ПРИЛОЖЕНИЕ 2
Методические указания к выполнению лабораторных работ “Разработка программ шифрования на основе методов Полибия, замены и умножения матриц”

Целью лабораторных работ является создание студентом программных реализаций шифрования на основе методов Полибия, замены и умножения матриц.

Разработанные программы шифрования демонстрируются преподавателю на примере тестовых задач.

Отчет по лабораторной работе должен содержать:

1. Цель работы.
2. Постановку задачи.
3. Метод решения задачи.
4. Структурную схему алгоритма.
5. Листинг программы.
6. Результаты работы программ.
7. Выводы.

П2.1. Шифрование и дешифрирование информации

Криптография дает возможность преобразовать информацию таким образом, что ее прочтение (восстановление) возможно только при знании ключа.

В качестве информации, подлежащей шифрованию и дешифрированию, будут рассматриваться *тексты*, построенные на некотором *алфавите*. Под этими терминами понимается следующее.

Алфавит - конечное множество используемых для кодирования информации знаков.

Текст - упорядоченный набор из элементов алфавита.

Шифрование - преобразовательный процесс: *исходный текст*, который носит также название *открытого текста*, заменяется *шифрованным текстом* (рис. П2.1).

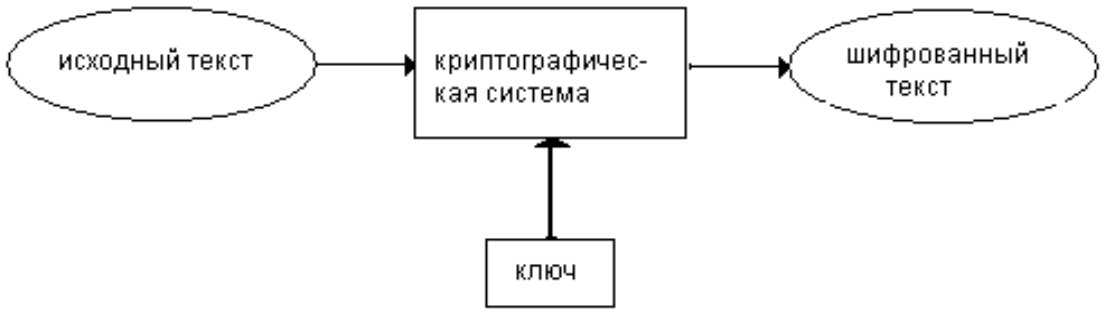

Рис. П2.1.

Дешифрирование - обратный шифрованию процесс. На основе ключа шифрованный текст преобразуется в исходный (рис. П2.2).

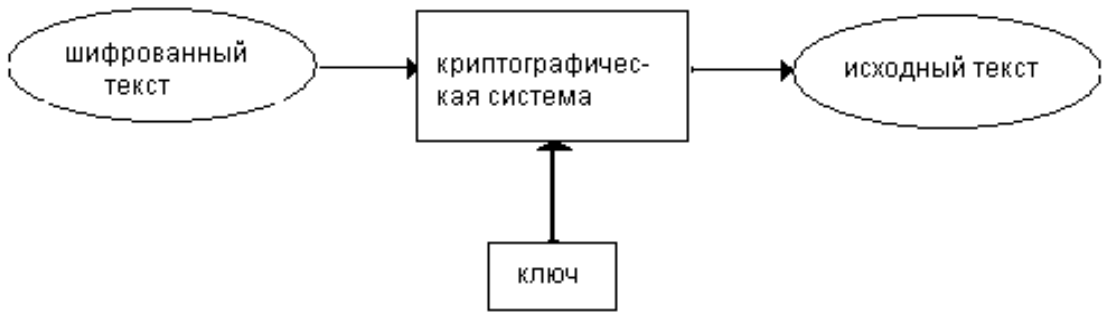

Рис. П2.2.

Ключ - информация, необходимая для беспрепятственного шифрования и дешифрования текстов.

Криптографическая система представляет собой семейство **T** преобразований открытого текста. Члены этого семейства индексируются, или обозначаются символом *k*; параметр *k* является *ключом*. Пространство ключей *K* - это набор возможных значений ключа. Обычно ключ представляет собой последовательный ряд букв алфавита.

Криптосистемы разделяются на *симметричные* и *с открытым ключом*.

В *симметричных криптосистемах* и для шифрования, и для дешифрования используется *один и тот же ключ*.

В *системах с открытым ключом* используются два ключа - *открытый* и *закрытый*, которые математически связаны друг с другом. Информация

шифруется с помощью открытого ключа, который доступен всем желающим, а расшифровывается с помощью закрытого ключа, известного только получателю сообщения.

Термины *распределение ключей* и *управление ключами* относятся к процессам системы обработки информации, содержанием которых является составление и распределение ключей между пользователями.

Электронной (цифровой) подписью называется присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения. *Криптостойкостью* называется характеристика шифра, определяющая его стойкость к дешифрованию без знания ключа (т.е. криптоанализу). Имеется несколько показателей криптостойкости, среди которых:

- количество всех возможных ключей;
- среднее время, необходимое для криптоанализа.

Преобразование T_k определяется соответствующим алгоритмом и значением параметра k. Эффективность шифрования с целью защиты информации зависит от сохранения тайны ключа и криптостойкости шифра.

П2.2. Реализация методов защиты информации

Проблема реализации методов защиты информации имеет два аспекта:

- разработку средств, реализующих криптографические алгоритмы,
- методику использования этих средств.

Каждый из рассмотренных криптографических методов может быть реализован либо программным, либо аппаратным способом.

Возможность программной реализации обуславливается тем, что все методы криптографического преобразования формальны и могут быть представлены в виде конечной алгоритмической процедуры.

При аппаратной реализации все процедуры шифрования и дешифрования выполняются специальными электронными схемами. Основным достоинством программных методов реализации защиты является их гибкость, т.е. возможность быстрого изменения алгоритмов шифрования.

Основным же недостатком программной реализации является существенно меньшее быстродействие по сравнению с аппаратными средствами (примерно в 10 раз).

В последнее время стали появляться комбинированные средства шифрования, так называемые программно-аппаратные средства. В этом случае в компьютере используется своеобразный “криптографический сопроцессор” - вычислительное устройство, ориентированное на выполнение криптографических операций (сложение по модулю, сдвиг и т.д.). Меняя программ-

ное обеспечение для такого устройства, можно выбирать тот или иной метод шифрования. Такой метод объединяет в себе достоинства программных и аппаратных методов.

Таким образом, выбор типа реализации криптозащиты информационной системы в существенной мере зависит от ее особенностей и должен опираться на всесторонний анализ требований, предъявляемых к системе защиты информации.

Ниже рассматривается программная реализация криптографических методов:

- метод Полибия;
- метод замены;
- умножение матриц.

П2.3. Метод Полибия

Шифровальная таблица представляла собой квадрат с пятью столбцами и пятью строками, которые нумеруются цифрами от 1 до 5. В каждую клетку такого квадрата записывалась одна буква. В результате каждой букве соответствовала пара чисел и шифрование сводится к замене буквы парой чисел.

Идею квадрата Полибия проиллюстрируем таблицей с русскими буквами (Табл. П2.1). Число букв в русском алфавите отличается от числа букв в греческом алфавите, поэтому и размер таблицы выбран иным (не квадрат 5х5,а прямоугольник 8х4).

Таблица П2.1

№	1	2	3	4	5	6	7	8
1	А	Б	В	Г	Д	Е	Ж	З
2	И	Й	К	Л	М	Н	О	П
3	Р	С	Т	У	Ф	Х	Ц	Ч
4	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я

Зашифруем фразу: КРИПТОГРАФИЯ:

23 31 21 28 33 27 14 31 11 35 11 35 21 48

В данном примере видно, что в шифрограмме первым указывается номер строки, а вторым – номер столбца.

Задание

1. Заполнить прямоугольник Полибия, в котором нужно отобразить все буквы русского алфавита от *а* до *я* и от *А* до *Я* плюс символы пробел, точка, двоеточие, восклицательный знак, вопросительный знак и запятая (всего 72 символа).
2. Методом Полибия зашифровать любую фразу, введенную с клавиатуры.
3. Расшифровать полученную в пункте 2 зашифрованную строку.

П.2.4. Метод замены

Шифрование методом замены (подстановки) основано на алгебраической операции, называемой подстановкой.

Подстановкой называется взаимно однозначное отображение некоторого конечного множества M на себя. Число N элементов этого множества называется степенью подстановки. Природа множества M роли не играет, поэтому можно считать, что M={1,2,...,N}.

Если при данной подстановке S число j переходит в I_j, то подстановка обозначается символом

$$S=\begin{bmatrix} 1 & 2 & . & . & n \\ I_1 & I_2 & . & . & I_n \end{bmatrix}$$

В этой записи числа $1,2,..,n$ можно произвольным образом переставлять, соответственно переставляя числа $I_1, I_2, .., I_n$.

Идею метода замены проиллюстрируем Таблицей П2.2 с русскими буквами

Таблица П2.2

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17

Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33

Основным недостатком рассмотренного метода является то, что статистические свойства открытого текста (частоты повторения букв) сохраняются в шифротексте.

Общая формула моноалфавитной замены выглядит следующим образом:

$$Y_i = k_1 \cdot X_i + k_2 (\mathrm{mod}\, n),$$

где Y_i - i-й символ алфавита; k_1 и k_2 - константы, X_i -i-й символ открытого текста (номер буквы в алфавите); n-длина используемого алфавита.

Шифр, задаваемый формулой:

$$Y_i = X_i + k_i (\mathrm{mod}\, n),$$

где k_i - i-ая буква ключа, в качестве которого используются слово или фраза, называется шифром Вижинера.

Пример

Открытый текст: "*ЗАМЕНА*".
Ключ: "*КЛЮЧ*".

$$Y_1 = 9 + 12 (\mathrm{mod}\, 33) = 21 \rightarrow У$$
$$Y_2 = 1 + 13 (\mathrm{mod}\, 33) = 14 \rightarrow М$$
$$Y_3 = 14 + 32 (\mathrm{mod}\, 33) = 13 \rightarrow Л$$
$$Y_4 = 6 + 25 (\mathrm{mod}\, 33) = 31 \rightarrow Э$$
$$Y_5 = 15 + 12 (\mathrm{mod}\, 33) = 27 \rightarrow Щ$$
$$Y_6 = 1 + 13 (\mathrm{mod}\, 33) = 14 \rightarrow М$$

Зашифрованный текст имеет вид: "*УМЛЭЩМ*".

Задание

1. Заполнить таблицу П2.2 в массив, в котором должны храниться все буквы русского алфавита от *а* до *я* и от *А* до *Я* плюс символы пробел, точка, двоеточие, восклицательный знак, вопросительный знак и запятая (всего 72 символа).
2. Зашифровать любую фразу с любым ключом (фраза и ключ вводятся с клавиатуры) методом замены.
4. Расшифровать полученный шифротекст, используя тот же ключ.

П2.5. Умножение матриц

Метод умножения матриц использует преобразования вида:

$$Y_i = C \cdot X,$$

где

$$Y = \|y_1, y_2, ..., y_n\|,$$

$$C = \|C_{ij}\|,$$

$$X = \|x_1, x_2, ..., x_n\|.$$

Идею метода умножения матриц также можно проиллюстрировать таблицей с русскими буквами (табл. П2.2).

Пример

Открытый текст: "ПРИКАЗ" (согласно табл. П2.2 представим в виде
"17 18 10 12 01 09").
Полагаем, что матрица C имеет вид:

$$C = \begin{bmatrix} 1 & 3 & 2 \\ 2 & 1 & 5 \\ 3 & 2 & 1 \end{bmatrix}.$$

Процедура получения зашифрованного текста представлена ниже

$$Y_1 = \begin{bmatrix} 1 & 3 & 2 \\ 2 & 1 & 5 \\ 3 & 2 & 1 \end{bmatrix} \cdot \begin{bmatrix} 17 \\ 18 \\ 10 \end{bmatrix} = \begin{bmatrix} 91 \\ 102 \\ 97 \end{bmatrix},$$

$$Y_2 = \begin{bmatrix} 1 & 3 & 2 \\ 2 & 1 & 5 \\ 3 & 2 & 1 \end{bmatrix} \cdot \begin{bmatrix} 12 \\ 01 \\ 09 \end{bmatrix} = \begin{bmatrix} 33 \\ 70 \\ 47 \end{bmatrix}.$$

В результате шифрования открытого текста имеем: “91 102 97 33 70 47”.

Задание

1. Заполнить таблицу П2.2 в массив, в котором должны храниться все буквы русского алфавита от *а* до *я* и от *А* до *Я* плюс символы пробел, точка, двоеточие, восклицательный знак, вопросительный знак и запятая (всего 72 символа).
2. Зашифровать любое сообщение, введенное с клавиатуры, методом произведения матриц.
3. Определить какой должна быть матрица, чтобы зашифрованную фразу можно было расшифровать.
4. Расшифровать сообщение.

ПРИЛОЖЕНИЕ 3

Темы для индивидуальных заданий проектирования криптографических систем

Цель индивидуального задания состоит:

- в подготовке реферата по предложенной теме на основе анализа литературных данных и информации, содержащейся в Internet;
- в разработке программной реализации соответствующего предложенной теме шифра, цифровой подписи, хэш-функции или комплекса криптоалгоритмов;
- в подготовке отчета по проделанной работе, по форме приведенной в Приложении 2.

Ниже приведены темы индивидуальных заданий:

1. Стандарт симметричного шифрования данных DES.
2. Блочный шифр IDEA.
3. Блочный шифр ГОСТ.
4. Блочный шифр CAST.
5. Блочный шифр BLOWFISH.
6. Блочный шифр RC5.
7. Блочный шифр LUCIFER.
8. Блочный шифр MADRYGA.
9. Блочный шифр NewDES.
10. Блочный шифр FEAL.
11. Блочный шифр REDOC.
12. Блочный шифр LOKI.
13. Блочный шифр KHUFU.

14. Блочный шифр RC2.
15. Блочный шифр MMB.
16. Блочный шифр CA-1.1.
17. Блочный шифр SKIPJACK.
18. Блочный шифр SAFER.
19. Блочный шифр 3-WAY.
20. Блочный шифр CRAB.
21. Блочный шифр SXAL8/MBAL.
22. Блочный шифр RC4.
23. Блочный шифр SEAL.
24. Асимметричный ранцевый криптоалгоритм.
25. Асимметричный алгоритм шифрования данных RSA.
26. Асимметричный алгоритм шифрования данных ElGamal.
27. Асимметричный алгоритм шифрования данных Pohlig-Hellman.
28. Асимметричный алгоритм шифрования данных Rabin.
29. Асимметричный алгоритм шифрования данных McEliece
30. Асимметричный алгоритм шифрования данных LUC.
31. Алгоритм цифровой подписи с открытым ключом DSA.
32. Алгоритм цифровой подписи с открытым ключом ГОСТ.
33. Однонаправленная хэш-функция Snefru.
34. Однонаправленная хэш-функция *N*-хэш.
35. Однонаправленная хэш-функция MD4.
36. Однонаправленная хэш-функция MD5.
37. Алгоритм безопасного хэширования (Secure Hash Algorithm, SHA).
38. Однонаправленная хэш-функция RIPE-MD.
39. Однонаправленная хэш-функция HAVAL.
40. Криптосистема шифрования корреспонденции VeriSign.
41. Комплекс криптоалгоритмов Pretty Good Privacy (PGP).

Литература

1. Молдовян А.А., Молдовян Н.А., Советов Б.Я. Криптография. - Серия «Учебники для вузов. Специальная литература». - СПб.: Издательство «Лань», 2000, 224 с.
2. Петров А. А. Компьютерная безопасность. Криптографические методы защиты. – М.: ДМК, 2000, 448 с.
3. http://www.ssl.stu.neva.ru/psw/crypto.html – Перевод на русский язык книги: Schneier B. Applied Cryptography: Protocols, Algorithms, and Source Code in C. John Wiley& Sons, Inc. 1994; (Шнайер Брюс. Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке С, 2-е издание.)
4. Шеннон К. Э. Теория связи в секретных системах / В кн.: Шеннон К. Э. Работы по теории информации и кибернетике. М. : ИЛ., 1963. С. 333-402.
5. Виноградов И. М. Основы теории чисел. М.: Наука. 1981. 176 с.
6. Кнут Д. Э. Искусство программирования для ЭВМ. М.: Мир. Т. 2. 724 с.
7. Домарев В. В. Безопасность информационных технологий. Методика создания систем защиты. – Москва “Санкт-Петербург” Киев, 2002, 688 с.
8. Спицын В.Г., Столярова Н.А. Защита информации и информационная безопасность. Учеб. пособие. - Томск: Изд. ТПУ, 2003, 167 с.
9. Алгоритм ГОСТ 28147-89. http:// argosoft.webservis.ru/index.html
10. TeNeT Archive - **Pretty Good Privacy** http://iron.te.net.ua/cgi-bin/mkindex?/pub/unix/crypto/pgp
11. **Pretty Good Privacy** защищает информацию сети Internet http://wings.machaon.ru/digest/digest/preety.html