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 АНАЛИТИЧЕСКИМИ МЕТОДАМИ

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 аналитическими методами: методические указания по выполнению лабораторной работы по дисциплине «Введение в криптографию» / Юго-Зап. гос. ун-т; сост.: М.А. Ефремов. Курск, 2016. 11 с.

Рассматриваются основные практические и теоретические положения этапов шифрования сообщений аналитическими преобразованиями, с помощью методов матричной алгебры. 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 методы шифрования сообщений, используя аналитические преобразования.

2. ЗАДАНИЕ

Ознакомьтесь с теоретическим материалом и методикой шифрования аналитическими методами. Получит шифртекст R, используя матрицу шифрования и выполнить расшифрование с применением обратной матрицы.

3. ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

1. Получить задание в соответствии с вариантом.
2. Изучить теоретическую часть.
3. Зашифровать слово, используя матрицу шифрования.
4. Выполнить расшифрование с применением обратной матрицы.
5. Повторить пункты 3 и 4, используя компьютер (режим электронных таблиц EXCEL).
6. Составить отчет.

4. СОДЕРЖАНИЕ ОТЧЕТА

1. Титульный лист.
2. Краткая теория.
3. Расчёты получения шифртекста R.
4. Расчёты получения T_0.
5. Скриншоты выполнения шифрования и расшифрования с использованием электронных таблиц EXCEL.
6. Вывод.

5. Теоретическая часть

Для шифрования информации могут использоваться аналитические преобразования. Наибольшее распространение получили методы шифрования, основанные на использовании матричной алгебры. Зашифрование k-го блока исходной информации, представленного в виде вектора $B_k = ||b_j||$, осуществляется путем перемножения матрицы-ключа $A = ||a_{ij}||$ и вектора B_k. В результате перемножения получается блок шифртекста в виде вектора $C_k = ||c_i||$, где элементы вектора C_k определяются по формуле:

$$c_i = \sum_j a_{ij} b_j$$

Расшифрование информации осуществляется путем последовательного перемножения векторов C_k и матрицы A^{-1}, обратной матрице А.

6. Пример выполнения работы

Шифрования информации с использованием алгебры матриц.

Пусть необходимо зашифровать и расшифровать слово

$T_0 =< ЗАБАВА >$ с помощью матрицы-ключа А:

$$A = \begin{vmatrix} 1 & 4 & 8 \\ 3 & 7 & 2 \\ 6 & 9 & 5 \end{vmatrix}$$

Для зашифрования исходного слова необходимо выполнить следующие шаги.

Шаг 1. Определяется числовой эквивалент исходного слова как последовательность соответствующих порядковых номеров букв слов Тэ: $T_Э =< 8, 1, 2, 1, 3, 1 >$

Шаг 2. Умножение матрицы А на векторы $B_1 = \{8, 1, 2\}$ и $B_2 = \{1, 3, 1\}$:

$$C_1 = \begin{vmatrix} 1 & 4 & 8 \\ 3 & 7 & 2 \\ 6 & 9 & 5 \end{vmatrix} \bullet \begin{vmatrix} 8 \\ 1 \\ 2 \end{vmatrix} = \begin{vmatrix} 28 \\ 35 \\ 67 \end{vmatrix}$$

$$C_2 = \begin{vmatrix} 1 & 4 & 8 \\ 3 & 7 & 2 \\ 6 & 9 & 5 \end{vmatrix} \bullet \begin{vmatrix} 1 \\ 3 \\ 1 \end{vmatrix} = \begin{vmatrix} 21 \\ 26 \\ 38 \end{vmatrix}$$

Шаг 3. Зашифрованное слово записывается в виде последовательности чисел $R =< 28, 35, 67, 21, 26, 38 >$. Расшифрование слова осуществляется следующим образом.

Шаг 1. Вычисляется определитель |A| = -115.

Шаг 2. Определяется присоединенная матрица А*, каждый элемент которой является алгебраическим дополнением элемента матрицы А

$$A^* = \begin{vmatrix} 17 & -3 & -15 \\ 52 & -43 & 15 \\ -48 & 22 & -5 \end{vmatrix}$$

Шаг 3. Получается транспонированная матрица A^T

$$A^T = \begin{vmatrix} 17 & 52 & -48 \\ -3 & -43 & 22 \\ -15 & 15 & -5 \end{vmatrix}$$

Шаг 4. Вычисляется обратная матрица A^{-1} по формуле:

$$A^{-1} = A^T / |A|$$

В результате вычислений обратная матрица имеет вид:

$$A^{-1} = \begin{vmatrix} -17/115 & -52/115 & 48/115 \\ 3/115 & 43/115 & -22/115 \\ 15/115 & -15/115 & 5/115 \end{vmatrix}$$

Шаг 5. Определяются векторы B_1 и B_2:

$B_1 = A^{-1}*C_1$; $B_2 = A^{-1}*C_2$.

$$B_1 = \begin{vmatrix} -17/115 & -52/115 & 48/115 \\ 3/115 & 43/115 & -22/115 \\ 15/115 & -15/115 & 5/115 \end{vmatrix} \bullet \begin{vmatrix} 28 \\ 35 \\ 67 \end{vmatrix} = \begin{vmatrix} 8 \\ 1 \\ 2 \end{vmatrix}$$

$$B_1 = \begin{vmatrix} -17/115 & -52/115 & 48/115 \\ 3/115 & 43/115 & -22/115 \\ 15/115 & -15/115 & 5/115 \end{vmatrix} \bullet \begin{vmatrix} 21 \\ 26 \\ 38 \end{vmatrix} = \begin{vmatrix} 1 \\ 3 \\ 1 \end{vmatrix}$$

Шаг 6. Числовой эквивалент расшифрованного слова

$T_Э =< 8, 1, 2, 1, 3, 1 >$ заменяется символами, в результате чего получается исходное слово $T_0 =< ЗАБАВА >$.

7. Варианты заданий

Вариант 1.

$$A=\begin{vmatrix}1 & 2 & 0\\ -1 & -3 & 4\\ 2 & 5 & 6\end{vmatrix};\ T_0 =< ЮМОРИСТИЧНЫЙ >$$

Вариант 2.

$$A=\begin{vmatrix}5 & 3 & -1\\ 3 & 2 & -1\\ 1 & 1 & 0\end{vmatrix};\ T_0 =< АЭРОДИНАМИКА >$$

Вариант 3.

$$A=\begin{vmatrix}11 & 7 & -4\\ 7 & 4 & -3\\ 2 & 2 & -1\end{vmatrix};\ T_0 =< БЛАГОВЕЩЕНИЕ >$$

Вариант 4.

$$A=\begin{vmatrix}-1 & 0 & -2\\ -5 & 4 & -7\\ 6 & -4 & -6\end{vmatrix};\ T_0 =< ЭВОЛЮЦИОНИСТ >$$

Вариант 5.

$$A=\begin{vmatrix}2 & 5 & 7\\ 6 & 3 & 4\\ 5 & -2 & -3\end{vmatrix};\ T_0 =< ТЕРМИНОЛОГИЯ >$$

Вариант 6.

$$A=\begin{vmatrix}1 & 2 & 3\\ 2 & 1 & 2\\ 3 & 1 & 3\end{vmatrix};\ T_0 =< НАМОРАЖИВАТЬ >$$

Вариант 7.

$$A=\begin{vmatrix}2 & 1 & 7\\ 3 & -5 & 9\\ -1 & 4 & 6\end{vmatrix};\ T_0 =< ПЯТИУГОЛЬНИК >$$

Вариант 8.

$$A=\begin{vmatrix}3 & 4 & 2\\ 2 & -1 & -3\\ 1 & 5 & 1\end{vmatrix};\ T_0 =< ОБЩЕСТВЕННИК >$$

Вариант 9.

$$A=\begin{vmatrix}2 & 5 & 1\\ 3 & 8 & 2\\ 1 & 2 & 0\end{vmatrix};\ T_0 =< КРИПТОГРАФИЯ >$$

Вариант 10.

$$A=\begin{vmatrix}2 & 7 & 3\\ 3 & 9 & 4\\ 1 & 5 & 3\end{vmatrix};\ T_0 =< ЕЖЕНЕДЕЛЬНИК >$$

Вариант 11.

$$A=\begin{vmatrix}2 & 2 & 7\\ -3 & -2 & 5\\ 4 & 3 & -1\end{vmatrix};\ T_0 =< ЧЕРНОКНИЖККНИК >$$

Вариант 12.

$$A=\begin{vmatrix}5 & 7 & 4\\ 8 & 3 & 4\\ 7 & 2 & 3\end{vmatrix};\ T_0 =< ЦАРЕУБИЙСТВО >$$

Вариант 13.

$$A=\begin{vmatrix}7 & 4 & 9\\ 3 & 4 & 7\\ 2 & 3 & 6\end{vmatrix};\ T_0 =< СПЕЦИФИКАЦИЯ >$$

Вариант 14.

$$A=\begin{vmatrix}4 & 8 & 12\\ 1 & 2 & 3\\ 1 & 3 & 5\end{vmatrix};\ T_0 =< УДИВИТЕЛЬНЫЙ >$$

Вариант 15.

$$A=\begin{vmatrix}2 & 1 & 5\\ 1 & 3 & 2\\ 7 & 6 & 3\end{vmatrix};\ T_0 =< ИМПРОВИЗАТОР >$$

Вариант 16.

$$A=\begin{vmatrix}1 & 2 & 3\\ 4 & 5 & 6\\ 7 & 8 & 9\end{vmatrix};\ T_0 =< МУСОРОПРОВОД >$$

Вариант 17.

$$A=\begin{vmatrix}1 & 1 & 1\\ 1 & 2 & 3\\ 7 & 3 & 6\end{vmatrix};\ T_0 =< РУКОВОДИТЕЛЬ >$$

Вариант 18.

$$A=\begin{vmatrix}3 & 2 & 1\\ 2 & 2 & 3\\ 5 & 1 & 2\end{vmatrix};\ T_0 =< ЗВЕРОВОДСТВО >$$

Вариант 19.

$$A=\begin{vmatrix}3 & 3 & 3\\ 5 & 2 & 1\\ 2 & 4 & 2\end{vmatrix};\ T_0 =< СЪЕХИДНИЧАТЬ >$$

Вариант 20.

$$A=\begin{vmatrix}3 & 2 & 1\\ 2 & 2 & 3\\ 5 & 1 & 2\end{vmatrix};\ T_0 =< ТРЁХДЮЙМОВЫЙ >$$

Вариант 21.

$$A=\begin{vmatrix}3 & 3 & 3\\ 3 & 2 & 1\\ 5 & 2 & 2\end{vmatrix};\ T_0 =< ШИФРОВАЛЬЩИК >$$

Вариант 22.

$$A=\begin{vmatrix}3 & 1 & 1\\ 2 & 3 & 3\\ 3 & 2 & 3\end{vmatrix};\ T_0 =< ОБЛИЗЫВАТЬСЯ >$$

Вариант 23.

$$A=\begin{vmatrix}5 & 1 & 1\\ 4 & 5 & 2\\ 1 & 6 & 5\end{vmatrix};\ T_0 =< ХЛАДНОКРОВИЕ >$$

Вариант 24.

$$A=\begin{vmatrix}3 & 2 & 3\\ 2 & 3 & 1\\ 1 & 2 & 7\end{vmatrix};\ T_0 =< ЯЙЦЕКЛАДУЩИЙ >$$

Вариант 25.

$$A=\begin{vmatrix}2 & 3 & 4\\ 5 & 6 & 8\\ 1 & 0 & 7\end{vmatrix};\ T_0 =< ВАЛЬЛСИРОВАТЬ >$$

Вариант 26.

$$A=\begin{vmatrix}3 & 1 & 1\\ 2 & 1 & 3\\ 4 & 1 & 1\end{vmatrix};\ T_0 =< ГИДРОСАМОЛЁТ >$$

Вариант 27.

$$A=\begin{vmatrix}2 & 3 & 4\\ 3 & 7 & 5\\ 4 & 5 & 1\end{vmatrix};\ T_0 =< АЭРОМЕХАНИКА >$$

Вариант 28.

$$A = \begin{vmatrix} 1 & 2 & 4 \\ 5 & 1 & 2 \\ 3 & 1 & 1 \end{vmatrix};\ T_0 =< УСПЕВАЕМОСТЬ >$$

Вариант 29.

$$A = \begin{vmatrix} 1 & 2 & 3 \\ 2 & 5 & 3 \\ 1 & 0 & 8 \end{vmatrix};\ T_0 =< ЖУРНАЛИСТКА >$$

Вариант 30.

$$A = \begin{vmatrix} 1 & 2 & 3 \\ 2 & 6 & 4 \\ 3 & 4 & 5 \end{vmatrix};\ T_0 =< КОНЦЕНТРАЦИЯ >$$

8. Контрольные вопросы

1. Что такое шифрование данных?
2. К какому виду шифрования относится данный метод?
3. В чём сущность шифрования аналитическими методами?
4. Что такое присоединенная матрица?
5. Что такое транспонированная матрица?
6. Какие ещё методы шифрования вы знаете?