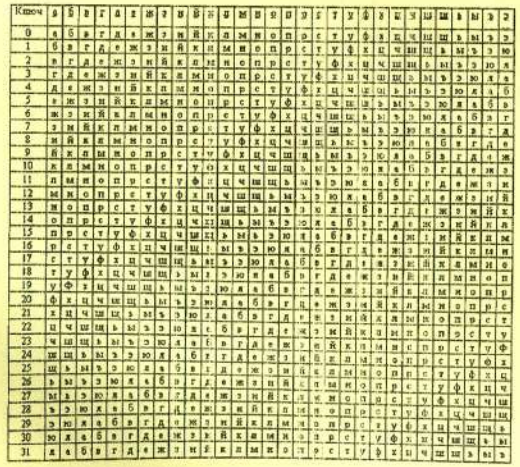
5611

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
РЯЗАНСКИЙ ГОСУДАРСТВЕННЫЙ РАДИОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
им. В.Ф. УТКИНА

ЗАЩИТА ИНФОРМАЦИИ

Методические указания
к лабораторным работам



Рязань 2020

УДК 621.396

Защита информации: методические указания к лабораторным работам /Рязан. гос. радиотехн. ун-т; сост.: С.Н. Кириллов, В.Т. Дмитриев. - Рязань, 2020. – 36 с.

Приведены методические указания к 3 лабораторным работам, посвященным изучению методов защиты информации и их разработке в программной среде MatLab. Первая лабораторная работа посвящена изучению шифров перестановки и методов их разработки. Вторая – изучению шифров замены и методов их разработки. Третья – изучению шифров гаммирования и их разработки.

Предназначены для студентов специальности 110501 «Радиоэлектронные системы и комплексы».

Табл. 9. Ил. 13. Библиогр.: 7 назв.

Защита информации, шифры гаммирования, шифры перестановки, шифры замены

Печатается по решению редакционно-издательского совета Рязанского государственного радиотехнического университета.

Рецензент: кафедра радиоуправления и связи Рязанского государственного радиотехнического университета (зав. кафедрой проф. С.Н. Кириллов)

Лабораторная работа № 1

ИЗУЧЕНИЕ ШИФРОВ ПЕРЕСТАНОВКИ И МЕТОДОВ ИХ РАЗРАБОТКИ В ПРОГРАММНОЙ СРЕДЕ MATLAB

ЦЕЛЬ РАБОТЫ

Изучение теоретического материала по шифрам перестановки по курсу «Основы криптографии». Приобретение практических навыков алгоритмизации и программирования шифров перестановки в среде MatLab.

1. ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

Шифры типа перестановки применялись еще с античных времен. Общая схема шифрования выглядит следующим образом: первый символ открытого текста заменяется i_1-м символом из этого же текста, второй – i_2-м и т.д. (табл. 1). Дешифрование производится аналогично в соответствии с табл. 1.

Таблица 1

1	2	3	4	…	N
I_1	i_2	i_3	i_4	…	i_n

Предположим, что номера букв открытого текста длиной в N знаков разбиты каким-либо способом на непересекающиеся множества $M_1,\ldots, M_r$.

Воздействуя на каждое множество M_i своей подстановкой (циклом) T_i, мы реализуем процесс зашифрования шифром перестановки, причем соответствующая шифропреобразованию подстановка равна $T_1,\ldots, T_r$ [2].

Изменяя разбиение множества индексов и выбирая различными способами соответствующие подстановки T_j', мы будем получать различные преобразования открытого текста вида $T'_1,\ldots, T'_s$. Причем рано или поздно мы построим все подстановки степени N, поскольку любая подстановка разлагается в произведение циклов. То же самое можно сказать и по отношению к некоторому иному, более

сложному процессу генерации подстановок, который, скажем, включает указанную процедуру в качестве одного из этапов.

Отсюда вытекает, что удачный способ генерации подстановок мог бы в принципе обеспечить достаточно качественный шифр перестановки, при котором использовались бы подстановки степени, меньшей, чем длина открытого текста. Последнее весьма важно, поскольку хранить и передавать ключи, длина которых равна длине открытого текста, в данном случае невыгодно (существуют намного более совершенные шифры с аналогичными требованиями) и, кроме того, невозможно зашифровать шифром перестановки текст, длина которого меньше степени соответствующей подстановки.

Для ручного использования таких шифров очень важными являются удобство зашифрования и легкость запоминания ключа. Именно способами генерации подстановок и различаются виды шифров перестановки.

Шифр вертикальной перестановки

Рассмотрим пример шифра вертикальной перестановки, для которого подстановка задается неявно с учетом так называемого ключевого слова - «лозунга» [2].

Открытый текст криптограммы следующий: *"В связи с создавшимся положением отодвигаем сроки возвращения домой Рамзай"*.

Для зашифрования шифром вертикальной перестановки построим прямоугольную таблицу, количество строк которой определяется длиной текста, а количество колонок равно шести. В качестве «лозунга» выберем слово "ЗАПИСЬ" (количество букв в ключевом слове должно равняться количеству колонок в нашей таблице).

Заменим теперь каждую букву ключевого слова на число от 1 до 6 таким образом, чтобы буква, имеющая меньший номер следования в алфавите, заменялась на меньшее число. Полученные числа (2,1,4,3,5,6) проставим подряд в начале соответствующих колонок таблицы и будем в дальнейшем считать их номерами этих колонок. Впишем открытый текст в таблицу, переходя обычным образом со строки на строку. В результате получим шифр, показанный на рис. 1.

2	1	4	3	5	6
в	с	в	я	з	и
с	с	о	з	д	а
в	ш	и	м	с	я
п	о	л	о	ж	е
н	и	е	м	о	т
о	д	в	и	г	а
е	м	с	р	о	к
и	в	о	з	в	р
а	щ	е	н	и	я
д	о	м	о	й	р
а	м	з	а	й	

Рис. 1. Таблица шифра вертикальной перестановки

Выпишем теперь буквы из столбцов таблицы: сначала весь столбец, в начале которого стоит единица, затем - столбец, помеченный двойкой, и т.д.

В итоге получим следующий шифртекст (представив его пятизначными группами знаков):

ссшои дмвщо мвсвп ноена даязм омирз ноаво илевс оемзз дсжог

овийй иаяет акряр.

Ясно, что шифртекст отличается от открытого текста лишь перестановкой букв, и мы, таким образом, совместили процесс генерации подстановок с процессом зашифрования.

В криптографической практике результат действия подстановки на последовательность номеров знаков открытого текста, являющуюся рядом чисел, указывающим место выбора очередных букв шифртекста из открытого текста, называется ***шкалой разноски***.

Нетрудно видеть, что для расшифрования, т.е. перестановки знаков шифртекста на исходное место, необходимо воспользоваться подстановкой, обратной шкале разноски, которая называется ***шкалой набора***.

В зависимости от частного вида закона построения шкалы разноски различают частные виды шифра перестановки - горизонтальную, вертикальную перестановки. В некоторых случаях шкала разноски строится как функция от двух независимых перестановок небольшой степени (двойная перестановка) или от перестановки и геометрической фигуры (так называемые шифры-решетки и лабиринты).

Шифр двойной перестановки

Для зашифрования двойной перестановкой [1] необходимо (рис. 2):

- построить таблицу, форматы которой определяются размерами двух ключевых слов (скажем, «гевара» и «риск»), выписываемых при этом сверху и сбоку таблицы;
- в таблицу по определенному маршруту (к примеру, «а») занести исходный текст (таблица а), а неиспользованные места полностью заполнить любыми, но лучше всего часто встречающимися буквами (здесь: с, в, и);
- переставить столбцы в порядке, соответствующем расположению букв в верхнем ключе («гевара»), как в шифре вертикальной перестановки (таблица б);
- аналогично переставить строки в соответствии с последовательностью букв второго ключевого слова («риск») в алфавите (таблица в);
- выписать построчно, начиная с первой строки, буквы из получившейся таблицы, разбивая их на пятизначные группы. Если последняя группа окажется неполной, то дописать ее любыми часто встречающимися буквами.

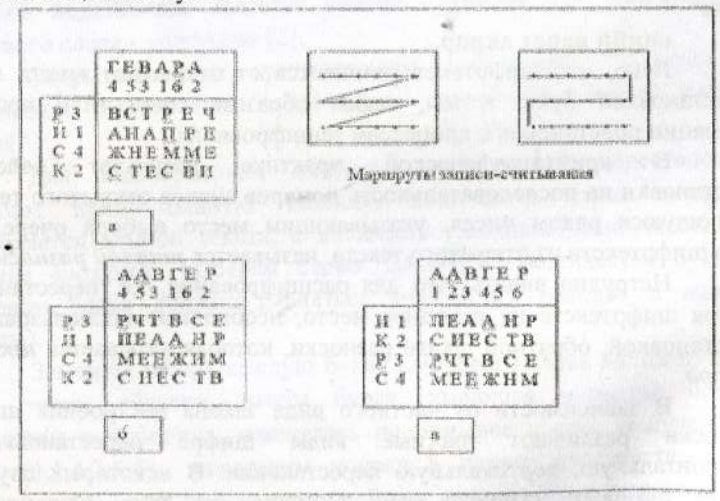


Рис. 2. Шифр двойной перестановки

Шифртекст - **ПЕААН РСИЕС ТВРЧТ ВСЕМЕ ЕЖНМИ**.

При расшифровывании криптограммы следует действовать в обратном порядке:

- шифртекст вписывается в таблицу, где столбцы и строки последовательно нумеруются, а избыток букв отбрасывается (так получается таблица в);
- строки располагают в соответствии с порядком номеров букв бокового ключевого слова (так получается таблица б);
- столбцы переставляются согласно нумерации букв верхнего ключа (так получается таблица а);
- буквы выписываются в строку, следуя обговоренному маршруту заполнения-чтения.

В заключение отметим, что зашифрование случайной, не обладающей закономерностями шкалой разноски при достаточно большой длине сообщения делает дешифрование такой криптограммы весьма проблематичным.

Шифр «Поворотная решетка»

Для использования данного шифра изготавливается трафарет из прямоугольного листа клетчатой бумаги размером 2m x 2k клеток [2], рис. 3. В трафарете вырезается m x k клеток так, чтобы при наложении его на чистый лист бумаги того же размера четырьмя возможными способами его вырезы полностью покрывали всю площадь листа. Буквы из сообщения последовательно вписываются в вырезы трафарета (по строкам слева направо) при каждом из четырех его возможных положений в заранее установленном порядке.

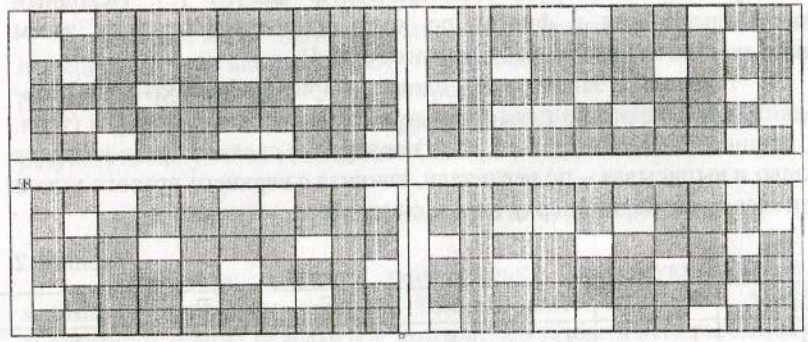


Рис. 3. Поворотная решетка

Пример шифрования текста. Зашифровать сообщение: “шифр решетка является частным случаем шифра маршрутной перестановки”. Наложив решетку на лист бумаги и поворачивая ее на

180 град. и на другую сторону в соответствии с рис. 4, вписываем буквы исходного сообщения, в результате получим следующий шифр (рис. 4).

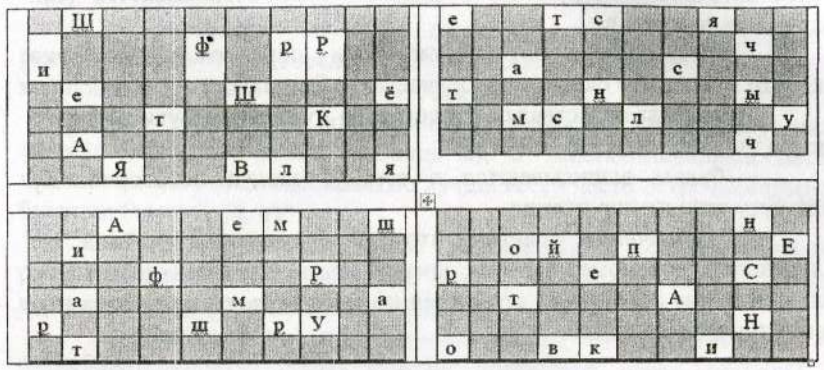


Рис. 4. Пример шифра «Поворотная решетка»

Здесь число возможных трафаретов (ключей шифра) составляет
4 m x k

Шифр маршрутной перестановки

Шифром маршрутной перестановки называется шифр, использующий некоторую геометрическую фигуру [2]. Исходный текст записывается в фигуру по ходу одного маршрута, а затем выписывается из него по ходу другого (рис. 4).

Пример. Зашифруем слово «Примермаршрутнойперестановки», вписывая его в прямоугольную таблицу по горизонтали (табл. 2), начиная с левого верхнего угла, поочередно слева направо и справа налево и выписывая – по вертикали, начиная с верхнего правого угла и двигаясь поочередно сверху вниз и снизу вверх.

Таблица 2

П	Р	И	М	Е	Р	М
Н	Т	У	Р	Ш	Р	А
О	Й	П	Е	Р	Е	С
И	К	В	О	Н	А	Т

Криптограмма будет иметь вид: МАСТАЕРРЕШРНОЕРМИУ-ПВКЙТРПНОИ.

Шифры перестановки с применением магических квадратов

Магическими квадратами называют квадратные таблицы с вписанными в их клетки последовательными натуральными числами, начиная от 1, которые дают в сумме по каждому столбцу, каждой строке и каждой диагонали одно и то же число (рис. 5).

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

О	И	Р	М
Е	О	С	Ю
В	Т	А	Ь
Л	Г	О	П

Рис. 5. Пример шифра перестановки
с применением магических квадратов

Шифруемый текст вписывается в квадрат в соответствии с нумерацией его клеток. Затем текст выписывается по строкам, в результате чего получается криптограмма.

Пример. Зашифруем фразу «ПРИЛЕТАЮВОСЬМОГО», в результате получится сообщение ОИРМЕОСЮВТАЬЛГОП.

«Общий метод» дешифрования шифра перестановки

Стойкость шифров перестановки напрямую связана с методами генерации ключей. Однако для этого типа шифров существуют общие недостатки, которые могут быть использованы для их дешифрования.

Прежде всего, статистика частот встречаемости знаков шифртекста совпадает со статистикой открытого текста независимо от

степени подстановки. Очевидно, длинные сообщения необходимо разбивать на блоки, соответствующие типичным длинам ключей (степеней подстановок).

Эти особенности позволяют определить тип шифра и ограничить возможные длины ключей по совокупности шифртекстов.

Кроме того, существует частный случай, позволяющий дешифровать комплект криптограмм одинаковой длины, зашифрованных одним ключом.

Для этого достаточно подписать криптограммы комплекта друг под другом и комбинировать колонки, получая читаемые сочетания в группе столбцов. Чем глубже колонки, тем легче подобрать текст.

Данный подход не зависит от сложности перестановки и по устаревшей терминологии называется общим (универсальным) методом дешифрования шифра перестановки.

2. ПРАКТИЧЕСКАЯ ЧАСТЬ

Основной целью практического занятия является приобретение практических навыков алгоритмизации и программирования шифров перестановки в среде MatLab. Перед началом работы необходимо изучить теоретический материал по шифрам перестановки, приведенный в методических указаниях к самостоятельным работам по курсу «Основы криптографии», ответить на контрольные вопросы, а также, используя литературу, освоить навыки работы и программирования в среде MatLab.

Занятие состоит из ознакомительной части с демонстрационным примером выполнения задания, где приведена программа шифрования сообщения с применением шифра вертикальной перестановки.

Выполнение задания осуществляется в соответствии с практической частью к занятию. При защите задания студентом составляется отчет, содержание которого должно удовлетворять требованиям, приведенным в разделе «Указания к составлению отчета».

Пример выполнения задания

Задание

С помощью шифра вертикальной перестановки разработать алгоритм и программу шифрования сообщения "Программное изделие" с ключевым словом «2 1 3 4 6 5 7» в среде MatLab.

Решение

Алгоритм шифрования сообщения будет осуществляться в такой последовательности.

1. Ввести исходные данные: ключевое слово – 2 1 3 4 6 5 7; текст открытого сообщения – программное изделие.
2. Определить размеры таблицы шифрования, учитывая при этом, что количество столбцов будет равняться длине ключевого слова.
3. Осуществить последовательную запись по строкам в таблицу шифрования текста открытого сообщения.
4. Осуществить перестановку столбцов таблицы в порядке возрастания чисел ключевого слова, т.е 1 2 3 4 5 6 7.
5. Осуществляя последовательное считывание сообщения по столбцам, получить криптограмму.
6. Конец алгоритма шифрования.

Программа в среде MatLab

```
% Пример шифра перестановки
T=[2 1 3 4 6 5 7]; % ключевое слово

T1='Программноеизделие'; % текст открытого сообщения

% Определение размера таблицы шифрования
TL1=length(T1); TL=length(T);
Vl=floor(TL1/TL); V2=TL1/TL;
P2=abs(V2-Vl); TT=0;
if P2<0.5
   TT=round(length(T1)/length(T))+1; % количество строк
таблицы
else
   TT=round(V2); % количество строк таблицы
end
```

```
% Запись исходного сообщения в таблицу шифрования
r=0;
for i=1:TT
   kh=0;
  for j=1:length(T)
     kh=j+r;
     if kh>length(T1)
        break
     else
       f(i,j)=T1(kh);
     end
  end
  r=r+length(T);
end

% Перестановка столбцов таблицы в порядке возрастания
чисел ключевого слова
for i=1:TT
for j=1:length(T);
   fd=findstr(T,j);
   kp(i,j)=f(i,fd);
end
end

% Последовательное считывание сообщения по столбцам
kpp=kp';
khh=0; r1=0;
for i=1:length(T)
  j=0;
  for j=1:length(deblank(kpp(i,:)))
      khh=j+r1;
    ff(khh)=kpp(i,j);
  end
  r1=r1+length(deblank(kpp(i,:)));
end
 C=ff % Криптограмма исходного сообщения
```

Практическая часть

Разработать алгоритм и программу шифрования сообщения в среде MatLab в соответствии с вариантом заданий (табл. 3).

Таблица 3

Вариант	Алгоритм
1	Шифр двойной перестановки
2	Шифр маршрутной перестановки (запись сообщения в таблицу – последовательное, построчное с возвращением к началу строки; считывание – последовательное по столбцам)
3	Шифр с применением магических квадратов
4	Шифр «Поворотная решетка»
5	Шифр маршрутной перестановки (запись сообщения в таблицу – последовательное, построчное; считывание – последовательное по столбцам)
6	Шифр «Поворотная решетка»
7	Шифр маршрутной перестановки (запись сообщения в таблицу – последовательное, построчное с возвращением к началу строки; считывание – последовательное по столбцам)
8	Шифр с применением магических квадратов
9	Шифр двойной перестановки
10	Шифр маршрутной перестановки (запись сообщения в таблицу – последовательное, построчное; считывание – последовательное по столбцам)
Примечание 1. Номер варианта задания соответствует номеру студенческой бригады. 2. Если число студенческих бригад превышает количество вариантов заданий, тогда 11-я бригада начинает выполнять вариант № 1 задания и т.д.	

Контрольные вопросы

1. Какие существуют способы защиты информации и в чем заключаются их особенности?
2. Как выглядит модель системы секретной связи, предложенная Шенноном?
3. Что такое симметричная криптографическая система?
4. В чем заключается практическая стойкость преобразования шифров?
5. Дайте определение следующим терминам: криптография, аутентичность, целостность информации, шифр, ключ.

6. Чем отличается криптография от криптоанализа?
7. Что такое шифр перестановки?
8. Приведите примеры шифров перестановки.
9. В чем заключается шифр вертикальной перестановки?
10. Каким образом записывается исходное сообщение в таблицу шифра маршрутной перестановки?
11. Как шифруется исходное сообщение при использовании шифра «Поворотная решетка»?
12. Что называется магическим квадратом?
13. Алгоритм шифрования сообщений шифра двойной перестановки.
14. Общий метод дешифрования шифров перестановки.
15. От чего зависит стойкость шифров перестановки?

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Бабаш А.В., Шанкин Г.П. Криптография / под ред. В.П. Шерстюка, Э.А. Применко. – М.: СОЛОН-ПРЕСС, 2007.
2. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях / под ред. В.Ф. Шаньгина. – М.: Радио и связь, 1999.

Лабораторная работа № 2

ИЗУЧЕНИЕ ШИФРОВ ЗАМЕНЫ И МЕТОДОВ ИХ РАЗРАБОТКИ В ПРОГРАММНОЙ СРЕДЕ MATLAB

ЦЕЛЬ РАБОТЫ

Изучение теоретического материала по шифрам замены по курсу «Основы криптографии».

Приобретение практических навыков алгоритмизации и программирования шифров перестановки в среде MatLab.

1. ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

Шифрами простой замены являются шифры, где каждый символ исходного сообщения заменяется символами того же алфавита, одинаково на всем протяжении. Примерами шифра простой замены являются: шифр Цезаря, Полибианский квадрат, шифрующие таблицы Трисемуса, система омофонов и т.д.

Шифр Цезаря [2]. Свое название шифр получил по имени римского императора Гая Юлия Цезаря, который использовал его при переписке с Цицероном (около 50 г. до н.э.). Шифр основан на замене каждой буквы открытого сообщения, расположенной в алфавите на *K* позиций правее, чем исходная. При выходе за пределы алфавита соответствующий знак шифртекста выбирался из второго алфавита, записанного вслед за первым.

Совокупность возможных подстановок для K = 3 приведена в табл. 4.

Таблица 4

A → D	J → M	S → V
B → E	K → N	T → W
C → F	L → O	U → X
D → G	M → P	V → Y
E → H	N → Q	W → Z
F → I	O → R	X → A
G → J	P → S	Y → B
H → K	Q → T	Z → C
I → L	R → U	

Так, известное послание Цезаря VENI VIDI VICI (в переводе на русский – «Пришел, увидел, победил») в зашифрованном виде выглядит следующим образом: YHQL YLGL YLFL.

Полибианский квадрат [1]. Данный шифр был разработан в Древней Греции (II в. до н. э.) полководцем и историком Полибием. Здесь для шифрования использовался квадрат размером 5x5 клеток (рис. 6), в который выписываются все буквы латинского алфавита, при этом буквы I,J не различаются (J отождествляется с буквой I). Шифруемая буква открытого сообщения заменяется на координаты квадрата, в котором она записана. Так, B заменяется на AB, F на BA, R на DB и т.д. При расшифровании каждая такая пара определяет соответствующую букву сообщения. Ключом такого шифра является расположение букв в таблице 5x5.

	A	B	C	D	E
A	A	B	C	D	E
B	F	G	H	I	K
C	L	M	N	O	P
D	Q	R	S	T	U
E	V	W	X	Y	Z

Рис. 6. Квадрат Полибия

В качестве примера зашифруем слово «LOVE». Зашифрованное сообщение будет иметь вид CACDEAAE.

Шифрующие таблицы Трисемуса [1]. В 1508 г. аббат из Германии Иоганн Трисемус написал печатную работу по криптологии под названием "Полиграфия". В этой книге он впервые систематически описал применение шифрующих таблиц, заполненных алфавитом в случайном порядке. Для получения такого шифра замены обычно использовались таблица для записи букв алфавита и ключевое слово (или фраза). В таблицу сначала вписывалось по строкам ключевое слово, причем повторяющиеся буквы отбрасывались. Затем эта таблица дополнялась не вошедшими в нее буквами алфавита по порядку.

Поскольку ключевое слово или фразу легко хранить в памяти, то такой подход упрощал процессы шифрования и расшифрования. Поясним этот метод шифрования на примере. Для русского алфавита

шифрующая таблица может иметь размер 4x8. Выберем в качестве ключа слово БАНДЕРОЛЬ. Шифрующая таблица с таким ключом показана на рис. 7.

Б	А	Н	Д	Е	Р	О	Л
Ь	В	Г	Ж	З	И	Й	К
М	П	С	Т	У	Ф	Х	Ц
Ч	Ш	Щ	Ы	Ъ	Э	Ю	Я

Рис. 7. Шифрующая таблица Трисемуса
с ключевым словом «Бандероль»

При шифровании находят в этой таблице очередную букву открытого текста и записывают в шифртекст букву, расположенную ниже ее в том же столбце. Если буква текста оказывается в нижней строке таблицы, тогда для шифртекста берут самую верхнюю букву из того же столбца.

Например, при шифровании с помощью таблицы Трисемуса (рис. 7) сообщения «ВЫЛЕТАЕМПЯТОГО» получим шифртекст «ПДКЗЫВЗЧШЛЫЙСЙ».

Система омофонов [2] обеспечивает простейшую защиту от криптоаналитических атак, основанных на подсчете частот появления букв в шифртексте. Система омофонов является одноалфавитной, хотя при этом буквы исходного сообщения имеют несколько замен. Число замен берется пропорциональным вероятности появления буквы в открытом тексте. Данные о распределениях вероятностей букв в русском тексте приведены в табл. 5.

Здесь буквы в таблицах указаны в порядке убывания вероятности их появления в тексте.

Шифруя букву исходного сообщения, выбирают случайным образом одну из ее замен. Замены (часто называемые омофонами) могут быть представлены трехразрядными числами от 000 до 999. Например, в английском алфавите букве E присваиваются 123 случайных номера, буквам B и G - по 16 номеров, а буквам J и Z - по 1 номеру. Если омофоны (замены) присваиваются случайным образом различным появлениям одной и той же буквы, тогда каждый омофон появляется в шифртексте равновероятно.

Таблица 5

i	Символ	P(i)	i	Символ	P(i)	i	Символ	P(i)
1		0.175	12	Л	0.035	23	Б	0.014
2	О	0.090	13	К	0.028	24	Г	0.012
3	Е	0.072	14	М	0.026	25	Ч	0.012
4	Е	0.072	15	Д	0.025	26	Й	0.010
5	А	0.062	16	П	0.023	27	Х	0.009
6	И	0.062	17	У	0.021	28	Ж	0.007
7	Т	0.053	18	Я	0.018	29	Ю	0.006
8	Н	0.053	19	Ы	0.016	30	Ш	0.006
9	С	0.045	20	З	0.016	31	Ц	0.004
10	Р	0.040	21	Ь	0.014	32	Щ	0.003
11	В	0.038	22	Ъ	0.014	33	Э	0.003
						34	Ф	0.002

При таком подходе к формированию шифртекста простой подсчет частот уже ничего не дает криптоаналитику. Однако в принципе полезна также информация о распределении пар и троек букв в различных естественных языках. Если эту информацию использовать при криптоанализе, он будет проведен более успешно.

Шифры сложной замены называют многоалфавитными, так как для шифрования каждого символа исходного сообщения применяют свой шифр простой замены [1]. Многоалфавитная подстановка последовательно и циклически меняет используемые алфавиты.

При r-алфавитной подстановке символ x_0 исходного сообщения заменяется символом y_0 из алфавита B_0, символ x_1 - символом y_1 из алфавита B_1 и так далее, символ x_{r-1} заменяется символом y_{r-1} из алфавита B_{r-1}, символ x_r заменяется символом y_r снова из алфавита B_0 и т.д.

Общая схема многоалфавитной подстановки для случая r = 4 показана на рис. 8.

Входной символ	X_0	X_1	X_2	X_3	X_4	X_5	X_6	X_7	X_8	X_9
Алфавит подстановки	B_0	B_1	B_2	B_3	B_0	B_1	B_2	B_3	B_0	B_1

Рис. 8. Схема r-алфавитной подстановки для случая r = 4

Эффект использования многоалфавитной подстановки заключается в том, что обеспечивается маскировка естественной статистики исходного языка, так как конкретный символ из исходного

алфавита А может быть преобразован в несколько различных символов шифровальных алфавитов B_j. Степень обеспечиваемой защиты теоретически пропорциональна длине периода r в последовательности используемых алфавитов B_j.

Многоалфавитные шифры замены предложил и ввел в практику криптографии Леон Батист Альберти, который также был известным архитектором и теоретиком искусства. Его книга "Трактат о шифре", написанная в 1566 г., представляла собой первый в Европе научный труд по криптологии. Кроме шифра многоалфавитной замены, Альберти также подробно описал устройства из вращающихся колес для его реализации. Криптологи всего мира считают Л. Альберти основоположником криптологии.

Примерами шифров сложной замены являются: шифр Гронсфельда, система шифрования Вижинера, шифр «двойной квадрат» Уитстона и др.

Шифр Гронсфельда [2]. Этот шифр сложной замены, называемый шифром Гронсфельда, представляет собой модификацию шифра Цезаря числовым ключом. Для этого под буквами исходного сообщения записывают цифры числового ключа. Если ключ короче сообщения, то его запись циклически повторяют. Шифртекст получают примерно, как в шифре Цезаря, но отсчитывают по алфавиту не третью букву (как это делается в шифре Цезаря), а выбирают ту букву, которая смещена по алфавиту на соответствующую цифру ключа. Например, применяя в качестве ключа группу из четырех начальных цифр числа e (основания натуральных логарифмов), а именно 2718, получаем для исходного сообщения ВОСТОЧНЫЙ ЭКСПРЕСС шифртекст, показанный на рис. 9.

Сообщение	В	О	С	Т	О	Ч	Н	Ы	Й	Э	К	С	П	Р	Е	С	С
Ключ	2	7	1	8	2	7	1	8	2	7	1	8	2	7	1	8	2
Шифртекст	Д	Х	Т	Ь	Р	Ю	О	Г	Л	Д	Л	Щ	С	Ч	Ж	Щ	У

Рис. 9. Шифр Гронсфельда

Чтобы зашифровать первую букву сообщения В, используя первую цифру ключа 2 , нужно отсчитать вторую по порядку букву от В в алфавите, в результате чего получается первая буква шифр-текста – Д.

Система шифрования Вижинера [1]. Является одной из старейших и наиболее известных многоалфавитных систем. Свое

название она получила по имени французского дипломата XVI века Блеза Вижинера, который развивал и совершенствовал криптографические системы.

Система Вижинера подобна такой системе шифрования Цезаря, у которой ключ подстановки меняется от буквы к букве. Этот шифр многоалфавитной замены можно описать таблицей шифрования, называемой таблицей (квадратом) Вижинера. На рис.10 приведена таблица Вижинера для русского алфавита.

Ключ	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э
0	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э
1	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю
2	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я
3	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а
4	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б
5	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в
6	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г
7	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д
8	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е
9	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж
10	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з
11	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и
12	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й
13	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к
14	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л
15	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м
16	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н
17	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о
18	т	у	ф	х	ц	ч	ш	щ	ь	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п
19	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р
20	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с
21	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т
22	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у
23	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф
24	ш	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х
25	щ	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц
26	ь	ы	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч
27	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш
28	ъ	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ
29	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь
30	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы
31	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ

Рис.10. Таблица Вижинера для русского алфавита

Таблица Вижинера используется для зашифрования и расшифрования. Таблица имеет два входа:

• верхнюю строку подчеркнутых символов, используемую для считывания очередной буквы исходного открытого текста;

• крайний левый столбец ключа.

Последовательность ключей обычно получают из числовых значений букв ключевого слова.

При шифровании исходного сообщения его выписывают в строку, а под ним записывают ключевое слово (или фразу). Если ключ оказался короче сообщения, то его циклически повторяют. В процессе шифрования находят в верхней строке таблицы очередную букву исходного текста и в левом столбце очередное значение ключа. Очередная буква шифртекста находится на пересечении столбца, определяемого шифруемой буквой, и строки, определяемой числовым значением ключа.

Рассмотрим пример получения шифртекста с помощью таблицы Вижинера. Пусть выбрано ключевое слово АМБРОЗИЯ. Необходимо зашифровать сообщение ПРИЛЕТАЮ СЕДЬМОГО.

Выпишем исходное сообщение в строку и запишем под ним ключевое слово с повторением. В третью строку будем выписывать буквы шифртекста, определяемые из таблицы Вижинера (рис. 11).

Сообщение	П	Р	И	Л	Е	Т	А	Ю	С	Е	Д	Ь	М	О	Г	О
Ключ	А	М	Б	Р	О	З	И	Я	А	М	Б	Р	О	З	И	Я
Шифртекст	П	Ъ	Й	Ы	У	Щ	И	Э	С	С	Е	К	Ь	Х	Л	Н

Рис. 11. Пример шифра Вижинера

Шифр "двойной квадрат" Уитстона [2]. Свое название этот шифр получил по аналогии с полибианским квадратом. Шифр Уитстона открыл новый этап в истории развития криптографии. В отличие от полибианского шифр "двойной квадрат" использует сразу две таблицы, размещенные по одной горизонтали, а шифрование идет биграммами, как в шифре Плейфейра. Эти не столь сложные модификации привели к появлению на свет качественно новой криптографической системы ручного шифрования. Шифр "двойной квадрат" оказался очень надежным и удобным и применялся Германией даже в годы второй мировой войны.

Поясним процедуру шифрования этим шифром на примере. Пусть имеются две таблицы со случайно расположенными в них русскими алфавитами (рис.12). Перед шифрованием исходное сообщение разбивают на биграммы. Каждая биграмма шифруется отдельно. Первую букву биграммы находят в левой таблице, а вторую букву - в правой таблице. Затем мысленно строят прямоугольник так, чтобы буквы биграммы лежали в его противоположных вершинах. Другие две вершины этого прямоугольника дают буквы биграммы шифртекста.

Ж	Щ	Н	Ю	Р
И	Т	Ь	Ц	Б
Я	М	Е	.	С
В	Ы	П	Ч	
:	Д	У	О	К
З	Э	Ф	Г	Ш
Х	А	,	Л	Ъ

И	Ч	Г	Я	Т
,	Ж	Ь	М	О
З	Ю	Р	В	Щ
Ц	:	П	Е	Л
Ъ	А	Н	.	Х
Э	К	С	Ш	Д
Б	Ф	У	Ы	

Рис. 12. Таблицы для шифра "двойной квадрат" Уитстона

Предположим, что шифруется биграмма исходного текста ИЛ. Буква И находится в столбце 1 и строке 2 левой таблицы. Буква Л находится в столбце 5 и строке 4 правой таблицы. Это означает, что прямоугольник образован строками 2 и 4, а также столбцами 1 левой таблицы и 5 правой таблицы. Следовательно, в биграмму шифртекста входят буква О, расположенная в столбце 5 и строке 2 правой таблицы, и буква В, расположенная в столбце 1 и строке 4 левой таблицы, т.е. получаем биграмму шифртекста ОВ.

Если обе буквы биграммы сообщения лежат в одной строке, то и буквы шифртекста берут из этой же строки. Первую букву биграммы шифртекста берут из левой таблицы в столбце, соответствующем второй букве биграммы сообщения. Вторая же буква биграммы шифртекста берется из правой таблицы в столбце, соответствующем первой букве биграммы сообщения. Поэтому биграмма сообщения ТО превращается в биграмму шифртекста ЖБ. Аналогичным образом шифруются все биграммы сообщения.

Сообщение ПР ИЛ ЕТ АЮ _Ш ЕС ТО ГО.

Шифртекст ПЕ 0В ЩН ФМ ЕШ РФ БЖ ДЦ.

Шифрование методом "двойного квадрата" дает весьма устойчивый к вскрытию и простой в применении шифр. Взламывание шифртекста "двойного квадрата" требует больших усилий, при этом длина сообщения должна быть не менее тридцати строк.

2. ПРАКТИЧЕСКАЯ ЧАСТЬ

Пример выполнения работы

Задание. С помощью шифра Цезаря разработать программу шифрования и расшифрования сообщения “Отлично” с ключевым словом $K = 3$ в среде MatLab.

Решение

Алгоритм шифрования сообщения будет осуществляться в такой последовательности.

1. Ввести исходные данные: массив символов русского алфавита, текст открытого сообщения, значение ключевого слова *N*.

2. Определить номер позиции *r* *i*-го символа сообщения в русском алфавите.

3. Определить новую позицию *k* для *i*-го символа зашифрованного сообщения следующим образом:

$$k = \begin{cases} r + N & при\ (r+N) \le l \\ (r+N) - l & при (r+N) > l, \end{cases}$$

где l - длина алфавита.

4. Заменить *i*-й символ позиции *r* на символ позиции *k*.

5. Если значение *i*-го символа равно длине открытого сообщения, тогда перейти к пункту 6, иначе - перейти к пункту 2.

6. Конец алгоритма шифрования.

Алгоритм дешифрования сообщения будет осуществляться в такой последовательности.

1. Ввести исходные данные: массив символов русского алфавита, текст криптограммы (зашифрованного сообщения), значение ключевого слова *N*.

2. Определить номер позиции *k* *i*-го символа криптограммы в русском алфавите.

3. Определить позицию *r* для *i*-го символа исходного открытого сообщения следующим образом:

$$r = \begin{cases} k - N & при\ (k-N) \le l, \\ (k-N) - l & при\ (k-N) > l. \end{cases}$$

4. Заменить *i*-й символ позиции *k* на символ позиции *r*.

5. Если значение *i*-го символа равно длине криптограммы, тогда перейти к пункту 6, иначе - перейти к пункту 2.

6. Конец алгоритма расшифрования.

Программа в среде MatLab

```
% Пример шифра Цезаря
% Ввод исходных данных
s='абвгдежзийклмнопрстуфхцчшщъыьэюя';
```

```
s1='отлично';
N=3; % ключевое слово
len=length(s);
% Зашифрование сообщения шифром Цезаря
for i=1:length(s1)
   r(i)=findstr(s,s1(i));
   rr(i)=r(i)+N;
   if rr(i)>len
      ssh(i)=s(rr(i)-len);
   else
      ssh(i)=s(rr(i));
   end
end
ss=ssh; % криптограмма
% Расшифрование сообщения
%for i=1:length(ss)
 %  rp(i)=findstr(s,ss(i));
  % rrp(i)=rp(i)-3;
   % sshp(i)=s(rrp(i));
   %end
  rcp=rr-N;  % Расшифрованное сообщение
sshp=s(rcp)
% сравнение исходного сообщения и расшифрованного
if strcmp(s1,ssh)==1
    fprintf('Расшифровка прошла успешно')
   else
    fprintf('Расшифровка прошла неправильно')
   end
```

Разработать алгоритм и программу шифрования сообщения в среде MatLab в соответствии с вариантом заданий (табл. 6).

Таблица 6

Буква	Вероятность	Буква	Вероятность	Буква	Вероятность	Буква	Вероятность
Пробел	0,175	Р	0,040	Я	0,018	Х	0,009
О	0,090	В	0,038	Ы	0,016	Ж	0,007
Е	0,072	Л	0,035	З	0,016	Ю	0,006
А	0,062	К	0,028	Ъ	0,014	Ш	0,006
И	0,062	М	0,026	Б	0,014	Ц	0,004
Н	0,053	Д	0,025	Г	0,013	Щ	0,003
Т	0,053	П	0,023	Ч	0,012	Э	0,003
С	0,045	У	0,021	Й	0,010	Ф	0,002

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Что такое шифр Цезаря?
2. Что такое Полибианский квадрат?
3. В чём заключается принцип с шифрование с помощью таблиц Трисемуса?
4. В чём заключается отличие шифра Гросфельда от шифра Цезаря?
5. В чём заключаются преимущества многоалфавитных систем шифрования над одноалфавитными?
6. Объясните процедуру шифрования шрифтом Уинстона.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях.-М.: Кудиц-образ, 2001. – 368 с.

2. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях / Под ред. В.Ф. Шаньгина – М.: Радио и связь, 1999 .

Лабораторная работа № 3

ИЗУЧЕНИЕ ШИФРОВ ГАММИРОВАНИЯ И МЕТОДОВ ИХ РАЗРАБОТКИ В ПРОГРАММНОЙ СРЕДЕ MATLAB

ЦЕЛЬ РАБОТЫ

Изучение теоретического материала по шифрам гаммирования по курсу «Основы криптографии». Приобретение практических навыков алгоритмизации и программирования шифров гаммирования в среде MatLab.

1. ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

Основные положения

В основе шифров гаммирования лежит метод наложения по определенному закону гаммы шифра на открытые данные.

Гамма шифра – это псевдослучайная последовательность, выработанная по заданному алгоритму для зашифрования открытых данных и расшифрования зашифрованных данных, схема шифрования методом гаммирования приведена на рис. 13.

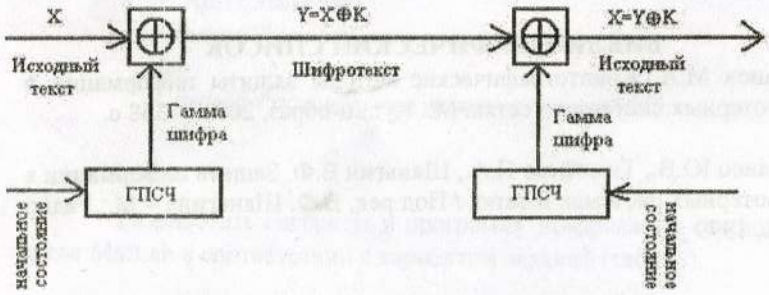


Рис. 13. Схема шифрования методом гаммирования

Принцип шифрования заключается в формировании генератором псевдослучайных чисел (ГПСЧ) гаммы шифра и наложении этой гаммы на открытые данные обратимым

образом, например путем сложения по модулю два. Процесс дешифрования данных сводится к повторной генерации гаммы шифра и наложению гаммы на зашифрованные данные. Ключом шифрования в данном случае является начальное состояние генератора псевдослучайных чисел. При одном и том же начальном состоянии ГПСЧ будет формировать одни и те же псевдослучайные последовательности.

Перед шифрованием открытые данные обычно разбивают на блоки одинаковой длины, например по 64 бита. Гамма шифра также вырабатывается в виде последовательности блоков той же длины.

Стойкость шифрования методом гаммирования определяется главным образом свойствами гаммы – длиной периода и равномерностью статистических характеристик. Последнее свойство обеспечивает отсутствие закономерностей в появлении различных символов в пределах периода. Полученный зашифрованный текст является достаточно трудным для раскрытия. По сути дела, гамма шифра должна изменяться случайным образом для каждого шифруемого блока.

Обычно разделяют две разновидности гаммирования – с конечной и бесконечной гаммами. При хороших статистических свойствах гаммы стойкость шифрования определяется только длиной периода гаммы. При этом если длина периода гаммы превышает длину шифруемого текста, то такой шифр теоретически является абсолютно стойким, т.е. его нельзя вскрыть с помощью статистической обработки зашифрованного текста, а можно раскрыть только прямым перебором. Криптостойкость в этом случае определяется размером ключа.

В шифрах гаммирования может использоваться сложение по модулю N (общий случай) и по модулю 2 (частный случай, ориентированный на программно-аппаратную реализацию).

Сложение по модулю N

$$C_i = (P_i + K_i) \bmod N, \quad (1)$$

$$P_i = (C_i + N - K_i) \bmod N, \quad (2)$$

где P_i, C_i - i-й символ открытого и шифрованного сообщения;
N –количество символов в алфавите;
K_i - i-й символ гаммы (ключа).

Данные формулы позволяют выполнить зашифрование / расшифрование по Виженеру при замене букв алфавита числами согласно табл. 7 (применительно к русскому алфавиту):

Таблица 7

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32

Например, для шифрования используется русский алфавит (N = 33), открытое сообщение – «АБРАМОВ», гамма – «ЖУРИХИН». При замене символов на числа буква **А** будет представлена как 0, **Б** – 1, …, **Я** – 32. Результат шифрования показан в табл. 8.

Таблица 8

Символ								
Открытого сообщения, P_i	А	Б	Р	А	М	О	В
	0	1	17	0	13	15	2
Гаммы, K_i	Ж	У	Р	И	Х	И	Н
	7	20	17	9	22	9	14
Шифрограммы, C_i	Ж	Ф	Б	И	В	Ч	П
	7	21	1	9	2	24	16

Сложение по модулю 2

При данном способе шифрования символы текста и гаммы представляются в двоичном виде, а затем каждая пара двоичных разрядов складывается по модулю 2. Процедуры шифрования и дешифрования выполняются по следующим формулам:

$$C_i = P_i \oplus K_i, \quad (3)$$

$$P_i = C_i \oplus K_i. \quad (4)$$

С развитием средств телекоммуникаций и вычислительной техники открытые сообщения обычно

представляются в виде последовательностей битов, полученных после замены знаков исходного алфавита сообщения на их битовые эквиваленты в соответствующей кодировке [например, кодировке в соответствии со стандартным американским кодом обмена информацией ASCII (табл. 9, [1])]. При этом сложение сообщения с гаммой шифром осуществляется по модулю 2.

Таблица 9

Символ	Десятичное представление	Двоичное представление	Символ	Десятичное представление	Двоичное представление
А	128	10000000	Р	144	10010000
Б	129	10000001	С	145	10010001
В	130	10000010	Т	146	10010010
Г	131	10000011	У	147	10010011
Д	132	10000100	Ф	148	10010100
Е	133	10000101	Х	149	10010101
Ж	134	10000110	Ц	150	10010110
З	135	10000111	Ч	151	10010111
И	136	10001000	Ш	152	10011000
Й	137	10001001	Щ	153	10011001
К	138	10001010	Ъ	154	10011010
Л	139	10001011	Ы	155	10011011
М	140	10001100	Ь	156	10011100
Н	141	10001101	Э	157	10011101
О	142	10001110	Ю	158	10011110
П	143	10001111	Я	159	10011111

Перед шифрованием исходные открытые данные разбивают на блоки $T_0^{(i)}$ одинаковой длины (обычно по 64 бита). Гамма шифров вырабатывается в виде последовательности блоков $Г_ш^{(i)}$ аналогичной длины.

Уравнение зашифрования можно записать как

$$T_ш^{(i)} = (Г_ш^{(i)} \oplus T_0^{(i)}) mod 2,\ i=1...M, \quad (5)$$

где $T_ш^{(i)}$ – *i-й* блок шифртекста; $Г_ш^{(i)}$ – *i-й* блок гаммы шифра; $T_0^{(i)}$ – *i-й* блок открытого текста; М – количество блоков открытого текста.

Процесс расшифрования сводится к повторной генерации гаммы шифра и наложению этой гаммы на зашифрованные данные. Уравнение расшифрования имеет вид

$$T_0^{(i)} = (Г_ш^{(i)} \oplus T_ш^{(i)}) mod 2,\ i=1...M. \quad (6)$$

Получаемый этим методом шифртекст достаточно труден для раскрытия, поскольку теперь ключ является переменным, так как гамма шифра должна изменяться случайным образом для каждого шифруемого блока. Если период гаммы превышает длину всего шифруемого сообщения, то такой шифр можно раскрыть только прямым перебором всех вариантов ключа. В этом случае криптостойкость шифра определяется длиной ключа.

К достоинствам шифров гаммирования следует отнести следующее.

1. Возможность достижения высоких скоростей шифрования.
2. Коэффициент размножения ошибки равен единице.
3. Поточность шифрования и расшифрования.
4. Сохранение размера текста при шифровании.

К недостаткам относятся следующие

1. Нестойкость шифра при повторном использовании ключа.
2. Последовательность доступа к информации.

Методы генерации гаммы шифра

На практике для генерации гаммы шифра (псевдослучайной последовательности) широкое распространение получили генераторы псевдослучайных чисел (ПСЧ) следующих видов:

- конгруэнтные генераторы;
- мультипликативный генератор.

Конгруэнтные генераторы. Генераторы данного вида являются наиболее доступными и эффективными. Для них можно сделать математически строгое заключение о том, какими свойствами обладают выходные сигналы этих генераторов с точки зрения периодичности и случайности.

Одним из наиболее распространенных конгруэнтных генераторов является **линейный конгруэнтный генератор** ПСЧ. Он вырабатывает последовательности псевдослучайных чисел Y_i, описываемые соотношением:

$$Y_i = (a^* Y_{i-1} + b)\ mod\ m, \quad (7)$$

где Y_i – текущее значение ПСЧ; Y_{i-1} – предыдущее значение ПСЧ; a – множитель; b – приращение.

Такой генератор формирует псевдослучайные числа с периодом повторения, зависящим от выбранных значений a и b. Значение m обычно устанавливается равным $2n$, где n - длина машинного слова в битах. Генератор имеет максимальный период m до того, как генерируемая последовательность начнет повторяться. По причине, отмеченной ранее, необходимо выбирать числа a и b такие, чтобы период m был максимальным. Как ранее было показано Д. Кнутом, линейный конгруэнтный генератор ПСЧ имеет максимальную длину m тогда и только тогда, когда b - нечетное и $a\ mod\ 4 = 1$.

Мультипликативный генератор. Вырабатывает ПСЧ с помощью соотношения вида:

$$Y_i = (a^* Y_{i-1})\ mod\ m. \quad (8)$$

Требования к значениям констант a и m такие же, как и для линейного конгруэнтного генератора.

Общий алгоритм шифрования и дешифрования методом гаммирования

Алгоритм зашифрования открытого сообщения методом гаммирования выполняется в следующей последовательности.

1. Осуществить инициализацию генератора ПСЧ.
2. Каждый символ открытого сообщения перевести в числовую форму, например, используя табл. 3.
3. Выделить блок открытого сообщения.
4. Сгенерировать гамму шифра, используя выражение (3) или (4).
5. Сложив блок открытого сообщения с гаммой шифра в соответствии с выражением (1), получить блок зашифрованного текста.
6. Если текст закончился, перейти к пункту 7, иначе – к пункту 2.
7. Конец алгоритма.

Алгоритм дешифрования криптограммы методом гаммирования выполняется в такой последовательности.

1. Осуществить инициализацию генератора ПСЧ.
2. Выделить блок криптограммы.
3. Сгенерировать гамму шифра, используя выражение (3) или (4).
4. Сложив блок криптограммы с гаммой шифра в соответствии с выражением (2), получить блок открытого сообщения.
5. Полученное открытое сообщение в числовой форме перевести в символ (символы), например, используя табл. 3.
6. Если текст закончился, перейти к пункту 7, иначе – к пункту 2.
7. Конец алгоритма.

2. ПРАКТИЧЕСКАЯ ЧАСТЬ

Основной целью практического занятия является приобретение практических навыков алгоритмизации и программирования шифров перестановки в среде MatLab. Перед началом работы необходимо изучить теоретический материал по шифрам перестановки, приведенный в методических указаниях к самостоятельным работам по курсу «Основы криптографии», ответить на контрольные вопросы, а также,

используя литературу, освоить навыки работы и программирования в среде MatLab.

Занятие состоит из ознакомительной части с демонстрационным примером выполнения задания, где приведена программа шифрования сообщения с применением шифра вертикальной перестановки.

Выполнение задания осуществляется в соответствии с практической частью к занятию. При защите задания студентом составляется отчет, содержание которого должно удовлетворять требованиям, приведенным в разделе «Указания к составлению отчета».

Пример выполнения задания

Задание. С помощью шифра гаммирования разработать алгоритм и программу шифрования и расшифрования текста открытого сообщения «Юла». Для формирования гаммы шифра использовать линейный конгруэнтный генератор с исходным значением порождающего числа $Y_0 = 203$, $b = 3$, m=256, $a = 5$ (согласно условию $a \bmod 4 = 1$). При переводе каждого значения символа текста открытого сообщения в двоичный вид использовать код ASCII (табл. 9). Предполагается также, что все сообщение состоит из одного блока.

Решение

Алгоритм шифрования сообщения будет осуществляться в такой последовательности.

1. Введем исходные данные для формирования гаммы шифра: $Y_0 = 203$, $b = 3$, m=256.

2. В соответствии с таблицей кодов ASCII (табл. 9) каждый символ открытого сообщения «Юла» переведем в двоичный вид, в результате получится последовательность 100111101000101110000000.

3. Выделим блок открытого сообщения, который в соответствии с условиями задачи будет равен целому сообщению, т.е. 100111101000101110000000.

4. Используя выражение для линейного конгруэнтного генератора, сгенерируем гамму шифра:

$Y_1 = (a^* Y_0 + b) \bmod m = (5*203+3) \bmod 256 = 250 = (11111010)_2;$
$Y_2 = (a^* Y_1 + b) \bmod m = (5*250+3) \bmod 256 = 229 = (11100101)_2;$
$Y_3 = (a^* Y_2 + b) \bmod m = (5*229+3) \bmod 256 = 124 = (01111100)_2.$

Таким образом, гамма шифра имеет вид: 111110101110010101111100.

5. Вычислим криптограмму, сложив блок открытого сообщения с гаммой шифра по модулю 2:

```
10011110100010111000000 открытое сообщение
⊕
11111010111001010111100 гамма шифра
-----------------------
01100100011011011111100 - криптограмма (зашифрованное
                           сообщение)
```

6. Конец алгоритма.

Алгоритм дешифрования сообщения будет осуществляться в такой последовательности.

1. Введем исходные данные для формирования гаммы шифра: $Y_0 = 203$, $b = 3$, $m=256$.

2. Выделим блок криптограммы, полученный в результате шифрования сообщения: 011001000110111011111001.

3. Используя выражение для линейного конгруэнтного генератора, сгенерируем гамму шифра:

$Y_1 = (a^* Y_0 + b) \bmod m = (5*203+3) \bmod 256 = 250 = (11111010)_2;$
$Y_2 = (a^* Y_1 + b) \bmod m = (5*250+3) \bmod 256 = 229 = (11100101)_2;$
$Y_3 = (a^* Y_2 + b) \bmod m = (5*229+3) \bmod 256 = 124 = (01111100)_2.$

Таким образом, гамма шифра имеет вид: 111110101110010101111100.

4. Вычислим текст открытого сообщения, сложив блок криптограммы с гаммой шифра по модулю 2:

```
01100100011011011111100 криптограмма
⊕
11111010111001010111100 гамма шифра
-----------------------
10011110100010111000000 открытое сообщение
```

5. В соответствии с таблицей кодов ASCII (табл. 9) получим открытое сообщение «Юла».

6. Конец алгоритма.

Программа в среде MatLab

```
% Пример шифра гаммирования
% Ввод исходных данных
Y0=203; a=5; b=3; m=256; % Параметры генератора
s='юла'; % Текст открытого сообщения
% Перевод текста открытого сообщения в числовой вид
  s1=[158 139 128];
  s2=[10011110 10001011 10000000]; % Сообщение в
двоичном виде
% Генерирование гаммы шифра
 Y(1)=Y0;
  for I=2:length(S1)+1
    Y(I)=mod((a*Y(I-1)+b),m);
    Y1(I-1)=Y(I);
  end
 Y2=dec2bin(Y1); % Гамма шифра в двоичном виде
% Вычисление криптограммы
C=bitxor(s1,Y1);
C1=dec2bin(C); % Криптограмма в двоичном виде
% Дешифрование сообщения
C2=bitxor(C,Y1);
% Проверка дешифрованного сообщения
if s1==C2
```

```
fprintf('Расшифровка прошла успешно!')
else
  fprintf('Расшифровка прошла неверно!')
end
```

Контрольные вопросы

1. Что такое гамма шифра?
2. В чем заключается процесс зашифрования открытого сообщения методом гаммирования?
3. Как осуществляется шифрование текста открытого сообщения, представленного двоичными символами?
4. Каким образом символы открытого сообщения могут быть заменены на числа?
5. Как осуществляется процесс расшифрования криптограммы методом гаммирования?
6. Чем определяется криптостойкость шифра гаммирования в случае, если период гаммы превышает длину всего шифруемого сообщения?
7. Какие существуют методы генерации гаммы-шифра?
8. Как формируется псевдослучайная последовательность чисел при использовании линейного конгруэнтного генератора?
9. Каким образом можно добиться максимального периода повторения псевдослучайных чисел в случае линейного конгруэнтного генератора?
10. Как формируется псевдослучайная последовательность чисел при использовании мультипликативного генератора?
11. В какой последовательности выполняется алгоритм зашифрования открытого сообщения методом гаммирования?
12. В какой последовательности выполняется алгоритм дешифрования открытого сообщения методом гаммирования?
13. Каким образом можно увеличить криптографическую стойкость шифра гаммирования?
14. Опишите алгоритм зашифрования открытого сообщения шифром гаммирования, состоящего из одного блока.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. [Электронный ресурс] – http://www.ascii.org.ru.
2. [Электронный ресурс]- https://www.sites.google.com/site/anisimovkhv/learning/kripto/lecture/tema6
3. https://studopedia.ru/11_46239_shifrovanie-metodom-gammirovaniya.html

Содержание

Защита информации

Составители: К и р и л л о в Сергей Николаевич

Д м и т р и е в Владимир Тимурович

Редактор М.Е. Цветкова

Корректор Р.К. Мангутова

Подписано в печать 25.07.20. Формат бумаги 60x84 1/16.

Бумага писчая. Печать трафаретная. Усл. печ. л. 2,25.

Тираж 50 экз. Заказ 3856

Рязанский государственный радиотехнический университет.

390005, Рязань, ул. Гагарина, 59/1.

Редакционно-издательский центр РГРТУ.