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.

ШИФР «КВАДРАТ ПОЛИБИЯ»

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*

Шифр «Квадрат Полибия»: методические указания по выполнению лабораторной работы по дисциплине «Введение в криптографию» / Юго-Зап. гос. ун-т; сост.: М.А. Ефремов. Курск, 2016. 13 с.: табл. 4. Библиогр.: с. 13.

Содержат сведения о способах сокрытия информации при помощи шифра «Квадрат Полибия», являющимся подстановочным шифром. 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 «Квадрат Полибия».

2 ЗАДАНИЕ

Ознакомиться с теоретическим материалом, получить представление о системе шифрования, 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 шифр «Квадрат Полибия».
4. Расшифровать сообщение, используя «Квадрат Полибия».
5. Составить отчет.

4 СОДЕРЖАНИЕ ОТЧЕТА

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

5 ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

5.1 Введение

Криптогра́фия (от др.-греч. κρυπτός – скрытый и γράφω – пишу) – наука о методах обеспечения конфиденциальности (невозможности прочтения информации посторонним) и аутентичности (целостности и подлинности авторства, а также невозможности отказа от авторства) информации.

Изначально криптография изучала методы шифрования информации – обратимого преобразования открытого (исходного) текста на основе секретного алгоритма и/или ключа в шифрованный текст (шифротекст). Традиционная криптография образует раздел симметричных криптосистем, в которых зашифрование и расшифрование проводится с использованием одного и того же секретного ключа. Помимо этого раздела современная криптография включает в себя асимметричные криптосистемы, системы электронной цифровой подписи (ЭЦП), хеш-функции, управление ключами, получение скрытой информации, квантовую криптографию.

Криптография не занимается: защитой от обмана, подкупа или шантажа законных абонентов, кражи ключей и других угроз информации, возникающих в защищенных системах передачи данных.

Криптография – одна из старейших наук, ее история насчитывает несколько тысяч лет.

Поли́бий (др.-греч. Πολύβιος, лат. Polybius, 201 до н. э.,

Мегалополь, Аркадия – 120 до н. э.) – греческий историк, государственный деятель и военачальник, автор "Всеобщей истории" ("Истории") в 40 томах, охватывающих события в Риме, Греции, Македонии, Малой Азии и в других регионах с 220 до н. э. по 146 до н. э.. Из книг "Истории" полностью сохранились только первые 5, остальные дошли в более или менее подробных изложениях. Прочие труды Полибия не сохранились. Исходя из учения стоиков о предвидении, он пришёл к метафизике истории, которая рассматривала последнюю как борьбу народов и отдельных личностей против власти судьбы.

В криптографии квадрат Полибия (англ. Polybius square), также известный как шахматная доска Полибия – оригинальный код простой замены, одна из древнейших систем кодирования, предложенная Полибием (греческий историк, полководец, государственный деятель, III век до н. э.). Данный вид кодирования изначально применялся для греческого алфавита, но затем был распространен на другие языки.

5.2 Шифр «Квадрат Полибия»

Квадрат Полибия является одной из модификации одноалфавитной замены, в котором символ алфавита заменяется парой чисел или символов по определенному правилу. Рассмотрим прямоугольник, часто называемый доской Полибия.

Таблица 1 – квадрат Полибия

	1	2	3	4	5	6
1	А	Б	В	Г	Д	Е
2	Ё	Ж	З	И	Й	Л
3	Л	М	Н	О	П	Р
4	С	Т	У	Ф	Х	Ц
5	Ч	Ш	Щ	Ъ	Ы	Ь
6	Э	Ю	Я	,	.	-

В такой прямоугольник буквы могут вписываться в произвольном порядке, причем схема записи держится в тайне и составляет ключ шифрования. Для того чтобы получались приближенные к квадрату матрицы (6x6, 5x7, 6x5), в алфавит могут включаться знаки препинания или исключаться редко используемые символы (такие как «ё», «й»).

В процессе шифрования каждая буква открытого текста представляется в шифротексте парой цифр, указывающих строку и столбец, в которых расположена данная буква. Так

представлениями букв В, Г, П, У будут 13, 14, 33, 41 соответственно. Если использовать приведенный выше квадрат в качестве ключа шифрования, то фраза «ШИФРОВАНИЕ» будет зашифрована в «462342343213113123 16». В приведенном примере размер шифротекста превышает размер исходного текста в 2 раза, учитывая, что получившийся квадрат имеет по 6 строк и столбцов, для кодирования каждой буквы будет достаточно 6 бит (3 для номера строки, 3 для номера столбца).

Максимальное количество ключей для шифра равно n!. Для латинкого алфавита в первую клетку можно вписать одну из 25 букв, во вторую – одну из 24, в третью – одну из 23 и т.д. Получаем максимальное количество ключей для шифра на таблице латинского алфавита:

$N = 25 * 24 * 23 * ... * 2 * 1 = 25!$

Соответственно для расшифрования сообщения потребуется не только знание алфавита, но и ключа, с помощью которого составлялась таблица шифрования. Но произвольный порядок букв тяжело запомнить, поэтому пользователю шифра необходимо постоянно иметь при себе ключ – квадрат.

6 ВЫПОЛНЕНИЕ РАБОТЫ

6.1 Шифрование сообщений при помощи квадрата Полибия

Используя теоретический материал зашифровать текст, используя квадрат Полибия, согласно вариантам. Регистр не учитывается.

Таблица 2 – квадрат Полибия

	1	2	3	4	5	6
1	А	Б	В	Г	Д	Е
2	Ё	Ж	З	И	Й	Л
3	Л	М	Н	О	П	Р
4	С	Т	У	Ф	Х	Ц
5	Ч	Ш	Щ	Ъ	Ы	Ь
6	Э	Ю	Я	,	.	-

Таблица 3 – Индивидуальные задания

№	Текст для расшифрования
1.	Баба с возу, кобыле легче
2.	Труд человека кормит, а лень портит
3.	Без труда не вытащить и рыбки из пруда
4.	Без беды друга не узнаешь
5.	Терпенье и труд все перетрут
6.	Людей много, а человека нет
7.	Живу, как живётся, а не как люди хотят

№	Текст для расшифрования
8.	Жизнь измеряется не годами, а трудами
9.	Язык болтает, а голова не знает
10.	Книги не говорят, а правду сказывают
11.	Муж жену любит здоровую, а брат сестру богатую
12.	Умный бы ты был человек - кабы не дурак
13.	На грубое слово не сердись, на ласковое не сдавайся
14.	Раз солгал, а на век лгуном стал
15.	Красота до вечера, а доброта навек
16.	Барская просьба — строгий приказ
17.	Боится, как черт ладана
18.	Бьется как рыба об лед
19.	В дороге и палка пригодится
20.	В зимний холод всякий молод
21.	В тихом омуте черти водятся
22.	Вертится, как черт перед заутреней
23.	Вернемся к нашим баранам
24.	Возвращаться на круги своя
25.	Все течет, все изменяется
26.	Как ручки сделают — так гузка сносит
27.	Краткость — сестра таланта
28.	Курица по зернышку клюет да сыта бывает
29.	Льет воду на чужую мельницу
30.	Прежде соберись, а потом дерись

6.2 Расшифрование при помощи квадрата Полибия

Используя теоретический материал расшифровать текст, используя квадрат Полибия, согласно вариантам. Регистр не учитывается.

Таблица 4 – Индивидуальные задания

№	Шифрограмма
1.	26 11 12 11 33 51 24 26
2.	11 15 36 16 41 11 33 42
3.	26 11 31 16 51 24 42 56
4.	12 24 36 32 11 33 26 11
5.	13 16 36 16 33 24 46 11
6.	13 55 46 16 15 24 42 56
7.	14 43 12 34 52 31 21 35
8.	14 36 63 23 33 43 42 56
9.	26 36 16 15 24 42 14 13
10.	26 36 11 41 11 13 26 11
11.	26 34 52 51 34 33 26 11
12.	32 24 56 16 13 11 42 56
13.	32 24 14 23 11 42 24 42
14.	32 16 42 11 41 42 11 23
15.	32 16 31 56 51 11 42 56
16.	33 11 15 43 12 24 42 56
17.	33 11 15 52 24 13 26 11

№	Шифрограмма
18.	33 11 15 55 32 24 42 56
19.	34 12 32 34 51 24 42 56
20.	34 12 32 11 33 53 24 26
21.	34 12 31 16 35 24 45 11
22.	34 35 56 63 33 24 42 56
23.	34 36 11 42 34 36 24 25
24.	14 34 36 31 34 13 34 25
25.	34 35 42 24 32 16 42 36
26.	34 35 31 34 52 33 55 26
27.	35 16 36 16 32 34 51 56
28.	35 16 36 16 14 33 34 25
29.	35 16 33 34 14 24 35 41
30.	35 16 31 56 32 16 33 56

7 КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Что такое криптография?
2. Что такое «Квадрата Полибия»?
3. Какое максимальное количество ключей для шифра на латинском и русском языках?
4. Как происходит шифрование и расшифрование шифром «Квадрат Полибия»?
5. Назовите недостатки и достоинства шифра «Квадрат Полибия»?

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.