МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра защиты информации и систем связи

УТВЕРЖДАЮ
Проректор по учебной работе
_____О.Г. Локтионова
«___» _____2015 г.

КРИПТОАНАЛИЗ ШИФРА МНОГОПЕТЛЕВОЙ ПОЛИАЛФАВИТНОЙ ПОДСТАНОВКИ

Методические указания по выполнению лабораторной работы для студентов специальностей 10.05.03, 10.05.02, 10.03.01

Курск 2015

УДК 004.056.55 (076.5)

Составитель: М.А. Ефремов

Рецензент
Кандидат технических наук, доцент *М.О. Таныгин*

Криптоанализ шифра многопетлевой полиалфавитной подстановки: методические указания по выполнению лабораторной работы / Юго-Зап. гос. ун-т; сост.: М.А. Ефремов. Курск, 2015. 14 с.: ил. 3, табл. 3. Библиогр.: с. 14.

Рассматриваются основные практические аспекты дешифрования криптограмм, зашифрованных методом многопетлевой полиалфавитной подстановки. В работе детально изложены стадии криптоанализа шифрограммы с использованием частотного анализа, индекса соответствия. Указывается порядок выполнения лабораторной работы, правила оформления и содержание отчета.

Методические указания соответствуют требованиям программы, утвержденной учебно-методическим объединением по образованию в области информационной безопасности (УМО ИБ).

Предназначены для студентов специальностей 10.05.03, 10.05.02, 10.03.01 дневной формы обучения.

Текст печатается в авторской редакции

Подписано в печать . Формат 60x84 1/16.
Усл.печ. л. . Уч.-изд.л. . Тираж 30 экз. Заказ. Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

СОДЕРЖАНИЕ

1. ЦЕЛЬ РАБОТЫ

Цель лабораторной работы - определить период шифра предлагаемой криптограммы; дешифровать криптограмму и получить составной ключ; вычислить первичные ключи.

2. ЗАДАНИЕ

Произвести подключение своего варианта, запустив исполняемый файл. Ознакомьтесь с руководством пользователя и с теоретическим материалом; определить период шифра предлагаемой криптограммы; дешифровать криптограмму, получив составной ключ; вычислить первичные ключи.

3. ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

1. Получить задание;
2. Изучить теоретическую часть;
3. Определить период шифра;
4. Получить составной ключ;
5. Вычислить первичные ключи;
6. Составить отчет.

4. СОДЕРЖАНИЕ ОТЧЕТА

1. Титульный лист;
2. Краткая теория;
3. Описание процесса дешифрования;
4. Подробное описание получения первичных ключей;
5. Вывод.

5. ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

5.1 Введение

Многопетлевая полиалфавитная подстановка является наиболее интересным подстановочным шифром. В шифре Виженера при шифровании используется только один ключ. В многопетлевом шифре используется не один, а несколько ключей шифрования. Их называют петлевыми или первичными ключами.

Многопетлевой шифр описывается формулой

$$Ei = (Mi + K1,i \bmod U1 + K2,i \bmod U2 + \ldots + Kj,i \bmod Uj + \ldots + KG,i \bmod UG) \bmod L, \quad (1)$$

где

Ei - i-ый символ криптограммы;

Mi - i-ый символ открытого текста;

L - мощность исходного алфавита;

G - количество петель шифра;

Uj - длина j-ого первичного ключа;

N - число символов в криптограмме;

$1 \le i \le N; \quad 1 \le j \le G.$

В качестве первичных ключей используются осмысленные слова русского языка. Последовательное и циклическое применение первичных ключей дает в итоге составной ключ.

Период составного ключа равен наименьшему общему кратному длин всех первичных ключей. Если длины первичных ключей являются взаимно простыми числами, то длина составного ключа равна их произведению и будет наибольшей.

Составной ключ равен сумме первичных ключей. В отличие от шифра Виженера составной ключ многопетлевых подстановок не является осмысленным словом и имеет гораздо больший период. Благодаря этому многопетлевые подстановки надежнее всех уже рассмотренных нами шифров.

Пусть, например, исходный текст будет “ЭТО СТРОКА ОТКРЫТОГО ИСХОДНОГО ТЕКСТА”, а в качестве первичных ключей будем использовать слова “ПЕРВЫЙ” и “БУКВА”. Процесс шифрования отражен в таблице 1:

Таблица 1 – Пример шифрования сообщения

Э	28	П	15	Б	1	(28+15+ 1) mod 32 = 12	М
Т	18	Е	5	У	19	(18+ 5+19) mod 32 = 10	К
О	14	Р	16	К	10	(14+16+10) mod 32 = 8	И
	31	В	2	В	2	(31+ 2+ 2) mod 32 = 3	Г
С	17	Ы	26	А	0	(17+26+ 0) mod 32 = 11	Л
Т	18	Й	9	Б	1	(18+ 9+ 1) mod 32 = 28	Э
Р	16	П	15	У	19	(16+15+19) mod 32 = 18	Т
О	14	Е	5	К	10	(14+ 5+10) mod 32 = 29	Ю
К	10	Р	16	В	2	(10+16+ 2) mod 32 = 28	Ю
А	0	В	2	А	0	(0 +2 + 0) mod 32 = 2	В
	31	Ы	26	Б	1	(31+26 +1) mod 32 = 26	Ы
О	14	Й	9	У	19	(14+ 9+19) mod 32 = 10	К
Т	18	П	15	К	10	(18+15+10) mod 32 = 11	Л
К	10	Е	5	В	2	(10+ 5+ 2) mod 32 = 17	С
Р	16	Р	16	А	0	(16+16+ 0) mod 32 = 0	А
Ы	26	В	2	Б	1	(26+ 2+ 1) mod 32 = 29	Ю
Т	18	Ы	26	У	19	(18+26+19) mod 32 = 31	
О	14	Й	9	К	10	(14+ 9+10) mod 32 = 33	Б
Г	3	П	15	В	2	(3+15+ 2) mod 32 = 20	Ф
О	14	Е	5	А	0	(14+ 5+ 0) mod 32 = 19	У
	31	Р	16	Б	1	(31+16+ 1) mod 32 = 16	Р
И	8	В	2	У	19	(8+ 2+ 19) mod 32 = 29	Ю
С	17	Ы	26	К	10	(17+26+10) mod 32 = 21	Х
Х	21	Й	9	В	2	(21+ 9+ 2) mod 32 = 0	А
О	14	П	15	А	0	(14+15+ 0) mod 32 = 29	Ю
Д	4	Е	5	Б	1	(4+ 5+ 1) mod 32 = 10	К
Н	13	Р	16	У	19	(13+16+19) mod 32 = 16	Р
О	14	В	2	К	10	(14+ 2+10) mod 32 = 26	Ы
Г	3	Ы	26	В	2	(3+26+ 2) mod 32 = 31	
О	14	Й	9	А	0	(14+ 9+ 0) mod 32 = 23	Ч
	31	П	15	Б	1	(31+15+ 1) mod 32 = 15	П
Т	18	Е	5	У	19	(18+ 5+19) mod 32 = 10	К
Е	5	Р	16	К	10	(5+16+10) mod 32 = 31	
К	10	В	2	В	2	(10 + 2+ 2) mod 32 = 14	О
С	17	Ы	26	А	0	(17+26+ 0) mod 32 = 11	Л

Т	18	Й	9	Б	1	(18+ 9+ 1) mod 32 = 28	Э
А	0	П	15	У	19	(0+15+19) mod 32 = 2	В

В результате шифрования получаем зашифрованный текст: “МКИГЛЭТЮЭВЫКЛСАЮ БФУРЮХАЮКРЫ ЧПК ОЛЭВ”. Для нашего примера L=32, N = 37, G=2, U1 = 6, U2 = 5. Длина составного ключа 30 символов.

Шифр Виженера является частным случаем многопетлевой постановки. Таким образом, выражение (1) наиболее полно описывает шифры замены и, как частный случай, включает в себя выражения для шифров Виженера и Цезаря.

5.2 Определение периода шифра. Метод Казиски

Криптоанализ многопетлевых шифров проводится, как и в случае шифра Виженера, в два этапа. Во-первых, необходимо определить период шифра (т.е. длину составного ключа) и, во-вторых, провести частотный анализ по группам периода.

Т.к. период обычно довольно большой (больше 10 символов), применение ИС не приведет к успеху. Однако существует и другой метод определения длины ключа. Это метод Казиски.

Суть его заключается в следующем. В открытом тексте сообщения встречаются одинаковые сочетания символов. В процессе криптографического преобразования может так случиться, что эти одинаковые сочетания зашифрованы одинаковой частью ключа. В результате и в криптограмме появятся одинаковые сочетания символов. Криптоаналитик может определить между ними расстояние и разложить это число на множители. Один из множителей будет равным периоду шифра. Если в криптограмме встретилось несколько пар одинаковых сочетаний, нужно определить расстояние для каждой пары и разложить его на множители. Множитель, который встретился чаще других, скорее всего и является искомой длиной ключа.

Однако возможны и “ложные тревоги”, когда одинаковые сочетания символов в криптограмме образованы случайным стечением обстоятельств.

Обычно, при использовании метода Казиски, криптоаналитики анализируют криптограммы на наличие в них одинаковых триграмм, т.к. вероятность присутствия в тексте одинаковых сочетаний из четырех и более символов слишком мала, а при использовании диаграмм велик процент ложных тревог.

Очевидным недостатком метода является его полная непригодность в случае отсутствия в тексте одинаковых сочетаний.

Рекомендуется использовать методы Казиски и ИС совместно. ИС показывает порядок длины ключа (больше или меньше 10 символов), а метод Казиски позволит определить точное значение.

6. ВЫПОЛНЕНИЕ РАБОТЫ

6.1 Запуск программы

Запустить на выполнение исполняемый файл pole.exe. Пользуясь клавишами управления курсором Up и Down, выберите номер Вашего варианта и нажмите Enter. Познакомьтесь с руководством пользователя и с теоретическим материалом, выбрав соответствующую опцию меню.

6.2 Определение периода шифра

Для этого выберите опцию меню “Нахождение периода”. Подменю, которое появится в результате на экране, содержит три пункта:

- Подход Ф. Казиски”. Позволяет автоматически определить период с помощью подхода Казиски. При выборе этой опции на экране появляется таблица, содержащая возможные значения периода шифра и их вес. Чем больше вес, тем вероятней это значение периода является истинным.
- “Использование индекса соответствия”. Позволяет уточнить значение периода, полученное методом Казиски.

- “Принятие решения”. Приняв решение о значении длины ключа, пользователь должен ввести это значение в появившемся окне ввода.

Методом Казиски получили таблицу возможных значений периода, пример представлен на рисунке 1.

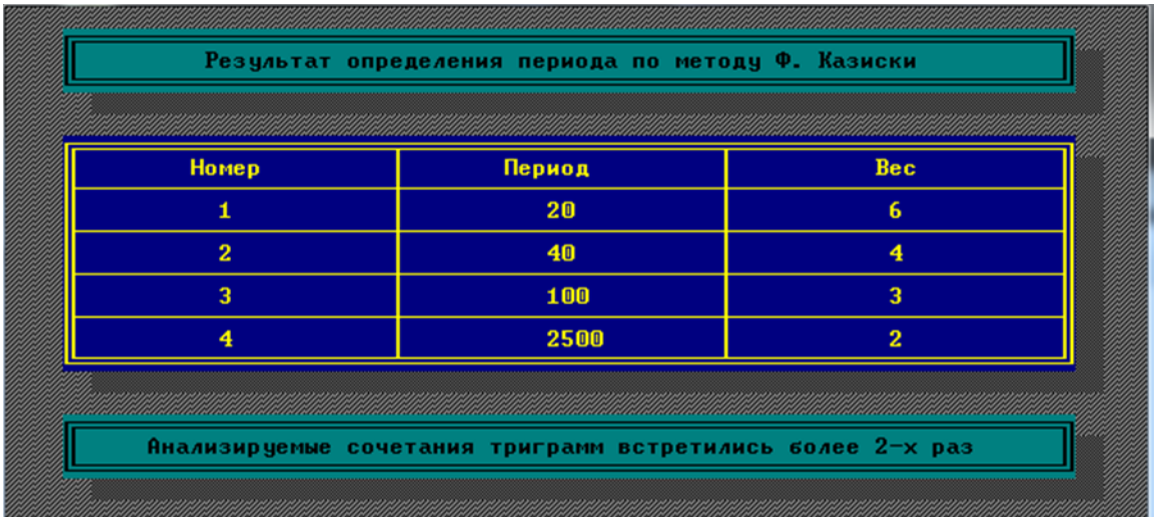

Рисунок 1 – Определение периода по методу Ф. Казиски

Наибольший вес имеет период 20.

Для большей уверенности уточним порядок периода с помощью ИС. Значение ИС для данной криптограммы равно 0.0314, что указывает на длину ключа более 10 символов.

Итак, окончательное решение: период равен 20.

6.3 Получение составного ключа

Для этого необходимо провести частотный анализ по группам периода и расшифровать криптограмму. Выберите опцию главного меню “Частотный анализ”. Чтобы изменить номер анализируемой группы, пользуйтесь клавишами управления курсором Left и Right. По клавише F4 осуществляется просмотр статистики текущей группы периода. В каждой группе периода заменяем самый часто встречаемый символ данной группы на самый частый символ русского языка - в нашем случае это “пробел”.

Замену символов нужно производить таким образом, для того чтобы ввести символ русского языка нужно использовать код данного символа (таблица 2), который вводиться при зажатии клавиши <Alt> цифрами, расположенными на клавиатуре справа.

Таблица 2 – таблица ASCII кодов

Символ	Код	Символ	Код
А	128	Р	144
Б	129	С	145
В	130	Т	146
Г	131	У	147
Д	132	Ф	148
Е	133	Х	149
Ж	134	Ц	150
З	135	Ч	151
И	136	Ш	152
Й	137	Щ	153
К	138	Ы	155
Л	139	Ь	156
М	140	Э	157
Н	141	Ю	158
О	142	Я	159
П	143	ПРОБЕЛ	032

Согласно частотному анализу наиболее часто встречающийся символ это пробел в соответствии со статистикой заменяемой поочередно наиболее часто встречающиеся символы криптограммы на пробел, представлено на рисунке 2.

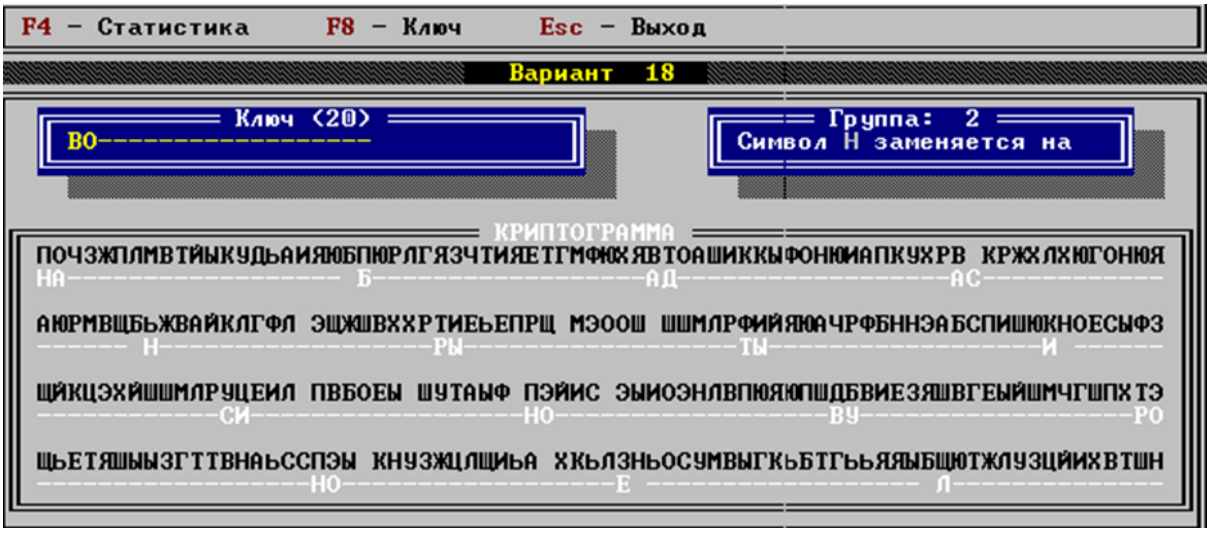

Рисунок 2 – Замена символов

Проделываем данные действия с каждым символом составного ключа пока не получим расшифрованную криптограмму и составной ключ, что представлено на рисунке 3.

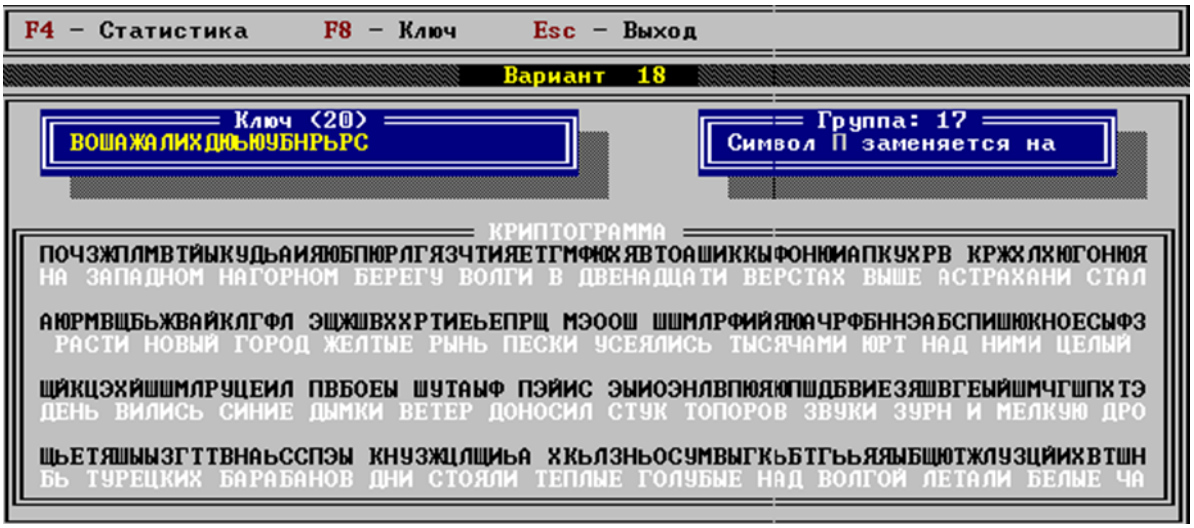

Рисунок 3 – Составной ключ

6.4 Получение первичных ключей

Составной ключ равен сумме циклически повторяющихся первичных ключей. Его длина является наименьшим общим кратным длин первичных ключей. T=20; p1= 5; p2=4.

Составим уравнения, из которых сможем найти значения первичных ключей. Подставим сюда конкретные значения символов составного ключа.

x1+y1= 2 (в)
x2+y2= 14 (о)
x3+y3= 24 (ш)
x4+y4= 0 (а)
x1+y5= 6 (ж)
x2+y1= 0 (а)
x3+y2= 11 (л)
x4+y3= 8 (и)
x1+y4= 21 (х)
x2+y5= 4 (д)
x3+y1=29 (ю)
x4+y2= 27 (ь)
x1+y3= 29 (ю)
x2+y4= 19 (у)
x3+y5= 1 (б)
x4+y1= 13 (н)
x1+y2= 16 (р)
x2+y3= 27 (ь)
x3+y4= 16 (р)
x4+y5= 17 (с)

Порядковые номера символов русского языка берутся из таблицы 3.

Таблица 3– Исходный алфавит

Нормативный алфавит	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П
Числовые эквиваленты	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Таблица 3 (продолжение)

Нормативный алфавит	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь	Э	Ю	Я	“_“
Числовые эквиваленты	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

Выразим ключи через одну переменную и выпишем 2 слова.

x1+y1=2
x2+y1=0
x3+y1=29
x4+y1=13

Заметим, что в данном случае y1-постоянна, а x изменяется от 1 до 4.

x1+y1=2
x1+y2=16
x1+y3=29
x1+y4=21
x1+y5=6

Для второго слова x1-постоянна, а y изменяется от 1 до 5.

Составим таблицу для слова состоящего из 4 букв, где y1-постоянна величина, которая может принимать значения от 0до 31. Перебор всех значений не обязателен, как только в столбце появиться слово можно прекратить перебор.

Получив один из первичных ключей, второй первичный ключ найдем из составного ключа, так же можно найти второй первичный ключ таким же методом, составив еще одну таблицу, но теперь x1 будем изменяться от 0 до 31, а в столбце y появиться слово. Первичные ключи являются словами русского языка, поэтому, перебрав все возможные значения, получим истинные значения первичных ключей.

7. КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Какие подстановочные шифры вам известны, назовите их?
2. Какими методами возможно определение периода шифра?
3. В чем особенности применения метода Метод Ф. Казиски?
4. Как узнать длину первичных ключей?
5. Какую длину имеют первичные ключи, если длинна составного ключа равна 48, 60?
6. В чем отличие шифра Виженера от многопетлевых подстановок, какой метод более криптостойкий?

8. СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

1. Н. Смарт. Криптография [текст] Издательство: М.: Техносфера, 2005. – 528 с.
2. С. Баричев Криптография без секретов [текст] Издательство: Горячая Линия – Телеком. 2004.- 43 с.
3. Нильс Фергюсон, Брюс Шнайер. Практическая криптография [текст] Издательство: Вильямс. 2005.- 416 с.