МИНОБРНАУКИ РОССИИ

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

Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе
_____ О.Г. Локтионова
«__» _____ 2016 г.

ШИФРОВАНИЕ МЕТОДОМ ПРЯМОЙ ЗАМЕНЫ

Методические указания по выполнению лабораторной работы по дисциплине «Введение в криптографию» для студентов специальностей 10.05.03, 10.05.02, 10.03.01

Курск 2016

УДК 004.056.55 (076.5)

Составитель М.А. Ефремов

Рецензент
Кандидат технических наук, доцент *И.В. Калуцкий*

Шифрование методом прямой замены: методические указания по выполнению лабораторной работы по дисциплине «Введение в криптографию» / Юго-Зап. гос. ун-т; сост.: М.А. Ефремов. Курск, 2016. 14 с.: ил. 3. Библиогр.: с. 14.

Рассматриваются основные практические и теоретические положения этапов шифрования сообщений, с помощью метода прямой замены. 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 – изучить и получить практические навыки в сокрытии информации при помощи шифра методом простой замены.

2 ЗАДАНИЕ

Ознакомиться с теоретическим материалом, получить представление о системе шифрования методом простой замены, зашифровать текст своего задания согласно варианту, используя представленные алгоритмы.

3 ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

1. Получить задание;
2. Изучить теоретическую часть;
3. Зашифровать открытый тест, используя шифрование методом простой замены;
4. Дешифровать сообщение, используя шифрование методом простой замены;
5. Составить отчет.

4 СОДЕРЖАНИЕ ОТЧЕТА

1. Титульный лист;
2. Краткая теория;
3. Описание процесса шифрования;
4. Описание процесса дешифрования;
5. Вывод.

5 ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

5.1 Введение

Шифрование - система передачи сообщения, где смысл сообщения скрывается с помощью шифра. Цель тайнописи, шифрования - сохранить информацию в тайне от противника и посторонних лиц. Задача в том - чтобы спрятать, замаскировать или записать (преобразовать) так, чтобы другим было непонятно.

Грандиозные достижения человечества – письменность и арифметика – есть не что иное, как системы кодирования речи и числовой информации. Любую запись на незнакомом нам языке можно рассматривать как своего рода криптограмму. Пиктографическое письмо – передача информации с помощью рисунка (пиктограммы). Позже картинки постепенно преобразовались в иероглифы. Некоторые древние надписи до сих пор учеными не расшифрованы.

Нередко авторы известных нам библейских рукописей совершенно намеренно употребляли загадочные слова и выражения, которые в наши дни приводят к неправильным толкованиям текста Библии. Множество тайн существует у любого языка. Не одно столетие учёные всего мира пытаются выяснить, что же таит в себе славянский алфавит. В древнерусских книгах тайнопись встречается довольно часто.

На Руси применялись различные системы тайнописи. Иногда в качестве тайнописи использовались буквы греческого и латинского алфавитов. Слово писалось буквами другого алфавита. Существовала урезанная тайнопись. Вместо буквы писалась её часть, различные сокращения (урезания) слов. Например, писали только первую и последнюю буквы, остальные выбрасывали. Обратное письмо (речь), цифровая тайнопись.

5.2 Метод прямой замены

Сущность методов замены (подстановки) заключается в замене символов исходной информации, записанных в одном алфавите, символами из другого алфавита по определенному правилу. Самым простым является *метод прямой замены.* Символам t_i исходного алфавита **A**, с помощью которых записывается исходная информация, однозначно ставятся в соответствие символы r_i

шифрующего алфавита B. В простейшем случае оба алфавита могут состоять из одного и того же набора символов. Например, оба алфавита могут содержать буквы русского алфавита.

Задание соответствия между символами обоих алфавитов осуществляется с помощью преобразования числовых эквивалентов символов слова T, длиной - m символов, по определенному алгоритму.

Пусть $A=(a_1,\ldots,a_n)$ исходный алфавит, с помощью которого представлено некоторое слово $T=(t_1,\ldots,t_m)$, t_i € A.

Введем в рассмотрение некоторый шифрующий алфавит $B=(b_1,\ldots,b_n)$, в котором необходимо представить шифртекст $R=(r_1,\ldots,r_m)$, r_i€B. В общем случае, элементами данного алфавита могут быть любые символы, в том числе и a_i.

Таким образом, требуется найти метод шифрования, позволяющий осуществлять взаимно-однозначное отображение любых T и R, при знании некоторой секретной (ключевой)информации.

Рассмотрим один из возможных вариантов, использующий в качестве ключевой следующую информацию:

$A=(a_1,\ldots,a_n)$ – исходный алфавит, $B=(b_1,\ldots,b_n)$ –шифрующий алфавит,

k1- весовой коэффициент символа, k2- коэффициент сдвига.

Алгоритм шифрования может быть представлен следующими основными шагами:

1. a) для алфавитов A и B строятся линейно упорядоченные множества натуральных чисел $DA=(da_1,\ldots,da_n)$ и $DB=(db_1,\ldots,db_n)$, причем DA=DB=(1,2,…,n).

   b) для символьного множества $T=(t_1,\ldots,t_m)$ задается числовое множество $DT=(dt_1,\ldots,dt_m)$, где dt_i € DA.

2. Формируется числовое множество $DR=(dr_1,\ldots,dr_m)$, где $dr_i=(dt_i *k1+k2)\mathrm{mod}(n)$.

3.Формируется символьное множество $R=(r_1,\ldots,r_m)$, где $r_i=f(dr_i, B)$.

Здесь, множество R определяет слово шифртекста.

Для выполнения обратной операции дешифрования (определения T) необходимо решить следующее целочисленное уравнение:

$dt_i*k1+k2=N*n+dr_i$,

здесь, считаются известными величины: $k1,k2,n,dr_i$. Параметр T изменяется в пределах от 1 до n.

Для пояснения материала рассмотрим пример. Пусть имеем:
A = (а,б,в,г,д,е,ж,з); T= (багаж);
B =(г,а,д,ж,з,в,е,б); k1=3, k2=6.
DA=DB=(1,2,3,4,5,6,7,8);
DT=(2,1,4,1,7);
Dr_1=(2*3+6)mod8=4; r_1=ж;
Dr_2=(1*3+6)mod8=1; r_2=г;
Dr_3=(4*3+6)mod8=2; r_3=а;
Dr_4=(1*3+6)mod8=1; r_4=г;
Dr_5=(7*3+6)mod8=3;r_5=д;
Следовательно, получен шифртекст R=(жгагд).
На практике, для выполнения шифрования и дешифрования данным методом используются таблицы следующего формата:

Таблица 1 – Общий вид таблицы шифрования

A	a_1	a_2		a_n	
DA	da_1	da_2		da_n	
$\overline{B}$	b_1	b_2		b_n	
$\overline{DB}$	db_1	db_2		db_n	

Где, $db_i=(da_i*k1+k3)\mod(n)$; $b_i= f(db_i,B)$.

Для рассмотренного примера получаем следующую таблицу:

Таблица 2 – Пример таблицы шифрования

A	а	б	в	г	д	е	ж	з
DA	1	2	3	4	5	6	7	8
$\overline{B}$	г	ж	е	а	з	б	д	в
$\overline{DB}$	1	4	7	2	5	8	3	6

Основным недостатком метода прямой замены является наличие одних и тех же статистических характеристик исходного и закрытого текста. Зная, на каком языке написан исходный текст и частотную характеристику употребления символов алфавита этого языка, криптоаналитик путем статистической обработки перехваченных сообщений может установить соответствие между символами обоих алфавитов.

6 ВЫПОЛНЕНИЕ РАБОТЫ

Для выполнения работы выдать студентам следующие исходные данные:

1. Алфавит A_0
2. Алфавит A_1
3. Исходный текст T_0
4. Коэффициенты k_1,k_2

Требуется получить шифртекст R и дешифрированный текст T, используя шифрование методом прямой замены.

Таблица 3- Индивидуальные задания

№	Исходные данные
1	A_0=А Б В Г Д Е Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я _ A_1= Р Щ Ь Я Т Э _ Ж М Ч Х А В Д Ы Ф К С Е З П И Ц Г Н Л Ъ Ш Б У Ю T_0=М Е Т О Д _ Ш И Ф Р О В А Н И Я k_1=5, k_2=5
2	A_0= А Б В Г Д Е Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я A_1= З П И Ц Г Н Л Ъ Ш Б У Ю Р Щ Ь Я Т Э Ж М Ч Х А В Д Ы Ф К С Е T_0=К Р И П Т О А Н А Л И З k_1=3, k_2=6
3	A_0= А Б В Г Д Е Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я _ A_1= В Д Ы Ф К С Р Щ Ь Я Т Э _ Ж М Ч Х А Е З П И Ц Г Н Л Ъ Ш Б У Ю T_0= К В А Д Р А Т _ П О Л И Б И Я k_1=3, k_2=5
4	A_0= А Б В Г Д Е Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я A_1= Н Л Ъ Ш Б У Ю Р Щ Ь Я Т Э Ж М Ч Ы Ф К С Х А В Д Е З П

	И Ц Г T_0= В И Д Е О А Д А П Т Е Р k_1=5, k_2=8
5	A_0= А Б В Г Д Е Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я _ A_1= М Ч Х А В Р Щ Ь Я Т Э Ж Д З П И Ц Г Ы Ф К С Е Н Л Ъ Ш Б У Ю T_0= К О Д И Р О В А Н И Е k_1=3, k_2=3
6	A_0= А Б В Г Д Е Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я A_1= Р Щ Ь Я Т Э Ж М Ч Х А В Д Ы Ф К С Е З П И Ц Г Н Л Ъ Ш Б У Ю T_0= И Н Ф О Р М А Ц И Я k_1=7, k_2=3
7	A_0= А Б В Г Д Е Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я A_1= Я Т Э Ж М Р Щ Ы Ф К Ь Ч Х А В Д С И Ц Г Е З П Н Л Ъ Ш Б У Ю T_0=К О Д И Р О В А Н И Е k_1=5, k_2=10
8	A_0= А Б В Г Д Е Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я _ A_1= А В Д Ы Р Щ Ь Я Т Э _ Ж М Ч Х С Е З П И Ц Ф К Г Н Л Ъ Ш Б У Ю T_0=Д В О И Ч Н Ы Й _ К О Д k_1=7, k_2=5
9	A_0= А Б В Г Д Е Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я _ A_1= Р Щ Ж М Ч Х Ь Я Т Э _ А В Д Ы Е З П И Ф К С Ц Г Н Л Ъ Ш Б У Ю T_0=Д И С П Е Т Ч Е Р _ Ф А Й Л О В k_1=3, k_2=7

10	A_0= А Б В Г Д Е Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я A_1= Р Щ Ь Я Т Э Ж М Ч Х А В Д Ы Ф К С Е З П И Ц Г Н Л Ъ Ш Б У Ю T_0=И Н Ф О Р М А Т И З А Ц И Я k_1=5, k_2=7
11	A_0= А Б В Г Д Е Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я A_1= Р Щ Ь Я Т Э Ж М Ч Х А В Д Ы Ф К С Е З П И Ц Г Н Л Ъ Ш Б У Ю T_0=К О Н Ф И Д Е Н Ц И А Л Ь Н О С Т Ь k_1=5, k_2=3
12	A_0= А Б В Г Д Е Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я _ A_1= Р М Ч Х А Щ Ь Я Т Э _ Ж В Д Е З П И Ы Ф К С Ц Г Н Л Ъ Ш Б У Ю T_0=Ц Е Л О С Т Н О С Т Ь _ Д А Н Н Ы Х k_1=7, k_2=10
13	A_0= А Б В Г Д Е Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я A_1= Р Н Л Щ В Д Ы Ь Я Ж М Ч Х А Т Э Ф К С Е З П И Ц Г Ъ Ш Б У Ю T_0=А У Т Е Н Т И Ф И К А Ц И Я k_1=9, k_2=2
14	A_0= А Б В Г Д Е Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я _ A_1= Р Щ Ь Я Т Э _ Ж М Ч Х А В Д Ы Ф К С Е З П И Ц Г Н Л Ъ Ш Б У Ю T_0=М Е Т О Д _ Ш И Ф Р О В А Н И Я k_1=11, k_2=5
15	A_0= А Б В Г Д Е Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я A_1= Р Б У Щ Ж М Ч Ь Я Т Э Х К С Е З П И А В Д Ы Н Л Ъ Ф Ц Г Ш Ю

	T_0=П О Д Л И Н Н О С Т Ь k_1=7, k_2=6
16	A_0= А Б В Г Д Е Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я A_1= Р Щ Ч Х А В Ь Я Т Э Н Л Ж Ф К С Е З П И М Д Ы Ц Г Ъ Ш Б У Ю T_0=К Р И П Т О С Т О Й К О С Т Ь k_1=13, k_2=4
17	A_0= А Б В Г Д Е Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я A_1= Р Щ Ь Я Т Ж М Д Ы Н Ч Х Э А В Ф Е З П И Ц Г К С Л Ъ Ш Б У Ю T_0=Ш И Ф Р О Т Е К С Т k_1=9, k_2=5
18	A_0= А Б В Г Д Е Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я _ A_1= Р Щ Ь Я Т Э _ Ж М Ч Х А В Д Ы Ф К С Е З П И Ц Г Н Л Ъ Ш Б У Ю T_0=М Е Т О Д _ Ш И Ф Р О В А Н И Я k_1=11, k_2=5
19	A_0= А Б В Г Д Е Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я _ A_1= Р Щ Ь М Ч Х А В Я Т Э _ Ж Д Ы Ф К Е С Ц Г Н З П И Л Ъ Ш Б У Ю T_0=У П Р А В Л Е Н И Е _ К Л Ю Ч А М И k_1=13, k_2=4
20	A_0= А Б В Г Д Е Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я _ A_1= Е З П Г Н Л Ъ И Ц Р Щ Ь Я Ж Д Ы М Ч Х А В Т Э Ф К С Ш Б У Ю T_0=К Р И П Т О А Н А Л И Т И К k_1=11, k_2=2
21	A_0= А Б В Г Д Е Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь

	Э Ю Я A_1= М Ч Х А В Р Щ Ь Я Т Ы Ф К Э Ж Д Ц Г Н Л Ъ С Е З П И Ш Б У Ю T_0=Р А С Ш И Ф Р О В Ы В А Н И Е k_1=9, k_2=4
22	A_0= А Б В Г Д Е Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я A_1= Д Ы Р Щ Ь Я М Ч Х А В Ф К С Т Э Ж Г Н Е З П И Ц Л Ъ Ш Б У Ю T_0=Х Е Ш И Р О В А Н И Е k_1=13, k_2=5
23	A_0= А Б В Г Д Е Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я A_1= Э Ж М Р Щ Ь Я Т А В Д К С Е Ф З П Г Н Ы Ч Х И Ц Л Ъ Ш Б У Ю T_0=П Р О Т О К О Л k_1=7, k_2=10
24	A_0= А Б В Г Д Е Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я A_1= У Ю М Ч Х Ж В А Р Щ Ь Я Ф Ъ Ш К С Е Д Ы Т Э И Ц Г З П Н Л Б T_0=И Д Е Н Т И Ф И К А Ц И Я k_1=9, k_2=6
25	A_0= А Б В Г Д Е Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я A_1= Ж М Ч Р Щ Ь Я У Ю Т Э Д Ы Х А В Ф К С Е З П И Ц Г Н Л Ъ Ш Б T_0=П Р О Г Р А М М А k_1=11, k_2=7
26	A_0= А Б В Г Д Е Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я A_1= Р Щ Ь Я Т Э Ж М Ч Х А В Д Ы Ф К С Е З П И Ц Г Н Л Ъ Ш Б У Ю T_0=С Т Е Г А Н О Г Р А Ф И Я

	k_1=3, k_2=6
27	A_0= А Б В Г Д Е Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я A_1= Р У Ю Щ Ь Я Э Ж М Т Ч Х Ф К С Е З П И А В Г Н Д Ы Ц Л Ъ Ш Б T_0=К О М П Ь Ю Т Е Р k_1=13, k_2=5
28	A_0= А Б В Г Д Е Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я A_1= Д Ы Ф К Р Щ Ь Я Т Э Ч Х А В Ю Ж М С Е И Ц З П Г Н Л Ъ Ш Б У T_0=И Н Т Е Р Ф Е Й С k_1=15, k_2=6
29	A_0= А Б В Г Д Е Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я A_1= Р Ь Я Т Э Щ Б Ж М Ч Х Ф К С Ы З Д Ц Г Н П И Ю Е А В Л Ъ Ш У T_0=К Л А В И А Т У Р А k_1=11, k_2=5
30	A_0= А Б В Г Д Е Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я A_1= М Ч Х У Ю А В Р Щ Ь Я Т Ы Ф И Ц Г К С Д П Н Е Л Ъ Ш З Э Ж Б T_0=Д Е Ф Р А Г М Е Н Т А Ц И Я k_1=7, k_2=6

7 КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Что такое шифрование?
2. Назовите определение прямого шифрования?
3. Допускается ли производить замену букв на цифры?
4. Назовите недостатки и достоинства метода прямой замены?

8 СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

1. Н. Смарт . Криптография [текст] Издательство: М.: Техносфера, 2005. – 325 с.
2. Сингх С. Книга шифров. Тайная история шифров и их расшифровки. [текст] М.: Аст, Астрель, 2006. 567 с.
3. Бауэр Ф. Расшифрованные секреты. Методы и принципы криптологии. [текст] М.: Мир, 2007. 432 с.