

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Локтионова Оксана Геннадьевна
Должность: проректор по учебной работе
Дата подписания: 08.02.2021 16:55:11
Уникальный программный ключ:
0b817ca911e6668abb13a5d426d39e5f1c11eabbf73e943df4a4851fda56d089

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.....	4
2. Задание.....	4
3. Порядок выполнения работы.....	4
4. Содержание отчета.....	4
5. Теоретическая часть.....	5
5.1. Введение.....	5
5.2. Метод прямой замены.....	5
6. Выполнение работы.....	9
7. Контрольные вопросы.....	14
8. Библиографический список.....	14

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 текст, 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 g_i

шифрующего алфавита В. 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 Т, длиной - m символов, по определенному алгоритму.

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

Введем в рассмотрение некоторый шифрующий алфавит $B=(b_1, \dots, b_n)$, в котором необходимо представить шифртекст $R=(r_1, \dots, r_m)$, $r_i \in B$. 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 Т и R, при знании некоторой секретной (ключевой) информации.

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

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

k_1 - весовой коэффициент символа, k_2 - коэффициент сдвига.

Алгоритм шифрования может быть представлен следующими основными шагами:

1. а) для алфавитов А и В строятся линейно упорядоченные множества натуральных чисел $DA=(da_1, \dots, da_n)$ и $DB=(db_1, \dots, db_n)$, причем $DA=DB=(1, 2, \dots, n)$.

б) для символьного множества $T=(t_1, \dots, t_m)$ задается числовое множество $DT=(dt_1, \dots, dt_m)$, где $dt_i \in DA$.

2. Формируется числовое множество $DR=(dr_1, \dots, dr_m)$, где $dr_i=(dt_i * k_1 + k_2) \bmod(n)$.

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

Здесь, множество R определяет слово шифртекста.

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

$$dt_i * k_1 + k_2 = N * n + dr_i,$$

здесь, считаются известными величины: k_1, k_2, n, dr_i . Параметр Т изменяется в пределах от 1 до n.

Для пояснения материала рассмотрим пример. Пусть имеем:

$A = (а,б,в,г,д,е,ж,з); T = (багаж);$

$B = (г,а,д,ж,з,в,е,б); k_1=3, k_2=6.$

$DA=DB=(1,2,3,4,5,6,7,8);$

$DT=(2,1,4,1,7);$

$Dr_1=(2*3+6)mod8=4; r_1=ж;$

$Dr_2=(1*3+6)mod8=1; r_2=г;$

$Dr_3=(4*3+6)mod8=2; r_3=а;$

$Dr_4=(1*3+6)mod8=1; r_4=г;$

$Dr_5=(7*3+6)mod8=3; r_5=д;$

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, $db_i=(da_i*k_1+k_3)mod(n); b_i= f(db_i,B).$

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 дешифрованный текст T , используя шифрование методом прямой замены.

Таблица 3- Индивидуальные задания

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

	ИЦГ T ₀ =ВИДЕОАДАПТЕР k ₁ =5, k ₂ =8
5	A ₀ =АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЪЫЬ ЭЮЯ_ A ₁ =МЧХАВРЩЬЯТЭ ЖДЗПИЦГЫФКСЕНЛЬШБ УЮ T ₀ =КОДИРОВАНИЕ k ₁ =3, k ₂ =3
6	A ₀ =АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЪЫЬ ЭЮЯ A ₁ =РЩЬЯТЭ ЖМЧХАВДЫФКСЕЗПИЦГНЛЬШБ УЮ T ₀ =ИНФОРМАЦИЯ k ₁ =7, k ₂ =3
7	A ₀ =АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЪЫЬ ЭЮЯ A ₁ =ЯТЭЖМРЩЫФКЬЧХАВДСИЦГЕЗПНЛЬШБ УЮ T ₀ =КОДИРОВАНИЕ k ₁ =5, k ₂ =10
8	A ₀ =АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЪЫЬ ЭЮЯ_ A ₁ =АВДЫРЩЬЯТЭ_ЖМЧХСЕЗПИЦФКГНЛЬШ БУЮ T ₀ =ДВОИЧНЫЙ_КОД k ₁ =7, k ₂ =5
9	A ₀ =АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЪЫЬ ЭЮЯ_ A ₁ =РЩЖМЧХЬЯТЭ_АВДЫЕЗПИФКСЦГНЛЬШ БУЮ T ₀ =ДИСПЕТЧЕР_ФАЙЛОВ k ₁ =3, k ₂ =7

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

	<p>T_0=ПОДЛИННОСТЬ $k_1=7, k_2=6$</p>
16	<p>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 Ъ 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=КРИПТОСТОЙКОСТЬ $k_1=13, k_2=4$</p>
17	<p>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 Ъ 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=ШИФРОТЕКСТ $k_1=9, k_2=5$</p>
18	<p>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 Ъ 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=МЕТОД_ШИФРОВАНИЯ $k_1=11, k_2=5$</p>
19	<p>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 Ъ 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=УПРАВЛЕНИЕ_КЛЮЧАМИ $k_1=13, k_2=4$</p>
20	<p>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 Ъ Я Ж Д Ы М Ч Х А В Т Э Ф К С Ш Б У Ю T_0=КРИПТОАНАЛИТИК $k_1=11, k_2=2$</p>
21	<p>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</p>

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

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

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.