Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Емельянов Сергей Геннадьевич
Должность: ректор
Дата подписания: 01.02.2021 17:01:31
Уникальный программный ключ:
9ba7d3e34c012eba476ffd2d064cf2781953be730df2374d16f3c0ee536f0fe6

МИНОБРНАУКИ РОССИИ

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

Кафедра информационной безопасности

ШИФРОВАНИЕ МЕТОДОМ ПОЛИАЛФАВИТНОЙ ЗАМЕНЫ

Методические указания по выполнению лабораторной работы для студентов направлений 02.03.03, 09.03.01, 09.03.02, 09.03.03, 09.03.04, 10.03.01, 10.05.02, 38.03.01, 38.03.03, 38.03.05, 38.05.01, 40.05.01, 43.03.02, 43.03.03, 45.03.03

Курск 2019

УДК 004.056.55 (076.5)

Составители: М.А. Ефремов, С.И. Егоров

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

Шифрование методом полиалфавитной замены: методические указания по выполнению лабораторной работы / Юго-Зап. гос. ун-т; сост.: М.А. Ефремов, С.И. Егоров. Курск, 2019. 9 с.: табл. 3. Библиогр.: с. 9.

Рассматриваются основные практические и теоретические положения этапов шифрования сообщений, с помощью метода полиалфавитной подстановки. 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 направлений 02.03.03, 09.03.01, 09.03.02, 09.03.03, 09.03.04, 10.03.01, 10.05.02, 38.03.01, 38.03.03, 38.03.05, 38.05.01, 40.05.01, 43.03.02, 43.03.03, 45.03.03 очной и заочной формы обучения.

Текст печатается в авторской редакции

Подписано в печать 04.04.19.. Формат 60x84 1/16.
Усл.печ. л. 0,4. Уч.-изд.л. 0,3. Тираж 30 экз. Заказ. 301 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 с помощью метода полиалфавитной замены.

2 ЗАДАНИЕ

Ознакомиться с теоретическим материалом, получить представление об алгоритме полиалфавитной замены, зашифровать текст своего задания согласно варианту, используя представленные алгоритмы.

3 ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

1. Получить задание.
2. Изучить теоретическую часть.
3. Получить шифртекст, используя матрицу шифрования.
4. Получить расшифрованный текст, используя матрицу шифрования.
5. Составить отчет.

4 СОДЕРЖАНИЕ ОТЧЕТА

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

5 ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

5.1 Введение

До начала XX века криптографические методы применялись лишь для шифрования данных с целью защиты от несанкционированного доступа. В двадцатом веке в связи с развитием техники передачи информации на дальние расстояния интерес к криптографии значительно возрос. Системы шифрования варьируются от самых элементарных до очень сложных. И если первые не требуют никаких математических познаний, то в последних используются понятия, знакомые лишь специалистам в некоторых областях математики и информатики.

История криптоанализа берет своё начало с моноалфавитных шифров. Данный шифр обеспечивал необходимую секретность передаваемым сообщениям до тех пор, пока развитие частотного криптоанализа не разрушило его стойкость. Первым слабость таких шифров к частотному криптоанализу показал ещё в IX веке арабский философ и математик Аль-Кинди в своем труде «Манускрипт о дешифровке криптографических сообщений». В Европе моноалфавитные шифры пользовались большой популярностью вплоть до XV века. Ярким примером ненадежности этого шифра послужила казнь Марии Стюарт в 1587 году. Доказательством заговора против английской королевы Елизаветы стало расшифрованное Томасом Фелиппесом письмо Марии Стюарт к Энтони Бабингтону. Таким образом, возникла потребность в создании более совершенного способа защиты информации, и на смену моноалфавитным шифрам пришли полиалфавитные.

В целях маскирования естественной частотной статистики исходного языка применяется полиалфавитная подстановка, которая также бывает нескольких видов. В полиалфавитных подстановках для замены символов исходного текста используется не один, а несколько алфавитов.

Методы полиалфавитной замены являются существенно более стойкими. Такие методы основаны на использовании нескольких алфавитов для замены символов исходного текста.

Наибольшее распространение получил алгоритм полиалфавитной замены с использованием таблицы (матрицы) Вижинера, которая представляет собой квадратную матрицу.

5.2 Алгоритм полиалфавитной подстановки

Формально полиалфавитную замену можно представить следующим образом. При N - алфавитной замене символ t_1 из исходного алфавита A_1 заменяется символом r_1 из алфавита A_2, символ t_2 заменяется символом r_2 из алфавита A_2 и так далее.

Полиалфавитная замена с использованием таблицы (матрицы) Вижинера M_v, представляет собой квадратную матрицу [nxn], где n - количество символов в используемом алфавите.

Матрица M_v строится следующим образом. В первой строке располагаются символы в алфавитном порядке. Начиная со второй строки, символы записываются со сдвигом влево на одну позицию. Выталкиваемые символы заполняют освобождающиеся позиции справа (циклический сдвиг). (если используется русский алфавит, то матрица Вижинера имеет размерность [32x32]).

Таблица 1- Матрица Вижинера M_v

a_1	a_2	……..	a_n
a_2	a_3	……...	a_1
a_3	a_4		a_2
…	…	……	…
a_n	a_1	……	a_{n-1}

Шифрование осуществляется с помощью ключа, состоящего из m неповторяющихся символов:

$K=(k_1,k_2,\ldots k_m)$

Для шифрования, вначале, строится матрица шифрования M_c размерностью [(m+1),n] следующего вида:

Таблица 2- Матрица шифрования M_c

a_1	a_2	…….	a_n
$\mathbf{a_i}$	a_{i+1}	……..	$a_{(i+n)mod(n)-1}$
$\mathbf{a_j}$	a_{j+1}		$a_{(j+n)mod(n)-1}$
…	…	……	…
$\mathbf{a_p}$	a_{p+1}	……	$a_{(p+n)mod(n)-1}$

Где**,** $\mathbf{a_i}=k_1$, $\mathbf{a_j}=k_2$, $\mathbf{a_p}=k_m$.

Предположим, что требуется выполнить шифрование некоторого текстового фрагмента $T=(t_1,t_2,\ldots t_s)$, пусть s>>m. Тогда ключ K последовательно записывается требуемое число раз под данным фрагментом, т.е. имеем

$(t_1 \;\; t_2 \;\; t_3 \;\; t_4 \ldots\ldots t_m \;\; t_{m+1} \;\; \ldots\ldots\ldots)$

$(k_1 \;\; k_2 \;\; k_3 \;\; k_4 \ldots\ldots k_m \;\; k_1 \;\; \ldots\ldots\ldots\ldots)$

Предположим, что шифртекст представлен текстовым фрагментом вида:

$R=(r_1,r_2,r_3,\ldots\ldots r_s)$**.**

Для нахождения любого r_l , (l=1,…,s) необходимо:

1. Записать ключ под исходным текстом.
2. Определить строку матрицы для которой соответствующий $k_l=\mathbf{a_d}$ **(**d=1,…,m).
3. Определить r_l , как элемент этой строки, расположенный в одном столбце с элементом t_l первой строки матрицы.

Для дешифрования, т.е. для нахождения любого t_l необходимо:

1. Записать ключ под зашифрованным текстом.
2. Определить строку матрицы для которой соответствующий $k_l=\mathbf{a_d}$ **(**d=1,…,m).
3. Определить t_l , как элемент первой строки, расположенный в одном столбце с элементом r_l найденной строки матрицы.

6 ВЫПОЛНЕНИЕ РАБОТЫ

Используя теоретический материал и представленный алгоритм, выполнить процедуру шифрования и дешифрования согласно следующим вариантам. Требуется получить шифртекст R и дешифрированный текст T, используя соответствующую матрицу шифрования.

Таблица 3- Индивидуальные задания

№	Исходные данные		
	Алфавит A	Исходный текст T	Ключ K
1	(1,2,3,4,5)	(13442)	(142)
2	(1,2,5,7,8)	(11725)	(182)
3	(1,4,6,7,8)	(28671)	(146)
4	(2,3,5,6,7)	(66237)	(237)
5	(3,6,7,8,9)	(89933)	(389)
6	(1,3,5,8,9)	(59113)	(158)
7	(2,5,7,8,9)	(77529)	(287)
8	(1,3,5,6,7)	(63511)	(135)
9	(3,4,6,8,9)	(81169)	(346)
10	(1,4,6,7,8)	(64177)	(167)
11	(4,5,7,8,9)	(48775)	(457)
12	(3,5,7,8,9)	(57388)	(389)
13	(2,3,5,7,8)	(82235)	(257)
14	(1,4,7,8,9)	(11748)	(147)
15	(2,3,4,6,7)	(64423)	(324)
16	(1,4,5,6,7)	(14766)	(146)
17	(3,4,5,6,8)	(55348)	(346)
18	(1,2,4,6,8)	(24661)	(124)
19	(1,4,7,8,9)	(87441)	(174)
20	(2,3,6,8,9)	(82366)	(263)

7 КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Что такое шифрование?
2. На чем основан метод полиалфавитной замены?
3. Что такое матрица Вижинера?
4. Как строится матрица Вижинера?
5. Как осуществляется шифрование сообщения?
6. Как осуществляется расшифрование сообщения?

8 СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

1. Н. Смарт . Криптография [текст] Издательство: М.: Техносфера, 2005. – 528 с.
2. Сингх С. Книга шифров. Тайная история шифров и их расшифровки. [текст] М.: Аст, Астрель, 2006. 447 с.
3. Бауэр Ф. Расшифрованные секреты. Методы и принципы криптологии. [текст] М.: Мир, 2007. 550 с.