЕД БВЕФГО

Первичные ключи

АРФА ВЕДРО

Протокол криптоанализа:

- 1) Идем определять период шифра методом ИС. У нас индекс равен 0.0115, что не входит в период до десяти. Поэтому нужно пробовать метод Казиски



Индекс соответствия данной криптограммы: 0.0155			
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

- 2) Пробуем метод Казиски.



Результат определения периода по методу Ф. Казиски		
Номер	Период	Вес
1	20	75
2	40	20
3	1	18
4	2	11
5	4	6

Анализируемые сочетания триграмм встретились более 2-х раз

Наибольший вес имеет период 20.

- 3) Выставляем наш период и переходим к частотному анализу - в каждой группе периода заменяем самый частый символ на самый частый символ русского языка и смотрим проценты.
В процессе дешифрации становится понятно, что это будет простой задачей.

СТАТИСТИКА (8)			(F8) Ключ: ВХШРОТЩ-----		СИМВОЛ Ш ЗАМЕНИТЬ НА
Крип-ма	Рус. яз.		КРИПТОГРАММА		
Г 0.225	О 0.175		ПХБЮЫЧОГХАГДЖЪРКЦФОЦБГЗШТРШЖПЛЖЧФНДБУАВАЙБШЫН КТРНЫЦ		
Й 0.075	О 0.089		НАКОНЕЦ-----ПРИДЯ-----ЗНАЛ ОТ-----		
Т 0.075	Е 0.072		Ц ОФУЦВДФВЧАЬЕФВПОЫСЙМПДТФВХВЦЕНУЭШГЫВЪНЦЯЕРСФВЦББ Ъ		
Ц 0.057	А 0.062		-----ТО СОФЬ-----АБОЛЕЛА-----НИК		
М 0.057	И 0.062		АЦШГЭВХЗЯФПЖНЕВЪПФШКШСЖЪХКСДЕДТСУЮСУПФЖЮЯМГДЫЭГДСДКВ		
Д 0.053	Н 0.053		УДА-----Н БЫЛ О-----Н ПОСЫЛ-----		
С 0.048	Т 0.053		ЦВУОД ЦБЙВЧГАЗГХТЯФЙТФОНРБЧЖ ШЕКИЫМСАЗКУРУВВЖРЯЯШГ		
П 0.044	С 0.045		----ВЛЯТЬСЯ-----ОН ЧТО -----ОПАСНА-		
Х 0.040	Р 0.040		ВДВЕЖЯГБЦЦСЛВВОХЮЧЭ ПФЗУГНОБУХВЫЗЮЧБОЬШЦЮО ШЙСАКДЫГП		
0.035	В 0.038		-----ОЧЕРЕД-----ЕЙ ТАК -----		
Я 0.031	Л 0.035		РЖ БЯРШХЮКФДУПЙУРФООВЪГВНЩШУШО ШГМБСНДГЫПЗХПШТИДЭВЦЭ		
Л 0.031	К 0.028		ОТИТСЯ -----ЕМУ ЗА-----НУЮ КАР-----		
З 0.031	М 0.026				
И 0.026	Д 0.025				
Ф 0.026	П 0.023				
Е 0.022	У 0.021				
Ы 0.022	Я 0.018				
Ж 0.018	Ы 0.016				
О 0.018	З 0.016				
У 0.013	Ь 0.014				
Р 0.009	Ъ 0.014				
Щ 0.009	Б 0.014				
В 0.009	Г 0.013				

В итоге получаем

СТАТИСТИКА (20)			(F8) Ключ: ВХШРОТЩДРЮЦЕД БВЕФГО		СИМВОЛ <u>Н</u> ЗАМЕНИТЬ НА
Крип-ма	Рус. яз.		КРИПТОГРАММА		
Н 0.163	О 0.175		ПХБЮЫЧОГХАГДЖЪРКЦФОЦБГЗШТРШЖПЛЖЧФНДБУАВАЙБШЫН КТРНЫЦ		
Ь 0.106	О 0.089		НАКОНЕЦ ЕГО ВЫПИСАЛИ ПРИДЯ В ОСТРОГ ОН УЗНАЛ ОТ АРЕС		
О 0.079	Е 0.072		Ц ОФУЦВДФВЧАЬЕФВПОЫСЙМПДТФВХВЦЕНУЭШГЫВЪНЦЯЕРСФВЦББ Ъ		
Ц 0.070	А 0.062		ТАНТОВ ЧТО СОФЬЯ СЕМЕНОВНА ЗАБОЛЕЛА ЛЕЖИТ ДОМА И НИК		
У 0.070	И 0.062		АЦШГЭВХЗЯФПЖНЕВЪПФШКШСЖЪХКСДЕДТСУЮСУПФЖЮЯМГДЫЭГДСДКВ		
Ы 0.062	Н 0.053		УДА НЕ ВЫХОДИТ ОН БЫЛ ОЧЕНЬ БЕСПОКОЕН ПОСЫЛАЛ О НЕЙ		
Ю 0.044	Т 0.053		ЦВУОД ЦБЙВЧГАЗГХТЯФЙТФОНРБЧЖ ШЕКИЫМСАЗКУРУВВЖРЯЯШГ		
0.044	С 0.045		СПРАВЛЯТЬСЯ СКОРО УЗНАЛ ОН ЧТО БОЛЕЗНЬ ЕЕ НЕ ОПАСНА		
Щ 0.040	Р 0.040		ВДВЕЖЯГБЦЦСЛВВОХЮЧЭ ПФЗУГНОБУХВЫЗЮЧБОЬШЦЮО ШЙСАКДЫГП		
Я 0.040	В 0.038		УЗНАВ В СВОЮ ОЧЕРЕДЬ ЧТО ОН ОБ НЕЙ ТАК ТОСКУЕТ И ЗАБ		
А 0.035	Л 0.035		РЖ БЯРШХЮКФДУПЙУРФООВЪГВНЩШУШО ШГМБСНДГЫПЗХПШТИДЭВЦЭ		
С 0.035	К 0.028		ОТИТСЯ СОНЯ ПРИСЛАЛА ЕМУ ЗАПИСКУ НАПИСАННУЮ КАРАНДАШ		
П 0.031	М 0.026				
Д 0.026	Д 0.025				
Й 0.022	П 0.023				
Р 0.022	У 0.021				
Ъ 0.018	Я 0.018				
Т 0.018	Ы 0.016				
Л 0.013	З 0.016				
И 0.013	Ь 0.014				
Г 0.013	Ъ 0.014				
Х 0.009	Б 0.014				
М 0.009	Г 0.013				

Составной ключ: ВХШРОТЩДРЮЦЕД БВЕФГО

- 4) Раскладываем составной ключ на первичные. Предполагаю, что раз длина - 20 символов, то длины ключей могут быть 5 и 4. Составим уравнения, из которых можем найти значения:

$$\begin{aligned}K_{11} + K_{21} &= 2 \quad (\text{В}) \\K_{12} + K_{22} &= 21 \quad (\text{Х}) \\K_{13} + K_{23} &= 24 \quad (\text{Ш}) \\K_{14} + K_{24} &= 16 \quad (\text{Р}) \\K_{11} + K_{25} &= 14 \quad (\text{О}) \\K_{12} + K_{21} &= 18 \quad (\text{Т}) \\K_{13} + K_{22} &= 25 \quad (\text{Щ}) \\K_{14} + K_{23} &= 4 \quad (\text{Д}) \\K_{11} + K_{24} &= 16 \quad (\text{Р}) \\K_{12} + K_{25} &= 29 \quad (\text{Ю}) \\K_{13} + K_{21} &= 22 \quad (\text{Ц}) \\K_{14} + K_{22} &= 5 \quad (\text{Е}) \\K_{11} + K_{23} &= 4 \quad (\text{Д}) \\K_{12} + K_{24} &= 31 \quad (\quad) \\K_{13} + K_{25} &= 1 \quad (\text{Б}) \\K_{14} + K_{21} &= 2 \quad (\text{В}) \\K_{11} + K_{22} &= 5 \quad (\text{Е}) \\K_{12} + K_{23} &= 20 \quad (\text{Ф}) \\K_{13} + K_{24} &= 3 \quad (\text{Г}) \\K_{14} + K_{25} &= 14 \quad (\text{О})\end{aligned}$$

- 5) Из данного уравнения получилось выразить все K_1 , получив

$$\begin{aligned}K_{11} &= 2 - K_{21} \\K_{12} &= 18 - K_{21} \\K_{13} &= 22 - K_{21} \\K_{14} &= K_{11}\end{aligned}$$

- 6) Методом перебора, получилось выделить слово АРФА, значит $K_{21} = 2$ (В)

- 7) Выражаем через него остальные буквы.

$$\begin{aligned}K_{21} &= 2 \quad (\text{В}) \\K_{22} &= 3 + K_{21} = 5 \quad (\text{Е}) \\K_{23} &= 2 + K_{21} = 4 \quad (\text{Д}) \\K_{24} &= 14 + K_{21} = 16 \quad (\text{Р}) \\K_{25} &= 12 + K_{21} = 14 \quad (\text{О})\end{aligned}$$

Спасибо за внимание!

Задание было довольно простым, ибо программа всё делала за меня, но поперебирать уравнения было весело :)