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 «ЛИТОРЕЯ»

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 «Литорея»: методические указания по выполнению лабораторной работы по дисциплине «Введение в криптографию» / Юго-Зап. гос. ун-т; сост.: М.А. Ефремов. Курск, 2016. 13 с.: ил. 3, табл. 3. Библиогр.: с. 13.

Содержат сведения о способах сокрытия информации при помощи древнерусского шифра «Литорея», являющимся наиболее интересным 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 древнерусского шифра «Литорея», зашифровать текст своего задания по описанному алгоритму.

2 ЗАДАНИЕ

Ознакомиться с теоретическим материалом, получить представление о древнерусской системе шифрования, зашифровать текст своего задания согласно варианту, используя представленные алгоритмы

3 ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

1. Получить задание;
2. Изучить теоретическую часть;
3. Дешифровать сообщение, используя шифр «Простая Литорея»;
4. Зашифровать открытый тест, используя шифр «Мудрая Литорея»;
5. Составить отчет;

4 СОДЕРЖАНИЕ ОТЧЕТА

1. Титульный лист;
2. Краткая теория;
3. Описание процесса дешифрования;
4. Описание процесса шифрования;
5. Представление расшифрованного и зашифрованного сообщения;
6. Вывод.

5 ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

5.1 Введение

Тайнопись существует столько же, сколько и письменность. Криптографическое закрытие является специфическим способом защиты информации, оно имеет многовековую историю развития и применения.

Шифрование - система передачи сообщения, где смысл сообщения скрывается с помощью шифра. Цель тайнописи, кодирования, 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, литорея.

5.2 Шифр «Литорея простая»

Литорея (от лат. littera — буква) — тайнописание, род шифрованного письма, употреблявшегося в древнерусской рукописной литературе. Известна литорея двух родов: простая и мудрая. Простая, иначе называемая тарабарской грамотой, заключается в следующем: поставив согласные буквы в два ряда, в порядке:

Таблица 1- Таблица шифрования

б	в	г	д	ж	з	к	л	м	н
щ	ш	ч	ц	х	ф	т	с	р	п

Для шифрования употребляют в письме верхние буквы вместо нижних и наоборот, причём гласные остаются без перемены; так, например, ИНФОРМАЦИЯ = ИПЗОМРАДИЯ и т. п.

Таблицу для шифрования совершенно необязательно куда-то записывать, её легко запомнить. В первой строке первые 10 согласных, записанных в обычном порядке. Во второй строке таблицы простой литореи - следующие 10 согласных, записанных в обратном порядке. При этом буква Й не участвует в таблице.

Гласные, пробелы и прочие несогласные из оппозиции в простой литореии замене не подлежат. Это является существенным недостатком такого рода шифровальных систем. Если пробелы не включены в таблицу замены, видно, сколько слов в тексте, сколько букв в каждом из них.

Еще большим недостатком является,то что не заменяются гласные. Не сложно отгадать слова без согласных, например: *ОЕ*И*Е*ИЕ - нетрудно догадаться, что правильный ответ - СОЕДИНЕНИЕ. В том-то и проблема, что есть немало слов, где гласные - большинство букв, и простая литорея этого не учла.

5.3 Шифр «Литорея мудрая»

В старину на Руси мудрая литорея представляла собой десятизначную систему условных знаков. Алфавит (возможно, не полностью) разбивали на три группы по десяти букв в каждой. Буквы первого десятка обозначались точками («а» — одна точка, «б» — две, «в» — три и т. д.), буквы второго десятка — черточками, буквы третьего десятка — кружочками или крестиками. Знаки, составляющие одну букву, выписывались столбиком. Текст, зашифрованный таким способом, разделяли по горизонтали на две равные части, которые надлежало хранить порознь. Расшифровать написанное мудрой литореей можно было, только имея обе половинки текста.

В современном русском алфавите тридцать три буквы. Разбивая их на три равные группы, можно составить одиннадцатизначную литорею.

Число 11 не делится пополам, поэтому горизонтальная черта делит каждую табличку на две неравные части: в верхних «половинках» по шести рядов, в нижних — по пяти. То, что части табличек не равны, никакого значения для головоломки не имеет.

Ниже представлены рисунки используя, которые можно зашифровать сообщение мудрой литореей.

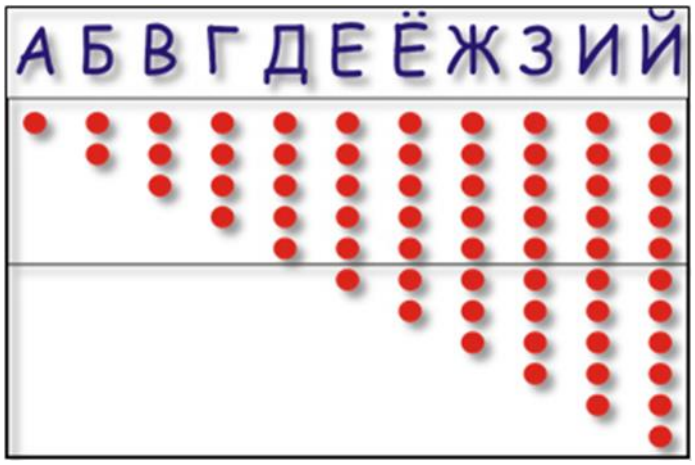

Рисунок 1- 1 группа системы шифрования

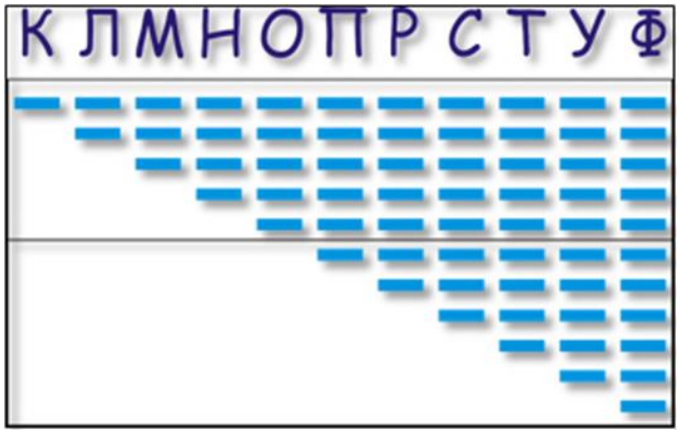

Рисунок 2- 2 группа системы шифрования

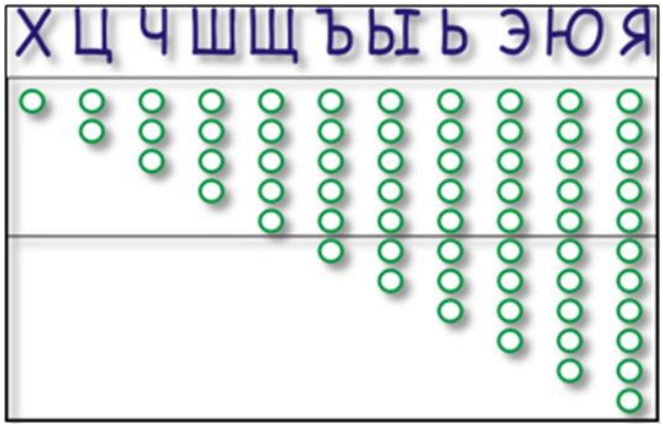

Рисунок 3- 3 группа системы шифрования

6 ВЫПОЛНЕНИЕ РАБОТЫ

6.1 Дешифрование сообщений при помощи простой Литореи

Используя теоретический материал и таблицу шифрования дешифровать сообщения, согласно вариантам. Запятые, пробелы, гласные, точки не подлежат замене. Буква ё в тестах сообщений замена на е. Регистр не учитывается.

Таблица 2- Индивидуальные задания

№	Текст для дешифрования
1	ИФ_ЧОМОЦА_УХЕ_ШЫЛКУНАСО_ПЕНМИЯКЕСЬЛТОЕ_ШОЙЛТО,_ЧМЕРЯ_Ш_СИКАШМЫ_И_КМУЩЫ.
2	ЧСЯЦЯ_Ш_ФЕМТАСЬПЫЙ_БИК,Ш_ТОКОМОР_ОКМАХАСАЛЬ_РЕЦУФА,НЕМЛЕЙ_НОЦЩЕХАС_Т_ПЕЙ_И_ОКЛЕТ_ЧОСОШУ.
3	ЛКАМИТ_НМИСЕЧ_Т_ФЕРСЕ_И,_ЕБЕ_ФАЦЫЖАЯЛЬ_ОК_ЛКМАЖА,_ЛКАС_ВЕНКАКЬ_ЛКМАППЫЕ_ЛСОША
4	Я_ЛКАС_ГИКАКЬ,_И_ШО_РПЕ_НМОЩУЦИСАЛЬ_ОЖОКА_Т_СИКЕМАКУМЕ.
5	КОГПАЯ_ИПЗОМРАДИЯ_РЧПОШЕППО_НМИШЕСА_Ш_ЦШИХЕПИЕ_ЖОМОВО_ПАСАХЕППУЮ,ПО_ФАЛКОЯШВУЮЛЯ_РАВИПУ_ИЛКОМИГЕЛТОЧО_НМОЧПОФА.
6	ЯШИШВИЛЬ_КОЧЦА_Л_ШИФИКОР,_ОП_ШОВЕС_Л_ГУШЛКШОР_ЩСАЧОЦЕКЕСЯ,_ЧОКОШЯБЕЧОЛЯ_НОХАКЬ_НСОЦЫ_И_ШЫЛСУВАКЬ_ШЕЛЬРА_ЛСАЦТИЕ_ТОРНСИРЕПКЫ.
7	ЦАХЕ_ШОМОП,_ЛИЦЯ_ПА_ИФЧОМОЦИ,_ТАМТАС_ОК_ЖОСОЦА_ШО_ШЛЕ_ЧОМСО.
8	Ш_ОЦПО_КИЖОЕ,_КЕНСОЕ_УКМО_Ш_ЩОСЬПИДУ_НМИПЕЛСИ_ЦОСЧОХЦАППОЕ_НИЛЬРО.
9	РОСОЦОЙ_ГЕСОШЕТ_ШФЯС_ИЖ_И_ЦО_КОЧО_МАЛЛЕМЦИСЛЯ,_ГКО_ЖОКЕС_ЩЫСО_УХЕ_УЙКИ,_ПО_ОЦУРАСЛЯ_.
10	НОЦ_ЕЧО_ПАЦФОМОР_ПА_ЦШЕПАЦДАКОР_ЧОЦУ_ШЫУГИСЛЯ_Я_МУЛЛТОЙ_ЧМАРОКЕ_И_РОЧ_ОГЕПЬ_ФЦМАШО_ЛУЦИКЬ_О_ЛШОЙЛКШАЖ_ЩОМФОЧО_ТОЩЕСЯ.
11	НМЯРАЯ_ЦОМОЧА_ФАПЕЛЕПА_ЩЫСА_ЛПЕЧОР,_ПО_НО_ШЛЕЙ_ЛКЕНИ_ШИЦПЫ_ЩЫСИ_ТОПЛТИЕ_ЛСЕЦЫ.
12	СЕЦ,ПЕОТМЕНВИЙ_ПА_МЕГТЕ_ЛКУЦЕПОЙ,_ЛСОШПО_ТАТ_КАЮБИЙ_ЛАЖАМ,СЕХИК_.

13	Л_ФАРИМАПИЕР_ЛЕМЦДА_И_ПЕМШПОЮ_ЦМОХЬЮ_НОЦ ОВЕС_ОП_Т_НМЕОЧМОРПЕЙВЕРУ_ЦОРУ,_ШЫЖОЦИШВЕР У_ОЦПОЮ_ЛКЕПОЙ_ПА_ТАПАШУ.
14	РЫЛСЬ_О_ЛТОМОЙ_МАФСУТИ_ЛО_РПОЮ_КАТ_НОМАФИС А_РАКУВТУ,ГКО_ОПА_УМОПИСА_СОХТУ_Ш_ ТАЛКМЮСЬТУ.
15	ОКЕД_СИФИП_ЩЫС_ЦОШОСЬПО_ФАХИКОГПЫЙ_НОЛЕСЯ ПИП,НОКОРУ_ГКО_ОП_СЮЩИС_ЛШОЮ_МАЩОКУ,НАЖАС _ЖОМОВО_ФЕРСЮ.
16	ЛАПЯ_УЛНЕС_Т_ЭКОЙ_НОМЕ_ШЫЛЫНАКЬ_Ш_ШЕЦМО_К МИ_КМЕЖСИКМОШЫЖ_ЩИЦОПА,_ПАНОСПИШ_ЕЧО_ЩОС ЬВЕ_ГЕР_ПАНОСОШИПУ.
17	ТПИЧА_РАМТО_НОСО_-_КАСАПКСИШЫЙ_НЕМЕЛТАФ_ ШНЕГАКСЕПИЙ_НЕМЛИЦЛТИЖ_ТУНДОШ_О_ЛКМАПЛКШ ИЯЖ_НО_ШОЛКОТУ.
18	РЕЛЯД_ЕБЕ_ПЕ_ШЛКАШАС,_И_КОСЬТО_ЦШЕ_ФШЕФЦОГТ И,_ТАТ_ЦША__РАЯТА,_ЛШЕМТАСИ_ПА_КЕРПО-ЛИПЕР_ЛШОЦЕ.
19	СЕШИКАП_ЛОФПАШАС_ЭКО,_И_НОЛСЕ_НОЕФЦТИ_Ш_ТМ ЫР_МЕВИС_ИФЧПАКЬ_ЛО_ЛШОИЖ_ЖОСЛКОШ_КЕРПЫЕ_К ОПА.
20	ЛАРЫЕ_РЯЧТИЕ_И_КМОЧАКЕСЬПЫЕ_ЛКИЖИ_И_ТАМКИП Ы_ПАНИЛАПЫ_МУЛЛТИРИ_НОЭКАРИ_И_ЖУЦОХПИТАРИ_ ОЩ_ОЛЕПИ.
21	СЕЛ_КЯПЕКЛЯ_ПА_РПОЧО_ШЕМЛК,_РПОЧО_Ш_ПЕР_ЖШО И_И,_ШЕМПО,_ЦОЛКАКОГПО_ФШЕМЬЯ.
22	СЕЛКПИДА_ПАГИПАЕКЛЯ_УХЕ_Л_НЕМШОЙ_ЛКУНЕПИ,_И _НЕПИЕ_ПАГИПАЕК_ЛШОЮ_РЕСОЦИЮ_УХЕ_Л_НЕМШОЧО _ФШУТА.
23	ЭКА_ИФСЕКЕШВАЯ_ИЛТМА_ЦУЖА_РОХЕК_ЩЫКЬ_ШОЛН МИПЯКА_И_НОЛКИЧПУКА_КОСЬТО_ЦУЖОШПО_ХИШЫР_ И_ИЛТМЯБИРЛЯ_ЦУЖОР_ЛЕМЦДЕР.
24	ЦМЕШПИЕ_ЧМЕТИ_И_МИРСЯПЕ_НМОДАМАНЫШАСИ_ЩУ ТШЫ_Ш_ЛСОЕ_ШОЛТА_ФАОЛКМЕППОЙ_НАСОГТОЙ,_ПА_ ЦМУЧОР_ТОПДЕ_ТОКОМОЙ_ИРЕСАЛЬ_СОНАКОГТА.
25	ЦМЕШПИЕ_ЧМЕТИ_И_МИРСЯПЕ_НИЛАСИ_ПА_НОТМЫКЫ Ж_ШОЛТОР_ЦЕМЕШЯППЫЖ_КАЩСИГТАЖ_ФАОЛКМЕППЫ РИ_НАСОГТАРИ,_ТОКОМЫЕ_ПАФЫШАСИ_ЛКИСОЛ.

26	ЛЕТМЕКАМЬ_ШФЯС_ЛО_ЛКОСА_ЦОТУРЕПКЫ_И_МУГТУ_И_ОКНМАШИСЛЯ_Ш_ТАЩИПЕК_ЧСАШПОЧО_ПАГАСЫПИТА
27	ЛОСПДЕ_ЛНМЯКАСОЛЬ_ФА_ПАЩЕХАШВУЮ_КУГТУ_И_НО_ФЕРСЕ_НМОЩЕХАСА_ЩОСЬВАЯ_КЕПЬ.
28	ТОЧЦА_ФПАЕВЬ,_ГКО_ШЛЕ_НЕМЕКЕМНИВЬ_И_ШЫЦЕМХИВЬ_МАЦИ_КОЧО,_ТОЧО_СЮЩИВЬ,_КОЧЦА_И_ПАГИПАЕКЛЯ_СЮЩОШЬ.
29	ОТЕАП_-_ЭКО_ПЕ_КОСЬТО_ШОЦА,_ЭКО__ШФАИРОЦЕЙЛКШИЕ_МАЛКШОМЕППЫЖ_Ш_ПЕЙ_ЛОСЕЙ,_РИПЕМАСЫПЫЖ_ГАЛКИД,_ЧАФОШ.
30	ОП_ЖОЦИС_И_ЖОЦИС_РЕХЦУ_ЛИЦЯБИРИ_И_ЛПУЮБИРИ_НАЛЛАХИМАРИ_УХЕ_ПЕЛТОСЬТО_ГАЛОШ.

6.2 Шифрование при помощи мудрой Литореи

Используя теоретический материал и рисунки 1,2,3 для шифрования сообщения, согласно вариантам зашифровать сообщения.

Таблица 3- Индивидуальные задания

№	Открытый тест
1.	Алгоритмизация
2.	Архитектура ЭВМ
3.	Видеоадаптер
4.	Вычислительная сеть
5.	Гибкий диск
6.	Двоичный код
7.	Дефрагментация
8.	Диалоговое окно
9.	Диспетчер файлов
10.	Жесткий диск
11.	Защита данных
12.	Интерфейс
13.	Информатизация
14.	Информация
15.	Клавиатура

16.	Кодирование
17.	Компьютер
18.	Контроллер
19.	Криптография
20.	Локальная сеть
21.	Микропроцессор
22.	Многозадачность
23.	Накопитель
24.	Оперативная память
25.	Панель задач
26.	Программирование
27.	Редактирование
28.	Текстовый редактор
29.	Технология
30.	Форматирование

7 КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Что такое шифрование?
2. Назовите определение Литореи?
3. Какие виды Литореи вам известны, назовите их?
4. В чем суть каждого вида Литореи?
5. Назовите недостатки и достоинства Литореи?

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.