ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

«ВСЕРОССИЙСКАЯ ГОСУДАРСТВЕННАЯ НАЛОГОВАЯ АКАДЕМИЯ МИНИСТЕРСТВА ФИНАНСОВ РОССИЙСКОЙ ФЕДЕРАЦИИ»

Е.Н. Каширская

Информационная безопасность

Защита информационных процессов в компьютерных системах

Учебно-методическое пособие по выполнению практических и лабораторных работ

Москва 2011

РЕЦЕНЗЕНТЫ:

Каширская Е.Н.
Информационная безопасность. Защита информационных процессов в компьютерных системах: Учебно-методическое пособие по выполнению лабораторных работ. – М.: ВГНА Минфина России, 2011. – 145 с.

В учебно-методическом пособии рассмотрены вопросы организации систем криптографической защиты информации с использованием как симметричных криптоалгоритмов, так и методов шифрования с открытым ключом. Задачи защиты информации, решаемые программными средствами, находят применение в самых различных сферах производственной и предпринимательской деятельности, и знакомство выпускников ВГНА с методами решения подобных задач повышает их профессиональный уровень и делает их более привлекательными в качестве потенциальных работников, независимо от полученной специализации. Учебно-методическое пособие предназначено для студентов, обучающихся по специальности «Комплексная защита объектов информатизации», по направлениям «Информационная безопасность», «Инфокоммуникационные технологии и системы связи», а также для студентов, обучающихся по специальности «Прикладная информатика (в экономике)» и по направлению «Прикладная информатика».

СОДЕРЖАНИЕ

1 СИММЕТРИЧНЫЕ КРИПТОАЛГОРИТМЫ

По мере развития и усложнения средств, методов и форм автоматизации процессов обработки информации повышается зависимость общества от степени безопасности используемых им информационных технологий, которая определяется степенью защищенности и устойчивости как компьютерных систем в целом, так и отдельных программ.

Для обеспечения защиты информации в настоящее время не существует какого-то одного технического приема или средства, однако общим в решении многих проблем безопасности является использование криптографии и криптоподобных преобразований информации.

Симметричные алгоритмы представляют собой алгоритмы, в которых ключ шифрования может быть рассчитан по ключу дешифрирования и наоборот. В большинстве симметричных систем ключи шифрования и дешифрирования одни и те же. Эти алгоритмы также называют алгоритмами с секретным ключом или алгоритмами с одним ключом. Для работы такой системы требуется, чтобы отправитель и получатель согласовали используемый ключ перед началом безопасной передачи сообщения (имели защищенный канал для передачи ключа). Безопасность симметричного алгоритма определяется ключом, таким образом, раскрытие ключа дает возможность злоумышленнику шифровать и дешифрировать все сообщения.

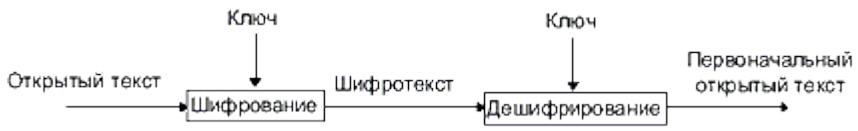


Рисунок 1 – Схема симметричного шифрования

Из-за большой избыточности естественных языков в зашифрованное сообщение трудно внести осмысленные изменения, поэтому помимо защиты информации обеспечивается защита от навязывания ложных данных. Если же естественная избыточность недостаточна, то используется специальная контрольная комбинация - имитовставка.

Так как используется один ключ, то каждый из участников обмена может зашифровывать и дешифрировать сообщения, поэтому данная схема шифрования работает на взаимном доверии. Если его нет, то могут возникать различные коллизии, так как при возникновении какого-либо спора по поводу достоверности сообщения, независимый наблюдатель не может сказать кем из участников было отправлено сообщение.

Симметричные алгоритмы делятся на две категории. Одни из них обрабатывают текст побитно (иногда побайтно) и называются потоковыми алгоритмами или **потоковыми** шифрами; те же, которые работают с группами битов открытого текста, называются **блочными** алгоритмами (шифрами).

Шифры появились на свет задолго до изобретения компьютера. Получившие широкое распространение криптографические алгоритмы выполняли либо замену одних букв на другие, либо переставляли буквы друг с другом. Самые стойкие шифры делали одновременно и то, и другое, причем многократно.

1.1 Перестановочные шифры

В шифре перестановки буквы открытого текста не замещаются на другие, а меняется сам порядок их следования. Например, в шифре простой колонной перестановки исходный открытый текст записывается построчно (число букв в строке фиксировано), а шифртекст получается считыванием букв по колонкам. Расшифрование производится аналогично: шифртекст записывается поколонно, а открытый текст можно затем прочесть по горизонтали.

Самым известным шифром перестановки является шифр Сцитала (или шифр Древней Спарты), переставляющий буквы сообщения таким образом, что исходное сообщение можно получить, лишь читая шифровку через k букв по модулю длины шифровки. Сам же процесс шифровки происходил следующим образом - на цилиндр (сциталу) наматывали тонкую полоску пергамента и писали на ней, после размотки на ленте образовывалась шифровка, расшифровать которую можно было только намотав эту ленту на такую же сциталу.

Для повышения стойкости полученный шифртекст можно подать на вход второго шифра перестановки. Существуют еще более сложные шифры перестановки, однако почти все они легко взламываются с помощью компьютера.

Хотя во многих современных криптографических алгоритмах и используется перестановка, ее применение ограничено узкими рамками, поскольку в этом случае требуется память большого объема, а также накладываются ограничения на длину шифруемых сообщений. Замена получила значительно большее распространение.

Задание. Расшифруйте перевод сообщения, переданного спартанцу в V веке до н. э. (шифр Сцитала): НУЗРАПААСАВТЙТ.

1.1.1 Простой столбцевой перестановочный шифр

В данном виде шифра текст пишется на горизонтально разграфленном листе бумаги фиксированной ширины, а шифротекст считывается по вертикали. Дешифрирование заключается в записи шифротекста вертикально на листе разграфленной бумаги фиксированной ширины и затем считывании открытого текста горизонтально. Открытый текст: ВСЕРОССИЙСКАЯ ГОСУДАРСТВЕННАЯ НАЛОГОВАЯ АКАДЕМИЯ

```
В С Е Р О С
С И Й С К А
Я   Г О С У
Д А Р С Т В
```

Е Н Н А Я
Н А Л О Г О
В А Я А К
А Д Е М И Я

Зашифрованный текст: ВСЯДЕНВАСИ АНААДЕЙГРНЛЯЕРСОСАО МОКСТЯГАИСАУВ ОКЯ

Задание. Зашифровать с помощью простой столбцевой перестановки фразу «*Неясное становится еще более непонятным*». Ключом в этом случае служит размер таблицы из 5 строк и 7 столбцов. Затем расшифровать полученную криптограмму.

1.1.2 Перестановочный шифр с ключевым словом

Буквы открытого текста записываются в клетки прямоугольной таблицы по ее строчкам. Буквы ключевого слова пишутся над столбцами и указывают порядок этих столбцов (по возрастанию номеров букв в алфавите). Чтобы получить зашифрованный текст, надо выписывать буквы по столбцам с учетом их нумерации.

Открытый текст: Прикладная математика

Ключ: Шифр

Ш	и	ф	р
4	1	3	2
П	р	и	к
л	а	д	н
а	я	м	а
т	е	м	а
т	и	к	а

Криптограмма: Раяеикнаааидммкплатт

Ключевое слово (последовательность столбцов) известно адресату, который легко сможет расшифровать сообщение.

Задание. С помощью ключа «ЛУНАТИК» зашифровать фразу «*Неясное становится еще более непонятным*». Применить таблицу из 6 строк и 7 столбцов. Затем расшифровать полученную криптограмму.

Для обеспечения дополнительной скрытности можно повторно шифровать сообщение, которое уже было зашифровано. Для этого размер второй таблицы подбирают так, чтобы длины ее строк и столбцов отличались от длин строк и столбцов первой таблицы. Лучше всего, если они будут взаимно простыми.

1.1.3 Шифрование с помощью магических квадратов

В средние века для шифрования применялись и магические квадраты. Магическими квадратами называются квадратные таблицы с вписанными в их клетки последовательными натуральными числами, начиная с единицы, которые дают в сумме по каждому столбцу, каждой строке и каждой диагонали одно и то же число. Для шифрования необходимо вписать исходный текст по приведенной в квадрате нумерации и затем переписать содержимое таблицы по строкам. В результате получается шифротекст, сформированный благодаря перестановке букв исходного сообщения.

Например, зашифруем фразу «ПРИЕЗЖАЮ ШЕСТОГО». Для этого сначала пронумеруем символы:

П	Р	И	Е	З	Ж	А	Ю	_	Ш	Е	С	Т	О	Г	О
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Затем составим магический квадрат и впишем в него буквы в соответствии с нумерацией:

16	3	2	13		О	И	Р	Т
5	10	11	8		З	Ш	Е	Ю
9	6	7	12		_	Ж	А	С
4	15	14	1		Е	Г	О	П

Теперь перепишем содержимое символьного магического квадрата по строкам:

ОИРТЗШЕЮ_ЖАСЕГОП

1.1.4 Двойная перестановка столбцов и строк

Кроме алгоритмов одиночных перестановок применяются алгоритмы двойных перестановок. Сначала в таблицу записывается текст сообщения, а потом поочередно переставляются столбцы, а затем строки. При расшифровке порядок перестановок был обратный. Пример данного метода шифрования показан в следующем примере:

	2	4	1	3			1	2	3	4			1	2	3	4
4	П	Р	И	Е		4	И	П	Е	Р		1	А	З	Ю	Ж
1	З	Ж	А	Ю		1	А	З	Ю	Ж		2	Е	_	С	Ш
2	_	Ш	Е	С		2	Е.	_	С	Ш		3	Г	Т	О	О
3	Т	О	Г	О		3	Г	Т	О	О		4	И	П	Е	Р

В результате перестановки получена шифровка АЗЮЖЕ_СШГТООИПЕР. Ключом к шифру служат номера столбцов 2413 и номера строк 4123 исходной таблицы.

Число вариантов двойной перестановки достаточно быстро возрастает с увеличением размера таблицы: для таблицы 3x3 их 36, для 4x4 их 576, а для 5x5 их 14400.

Так как символы криптотекста те же, что и в открытом тексте, то частотный анализ покажет, что каждая буква встречается приблизительно с той же частотой, что и обычно. Это дает криптоаналитику информацию о том, что это перестановочный шифр. Применение к криптотексту второго перестановочного фильтра значительно повысит безопасность. Существуют и еще более сложные перестановочные шифры, но с применением компьютера можно раскрыть почти все из них.

1.1.5 Перестановка по случайному ключу в MS Excel

Создадим шифр с длиной ключа, равной, например, 30. Для этого нам понадобится любой компьютер с установленным на нем MS Excel.

Сначала надо настроить параметры листа Excel. Установите стиль ссылок R1C1. Для этого выберите в главном меню пункт «Сервис» - «Параметры...» и на вкладке «Общие» выберите «Стиль ссылок» R1C1. После этого надо уменьшить ширину столбцов листа. (ля этого выделите весь лист, выберите в главном меню пункт «Формат» - «Столбец» - «Ширина...» и задайте значение, равное 2.

Теперь можно начинать шифрование. В ячейку R1C1 введите исходный текст.

В ячейки R2C1, ..., R2C30 второй строки введите в произвольном порядке все целые числа от 1 до 30. Эта случайная перестановка чисел и является ключом.

В ячейку R3C1 введите формулу =ПСТР(R1C1;R2C;1).

Введите ту же формулу и в ячейки R3C2, ..., R3C30. Это можно сделать одним легким движением мыши: выделив ячейку R3C1, устанавливаем курсор на маленький черный квадрат в углу этой ячейки и тянем вправо до ячейки R3C30.

В 3-й строке получаем зашифрованный текст (по одной букве в 30 ячейках).

Если в ячейку R1C1 ввести другой исходный текст, то в 3-й строке автоматически появится новый шифртекст.

Для того чтобы обмениваться с кем-нибудь секретной информацией, вам надо скрытно передать этому лицу (до начала взаимодействия) выбранный вами секретный ключ. Получатель на своем компьютере должен аналогично вам настроить параметры листа Excel своего файла и ввести полученный ключ в ячейки R1C1, ..., R1C30.

Расшифровка криптограммы выполняется следующим образом. Зашифрованный текст вводится посимвольно в ячейки R2C1, ..., R2C30 второй строки непосредственно под ключом.

Выделяется диапазон ячеек, в которых записаны ключ и символы шифртекста (для этого надо протащить указатель от ячейки R1C1 к R2C30).

Выделенный диапазон копируется.

Щелкнув правой кнопкой мыши на ячейке R4C1, выбираем из появившегося контекстного меню команду «Специальная вставка...».

В появившемся диалоговом окне «Специальная вставка» устанавливается флажок «транспонировать» и нажимается кнопка OK.

Вставленный диапазон ячеек сортируется (для этого надо, не снимая выделения с указанного диапазона ячеек, щелкнуть кнопку «Сортировка по возрастанию» на панели инструментов «Стандартная»).

Во второй колонке сверху вниз (начиная с 4-й строки) можно прочесть расшифрованный текст.

Рассмотренный шифр классифицируется как блочный шифр простой перестановки с длиной блока N=30 и длиной ключа, равной 30.

Если в вашем исходном тексте количество символов больше N, то надо предварительно разбить его на блоки по N символов в каждом и затем шифровать каждый блок в отдельности. То же относится и к расшифровке.

Криптостойкость созданного шифра. Учитывая, что количество перестановок из 30 символов равно 30! = 265252859812191058636308480000000, можно было бы предположить, что полный перебор на таком множестве ключей невозможен, потому что, если опробовать каждый возможный ключ, когда в течение каждой секунды проверяется миллиард ключей, это заняло бы 8*1015 лет! Тем не менее, современные методы криптоанализа позволяют вскрыть многие шифры, и не перебирая всех возможных комбинаций. Вообще говоря, очень трудно придумать шифр, который нельзя было бы вскрыть другим более эффективным способом (одним из таких способов является метод грубой физической силы).

Если вы хотите, чтобы ваш шифр очень сложно было взломать, надо:

• чаще менять ключ (желательно, каждый сеанс);

• не допускать перехвата ключа;

• не оставлять на винчестере или съемном носителе копию исходного текста;

• защитить компьютер от вирусов, троянских коней и тому подобного;

• вводить исходный текст без пробелов, в одном регистре (только верхнем или только нижнем).

Вскрывать ваши криптограммы будет сложно еще и в том случае, если у вас по орфографии была двойка.

В соответствии с «правилом Керкхоффа», сформулированным еще в XIX веке, секретность шифров должна быть основана не на секретности алгоритма, а на секретности ключа. Иными словами, правило Керкхоффа состоит в том, что весь механизм шифрования, кроме значения секретного ключа, известен криптоаналитику противника.

1.1.6 Случайная перестановка символов

Задание. Зашифруйте строку текста случайной перестановкой символов. При шифровании не забудьте сохранить вектор перестановки, чтобы строку можно было расшифровать!

1.1.7 Перестановка букв в середине слова

В файле содержится русскоязычный текст без переносов слов, зашифрованный по следующему алгоритму: первая и последняя буква каждого слова остаются на месте, а все остальные переписываются в обратном порядке. Например, слово «картофель» было бы заменено на слово «клефотрь».

Задание. Напишите программу для расшифровки закодированного файла. Результат работы программы сохраняйте в файле, имя которого начинается с префикса "new_" и завершается именем входного файла. Например, при расшифровке текста, содержащегося в файле tmp.txt, выходной файл должен называться new_tmp.txt. Ниже приводится пример зашифрованного текста. Сохраните его в файле и приступайте к раскодированию.

```
Винамине! Через ондо зитянае (на вомьсом по стечу)
нстенчая пкревора Вишах зинанй, так нымеавызай, рынжебуй
клортноь. Ннжуо бедут в кссале втинлопыь нуротокею ртобау
по мкитаметае и нуротокею ртобау по икитамрофне. За
куджаю ртобау Вы птеачулое ооннеледерпе члсио боллав.
Елси ныннарбае Вмаи бллаы пюашыверт зунтечаю гцинару, то
зичант Вы слади эту тмеу. В понвиторм сачуле, Вам
пстедиря птавыледереь ртобау свона и свона, до тех пор,
пкоа тмеа не бедут снада. Мкитаметаа и икитамрофна
зстюавытичсая оньледто дург от дгура. Уохепсв!
```

1.2 Подстановочные шифры (шифры замены)

Хотя многие современные алгоритмы используют перестановку, с этим связана проблема использования большого объема памяти, а также иногда требуется работа с сообщениями определенного размера. Поэтому чаще используют подстановочные шифры.

В подстановочных шифрах буквы исходного сообщения заменяются на подстановки. Замены в криптотексте расположены в том же порядке, что и в оригинале. Если использование замен постоянно на протяжение всего текста, то криптосистема называется одноалфавитной (моноалфавитной). В многоалфавитных системах использование подстановок меняется в различных частях текста.

Рассмотрим схему шифрования методом простой подстановки. Работа по шифрованию информации этим методом начинается с составления таблицы шифрования. Первый столбец этой таблицы состоит из всех символов

исходного текста. Во втором столбце записываются символы, которыми символы исходного текста будут заменяться. Каждый символ исходного текста заменяется одним символом. Следует заметить, что каждый символ замены можно использовать только один раз, то есть если, например, символ «р» заменяет символ «а», то он больше не может заменять ни один другой символ.

После того как каждому символу исходного алфавита поставлен в соответствие символ замены, получаем таблицу шифрования, на основании которой и производится шифрование.

Шифрование включает в себя зашифрование, то есть перевод открытого текста в зашифрованный вид, и расшифрование - восстановление исходного текста по его зашифрованному представлению. Оба действия используют одну и ту же таблицу шифрования.

Зашифрование информации методом простой подстановки производится следующим образом. Берется первый символ из шифруемого текста. Этот символ отыскивается в первом столбце таблицы шифрования. Символ, стоящий справа от выбранного символа, является шифром первого символа. Далее берется второй символ и с ним проделывается то же самое до тех пор, пока не будет зашифрован весь исходный текст. После проведения таких операций с каждым символом исходного текста мы получим зашифрованный текст.

Расшифрование происходит аналогичным образом с использованием той же самой таблицы шифрования. Выбирается первый символ зашифрованного текста. Этот символ ищется среди символов замены во втором столбце таблицы шифрования. Символ, стоящий в первом столбце строки, в которой находится найденный символ, и будет символом исходного (расшифрованного) текста. Такая же операция проводится с каждым символом зашифрованного текста. После ее проведения над всеми символами зашифрованного текста получим расшифрованный текст.

Процесс дешифрования информации, зашифрованной методом простой подстановки, заключается в определении таблицы шифрования, использовавшейся при зашифровании данной информации, и расшифровании информации по полученной таблице.

Шифром замены называется алгоритм шифрования, который производит замену каждой буквы открытого текста на какой-то символ шифрованного текста. Получатель сообщения расшифровывает его путем обратной замены.

В классической криптографии различают 4 разновидности шифров замены.

Простая замена, или одноалфавитный шифр. Каждая буква открытого текста заменяется на один и тот же символ шифртекста.

Омофонная замена аналогична простой замене с единственным отличием: каждой букве открытого текста ставятся в соответствие несколько символов шифртекста. Например, буква «А» заменяется на цифру 5, 13, 25 или 57, а буква «Б» — на 7, 19, 31 или 43 и так далее.

Блочная замена. Шифрование открытого текста производится блоками. Например, блоку «АБА» может соответствовать «РТК», а блоку «АББ» — «СЛЛ».

Многоалфавитная замена состоит из нескольких шифров простои замены. Например, могут использоваться пять шифров простой замены, а какой из них конкретно применяется для шифрования данной буквы открытого текста, — зависит от ее положения в тексте.

1.2.1 Шифр Цезаря

Юлий Цезарь повествует о посылке зашифрованного сообщения Цицерону. Используемая при этом система подстановок была одноалфавитной, но не являлась системой Цезаря: латинские буквы заменялись на греческие способом, который не был ясен из рассказа Цезаря. Информация о том, что Цезарь действительно использовал систему Цезаря, пришла от Светония.

В шифре Цезаря каждая буква замещается на букву, находящуюся k символами правее, по модулю, равному количеству букв в алфавите. Если буква кодируемой фразы имеет в алфавите позицию j, то она в «шифровке» будет заменяться буквой, находящейся в алфавите на позиции $j + k$ (согласно Светонию, у Цезаря k=3, n=50):

$$C_k(j) = (j + k) \bmod n,$$

где n - количество букв в алфавите.

Очевидно, что обратной подстановкой является

$$C_k^{-1}(j) = C_{n-k} = (j + n - k) \bmod n.$$

Задание. Зашифруйте описанным методом известную фразу Юлия Цезаря «VENI VIDI VICI» – *пришел, увидел, победил*. Задайте смещение на 4 символа. Потом расшифруйте полученную криптограмму.

Задание. Расшифруйте сообщение: ТУЛЫИО, ЦЕЛЖЗО, ТСДЗЖЛО!

1.2.2 Шифры Полибия

Система Цезаря не является старейшей. Возможно, что наиболее древней из известных является система греческого историка Полибия, умершего за 30 лет до рождения Цезаря. Его суть состоит в следующем: рассмотрим прямоугольник, часто называемый доской Полибия. Верхняя строка и левый столбец могут содержать буквы или цифры.

Каждая буква может быть представлена парой букв, указывающих строку и столбец, в которых расположена данная буква (или аналогично парой цифр). Так, представления букв В, Г, П, У будут АВ, АГ, ВГ, ГБ соответственно, а сообщение ПРИКЛАДНАЯ МАТЕМАТИКА зашифруется как

ВГВДБВБДБЕАААДВБААЕБЕЕВАААГААЕВАААГАБВБДААЕЕ.

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

При шифровании текстов, написанных латиницей, используется квадрат Полибия, имеющий размерность 5x5, а буквы I и J считаются одной и той же буквой.

Есть еще несколько вариантов шифрования, придуманных Полибием. Вот один из них. Полибием за 100 лет до н.э. был изобретен так называемый полибианский квадрат размером 5x5, заполненный алфавитом в случайном порядке. Греческий алфавит имеет 24 буквы, а 25-м символом является пробел. Для шифрования на квадрате находили букву текста и записывали в шифротекст букву, расположенную ниже ее в том же столбце. Если буква оказывалась в нижней строке таблицы, то брали верхнюю букву из того же столбца.

Задание. Расшифруйте сообщение на русском языке (алфавит содержит 33 буквы, пробел, восклицательный и вопросительный знаки). Доска Полибия имеет размерность 6x6.

6364433216626436111234421142546445224443634326564116442556 6

1.2.3 Шифрование методом Атбаш

Атбаш можно считать шифром сдвига на всю длину алфавита или того числа символов, которые представлены к замене. Это простая замена для двух статических алфавитов.

Возьмем два алфавита, один из которых написан наоборот:

АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ

ЯЮЭЬЫЪЩШЧЦХФУТ С Р ПОНМЛКЙИ ЗЖЁ Е ДГВ Б А

Вы видите, взаимное соответствие букв, которые заменяют друг друга.

Закодировать сообщение этим шифром очень простою

Возьмем текст: *ШИРОКОЕ ПОЛЕ*

Получаем перевод:*ЖЦОРФРЪ ПРУЪ*

Название Атбаш и само даёт подсказку, как работает этот шифр. В еврейском алфавите слово «атбаш» состоит из двух первых и двух последних букв алфавита: алеф(а), таб(т), бет(б), шин(ш).

Шифр Атбаш был использован в Библии, в Ветхом завете. Там есть кпоминание о царе Сесаха, хотя такой страны не существовало. На самом деле, это защиврованное название Вавилона - Сесах (или Шешах).

На иврите Вавилон пишется буквами «бет», и «ламед» (на английском это beth, beth и lamed, что соответствует согласным буквам в слове Babel - Вавилон). При шифровании Атбашем вторая в алфавите буква «бет» заменяется предпоследней в алфавите буквой «шин» (shin), а двенадцатая с начала буква «ламед» - двенадцатой с конца буквой «каф». Таким образом, после всех переводов с языка на язык было выяснено, что в тексте Библии слово Сесах (Шешах) обозначает Вавилон.

Правило зашифрования состоит в замене *i*-ой буквы алфавита буквой с номером *n* - *i* + 1, где *n* - число букв в алфавите. Для дешифрования сообщения нужно просто повторно применить к нему этот же алгоритм.

Функция, шифрующая строку методом Атбаш, имеет вид:

```
function Atbash(toCode: string): string;
var i: integer;
begin
  for i := 1 to length(toCode) do
    toCode[ i ] := Chr(256 - Ord(toCode[ i ]));
  Atbash := toCode;
end;

{ Использование: }
var
  s: string;

begin
  s := Atbash('Just a test'); { зашифровать }
  writeln(s);
  writeln('s = ', Atbash(s)); { расшифровать }
end.
```

Для дешифрования сообщения нужно просто повторно применить к нему этот же алгоритм.

Задание. Расшифруйте текст, зашифрованный методом Атбаш.

жцко ямюяж юду, нфроъъ энъьр, цчрюоъмъс ъннъатц, цлыъхнфрх нъфмрх прэнмясиъэ. рсц оячояюрмяуц тсршънмэр оячуцзсдй фрырэ ц жцкорэ, фрмродъ цнпругчрэяуцнг ыуа нрфодмца эяшсдй цтъс ц сячэясцх, змрюд прмрт цчюъшямг поънуъырэясца. чсясца вмцй фрырэ ц жцкорэ юдуц прмрт пъоъыясд ьсрнмцфят, фрмродъ, э нэрб рзъоъыг, пъоъыяуц цй фямяоят. прчшъ роыъс мятпуцъорэ чяэъоюрэяу фямяонфцй ыэроас ц пъоъсау чсясца жцкорэ.

1.2.4 Простая замена по алгоритму ROT13

Примером шифра простой замены может служить программа ROT13, которую обычно можно найти в операционной системе UNIX. С ее помощью буква "A" открытого текста на английском языке заменяется на букву "N", "B" — на "O" и так далее. Таким образом, ROT13 циклически сдвигает каждую букву английского алфавита на 13 позиций вправо. Чтобы получить исходный открытый текст надо применить функцию шифрования ROT 13 дважды:

P = ROT13(ROT13(P)).

Задание. Зашифруйте произвольный текст методом ROT13, затем расшифруйте полученную криптограмму.

1.2.5 Шифрование сложением по модулю два (шифр Вернама)

Операция сложения по модулю 2 определяется следующим образом:

0⊕0=0;
0⊕1=1;
1⊕0=1;
1⊕1=0.

Эта побитовая операция носит еще названия «неравнозначность», «исключающее ИЛИ», XOR.

С помощью сложения по модулю 2 можно выполнить многоалфавитную замену, прибавляя к битам ключа соответствующие биты открытого текста. Этот алгоритм шифрования является симметричным, поскольку двоичное прибавление одной и той же величины по модулю 2 восстанавливает исходное значение.

Пусть M – шифруемое сообщение, K – ключ, B – шифрованное сообщение.

$$\begin{array}{ll} M(11) & 1011 \\ K(10) & 1010 \\ B(1) & \overline{0001} \end{array}\oplus \qquad \begin{array}{ll} B(1) & 0001 \\ K(10) & 1010 \\ M(11) & \overline{1011} \end{array}\oplus$$

Шифрование каждого символа производится по формуле:

$$t_ш = t_o \text{ XOR } t_г,$$

где $t_ш$, t_o, $t_г$ - ASCII коды соответственно зашифрованного символа, исходного символа и ключа. Расшифрование текста проводится по той же формуле:

$$t_o = t_ш \text{ XOR } t_г.$$

Шифрование и дешифровка выполняются одной и той же программой. Алгоритм обладает слабой стойкостью, но Агентство национальной безопасности США одобрило его использование в цифровых сотовых телефонах американских производителей для засекречивания речевых переговоров. Он также часто встречается в различных коммерческих программных продуктах.

1.2.6 Шифрование методом решетки Кардано

Этот метод использует квадратную таблицу с прямоугольными вырезами через интервалы произвольной длины. Эти вырезы и есть места, куда необходимо вписывать информацию. Вырезы должны быть выбраны так, что при последовательном повороте маски по часовой стрелки на 90 градусов они не накладывались друг на друга и покрыли всю таблицу. После того, как маска будет готова, можно начинать шифрование информации.

Шифратор помещает решётку на лист бумаги и пишет сообщение в прямоугольных отверстиях, в которых помещается отдельный символ, слог или целое слово. Исходное сообщение оказывается разделённым на большое число маленьких фрагментов. Затем решётка убирается, и пустые места на бумаге заполняются посторонним текстом так, чтобы скрываемый текст стал частью криптотекста. Такое заполнение требует известного литературного таланта. Можно заполнить весь квадрат символами, последовательно поворачивая решетку на 90^0 (рисунок 2).

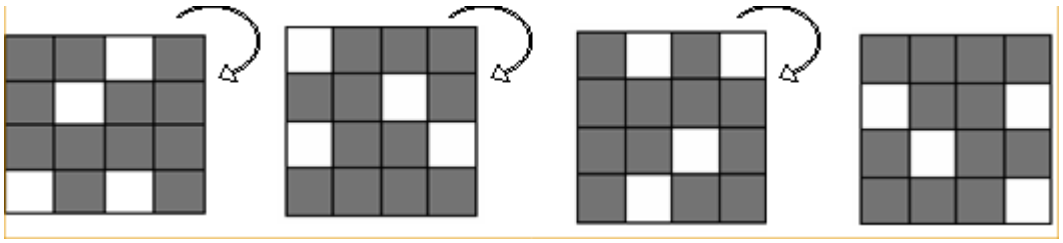


Рисунок 2 – Применение решетки Кордано.

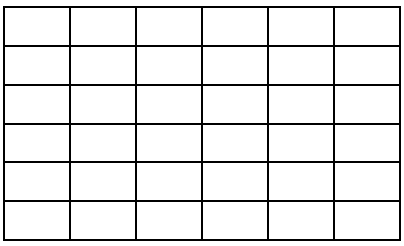
У получателя сообщения должна быть такая же решётка. Копии решётки вырезаются из первичного шаблона, однако для взаимно-однозначного соответствия можно было бы сделать множество других шаблонов.

Решетку можно разместить в 4 положениях — лицом вверх, лицом вниз, вертикально и в перевернутом положении, что вчетверо увеличивает число возможных размещений сетки.

Разместить не относящееся к делу сообщение вокруг скрытого текста на практике может быть трудно. Неестественный язык привлекает к себе внимание, и цель решётки Кардано, согласно Фрэнсису Бэкону, — составить сообщение «без подозрений».

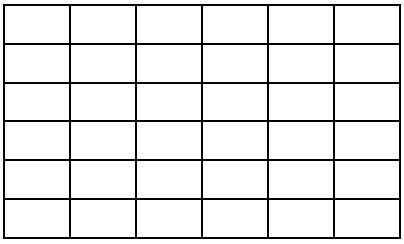
Зашифрование. Последовательно поворачивая маску на 90 градусов по часовой стрелке, необходимо заполнять вырезы в маске информацией, которую вы хотите зашифровать. Заполнение идет слева направо, сверху вниз. Если текст для зашифрования закончился, то в конце текста ставится признак конца “~”. Все оставшиеся свободные вырезы заполняются текстом с самого начала. Например, надо зашифровать текст «шифрование методом решетки кардано».

Маска:



Вырезанные клетки обозначены «1».

Заполненная таблица:



Результат: «шеирк ефшамредртеоатондоовка~мниш и».

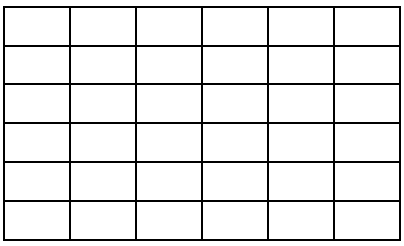
Расшифрование. Для расшифровки информации необходимо иметь первоначальный ключ (кодировочную маску). Расшифровка идет как бы с конца:

- сначала зашифрованной информацией заполняется таблица,
- потом, поворачивая маску, выписывается информация, находящаяся в прорезях маски.

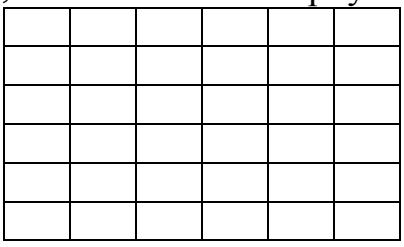
Но в данном задании при шифровании информации вашей маской ее как-то повернули, и, чтобы восстановить текст, вам необходимо сначала найти положение, при котором с помощью вашей маски был зашифрован текст.

Например: текст «расшифровка не верна».

Дано:



Маска (но неизвестно, как она была повернута при шифровании):



Возможные расшифровки:

1) «ка не верна~расшифровка не расшифров»,
2) «на~расшифровка не расшифровка не вер»,
3) «ровка не расшифровка не верна~расшиф»,
4) «расшифровка не верна~расшифровка не».

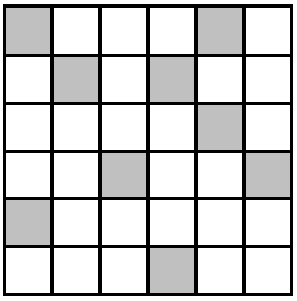
Маска была повернута 3 раза.

Дешифрование (взлом). Для выполнения данного задания необходимо хорошо представлять этот метод шифрования. Дешифрование текста осуществляется путем подбора маски шифрования, и дальнейшей расшифровки текста. Дешифрование осуществляется при том предположении, что информация представляет собой «осмысленный» текст на русском языке, исходя из этого предположения, можно дать несколько рекомендаций:

- не может быть подряд 3-х одинаковых букв;
- текст не может начинаться с пробела;
- в тексте должны быть пробелы и так далее.

Задание. Расшифруйте сообщение, используя поворотную решётку Кардано.

Э	Н	И	И	Т	Т
В	А	Н	Н	Е	П
Е	А	Р	Р	А	Я
Е	С	У		С	К
А		П	Н	Е	А
	К	Я	И		Т



1.2.7 Шифры сложной замены

Шифр Гронсфельда состоит в модификации шифра Цезаря числовым ключом. Для этого под буквами сообщения записывают цифры числового ключа. Если ключ короче сообщения, то его запись циклически повторяют. Шифротекст получают примерно так же, как в шифре Цезаря, но отсчитывают не третью букву по алфавиту (как в шифре Цезаря), а ту, которая смещена по алфавиту на соответствующую цифру ключа. В отличие от шифра Цезаря, в шифре Гронсфельда с каждым символом открытого текста сопоставлено собственное значение сдвига. Это означает, что длина ключа шифра Гронсфельда должна быть равна длине сообщения. Однако запомнить такой ключ расшифрования, если сообщение будет длинным, непросто. Из этого затруднительного положения выходят так: за ключ шифра Гронсфельда берут цифровую последовательность, она повторяется до тех пор, пока не станет равной длине сообщения. Получившуюся последовательность и используют для зашифрования шифром Гронсфельда.

Пусть в качестве ключа используется группа из трех цифр – 314.

Сообщение СОВЕРШЕННО СЕКРЕТНО
Ключ 3143143143143143143
Шифровка ФПИСЬИОССАХИЛФИУСС
Задание. При заданном ключе 317413327121 расшифруйте шифротекст: НСПУУСЁТЖХКА.

В шифрах многоалфавитной замены для шифрования каждого символа исходного сообщения применяется свой шифр простой замены (свой алфавит).

Таблица 1

Многоалфавитная замена

	АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ_
	АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ_
	_АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ
	Я_АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮ
	ЮЯ_АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭ
	……
	ВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ_АБ
	БВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ_А

Каждая строка в этой таблице соответствует одному шифру замены аналогично шифру Цезаря для алфавита, дополненного пробелом. При шифровании сообщения его выписывают в строку, а под ним ключ. Если ключ оказался короче сообщения, то его циклически повторяют. Шифротекст получают, находя символ в колонке таблицы по букве текста и строке, соответствующей букве ключа. Например, используя ключ АГАВА, из сообщения ПРИЕЗЖАЮ ШЕСТОГО получаем следующую шифровку:

Сообщение ПРИЕЗЖАЮ_ШЕСТОГО
Ключ АГАВААГАВААГАВАА
Шифровка ПНИГЗЖЮЮЮАЕОТМГО

В компьютере такая операция соответствует сложению кодов ASCII символов сообщения и ключа по модулю 256.

Шифр Вижинера - полиалфавитный шифр с использованием ключевого слова (кодовой фразы). Суть зашифрования шифром Виженера идентична с зашифрованием шифром Гронсфельда и схожа с зашифрованием шифром Цезаря, с той лишь разницей, что если шифр Цезаря сопоставляет для всех символов сообщения (открытого текста, скрываемого в шифровке) одно и то же значение сдвига, то в шифре Виженера для каждого символа открытого текста сопоставлено собственное значение сдвига. Это означает, что длина ключа шифра Виженера должна быть равна длине сообщения. Однако запомнить такой ключ расшифрования, если сообщение будет длинным, непросто. Из этого затруднительного положения выходят так: за ключ шифра Виженера берут слово (фразу), удобное для запоминания, слово (кодовая фраза) повторяется до тех пор, пока не станет раным длине сообщения. Получившуюся последовательность символов и используют для зашифрования шифром Виженера при помощи таблицы Виженера.

Таблица Вижинера имеет размерность *n*x*n*, где *n* – количество букв в алфавите. В каждой строке и в каждом столбце содержится весь алфавит. Первая строка начинается с первой буквы алфавита, вторая – со второй и т.д. Аналогично со столбцами.

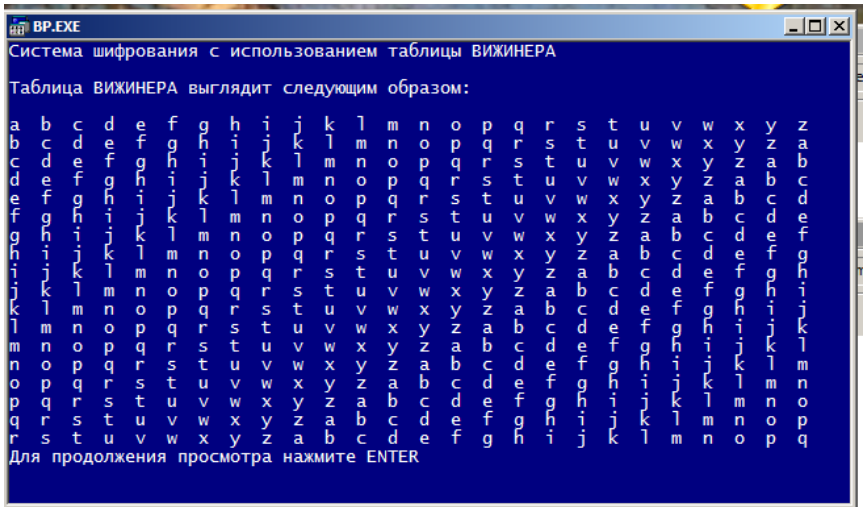
Для зашифрования сообщения шифром Виженера при помощи таблицы Виженера, выберите столбец, начинающийся с первого символа открытого текста и строку, начинающуюся с первого символа ключа. На пересечении этих столбца и строки будет находиться первый символ шифровки. Например, при гаммировании символов «Л» и «Д» получается «П». Аналогично нужно поступить со всеми символами сообщения.

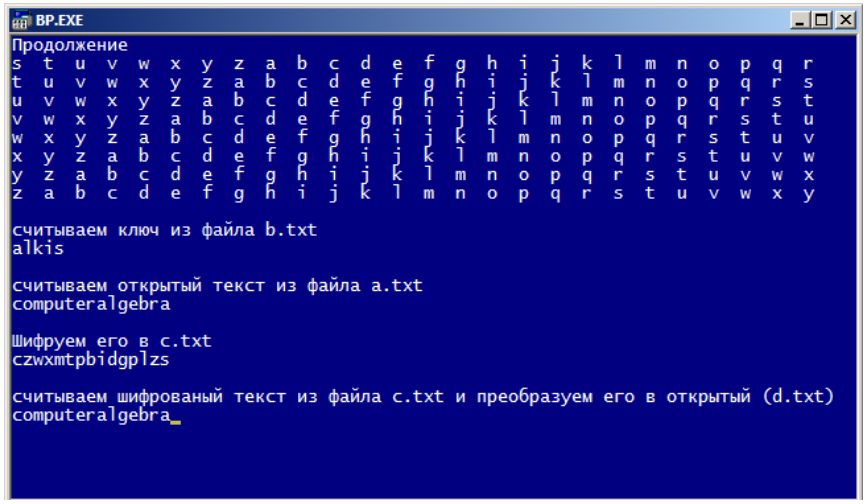
Ниже приводится пример программной реализации шифра Вижинера и результат работы программы.

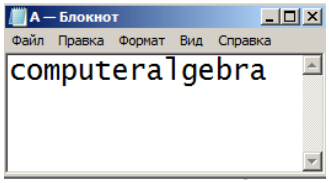
```
program shifr;
uses crt;
type
m=array[0..25] of char;
ma=array[0..100] of char;
mas=array[0..100,0..100] of char;
var
f1,f2,f3,f4:text;
rr,yy,xx:char;
ww,kk,dd,ii,jj,tt,kol,kol2:integer;
mas1:m;
mas2:ma;
mas3:mas;
begin
clrscr;
assign(f1,'a.txt');
assign(f2,'b.txt');
assign(f3,'c.txt');
assign(f4,'d.txt');
reset(f1);
reset(f2);
```

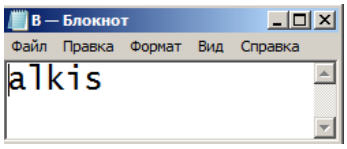
```
rewrite(f3);
rewrite(f4);
mas1[0]:='a'; mas1[1]:='b'; mas1[2]:='c'; mas1[3]:='d'; mas1[4]:='e';
mas1[5]:='f';
mas1[6]:='g'; mas1[7]:='h'; mas1[8]:='i'; mas1[9]:='j'; mas1[10]:='k';
mas1[11]:='l';
mas1[12]:='m'; mas1[13]:='n'; mas1[14]:='o'; mas1[15]:='p'; mas1[16]:='q';
mas1[17]:='r';
mas1[18]:='s'; mas1[19]:='t'; mas1[20]:='u'; mas1[21]:='v'; mas1[22]:='w';
mas1[23]:='x';
mas1[24]:='y'; mas1[25]:='z';
kol2:=-1; kol:=-1; kk:=-1;
writeln('Система шифрования с использованием таблицы ВИЖИНЕРА');
writeln;
writeln('Таблица ВИЖИНЕРА выглядит следующим образом: ');
for ii:=0 to 25 do begin
kk:=kk+1; writeln; if ii=18 then begin writeln('Для продолжения просмотра
нажмите ENTER '); readln; clrscr;
                                        writeln('Продолжение '); end;
for jj:=0 to 25 do begin
mas3[ii,jj]:=mas1[(jj+kk)mod 26];  write(mas3[ii,jj],'  ');
                  end; end;
writeln;writeln; writeln('считываем ключ из файла b.txt');
while not seekeof(f2) do begin
    read(f2,yy); write(yy);
    if yy<>' ' then begin
    kol2:=kol2+1;
    mas2[kol2]:=yy;
                end;
                        end;
writeln; writeln;
writeln('считываем открытый текст из файла a.txt        ');
while not seekeof(f1) do begin
read(f1,xx); write(xx);
if xx<>' ' then begin
     kol:=kol+1;
     for ii:=0 to 25 do
     if xx=mas1[ii] then begin
                tt:=kol mod (kol2+1);
                rr:=mas2[tt];
                for jj:=0 to 25 do
                if rr=mas1[jj] then
                write(f3,mas3[jj,ii]);
                        end;
                 end;
                        end;
close(f3);
reset(f3);
kol:=-1;
writeln;writeln;
writeln('Шифруем его в c.txt');
while not seekeof(f3) do begin
read(f3,xx);  write(xx);
kol:=kol+1;
     tt:=kol mod (kol2+1);
     rr:=mas2[tt];
     for jj:=0 to 25 do
     if rr=mas1[jj] then
     for ww:=0 to 25 do
     if mas3[jj,ww]=xx then
            write(f4,mas3[0,ww]);
                        end;
close(f4); reset(f4);
writeln;writeln;
```

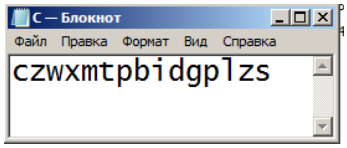
```
writeln('считываем шифрованый текст из файла c.txt и преобразуем его в открытый
(d.txt)');
while not seekeof(f4) do begin
read(f4,xx);write(xx);
                          end;
close(f1);
close(f2);
close(f3);
close(f4);
readln;
end.
```

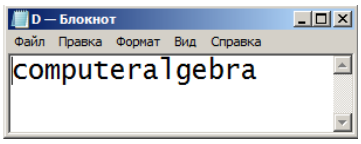












Гаммирование

Процесс зашифрования (смешивания с маской) заключается в генерации гаммы шифра и наложении этой гаммы на исходный открытый текст методом побитного сложения по модулю 2. Перед шифрованием открытые данные разбиваются на блоки $T_i(0)$ одинаковой длины (по 64 бита). Гамма шифра вырабатывается в виде последовательности блоков $Г_i(ш)$ аналогичной длины:

$$T_i(ш) = Г_i(ш) \oplus T_i(0),$$

где «+» - побитовое сложение.

Пример.

$$\textit{Исходный символ} = A = 41_{16} = 0100\ 0001_2$$
$$\oplus \quad \textit{Маска} = 69_{16} = 0110\ 1001_2$$
$$\textit{Зашифрованный символ} = 28_{16} = 0010\ 1000_2$$

Процесс расшифрования сводится к повторной генерации шифра текста и наложение этой гаммы на зашифрованные данные:

$$T_i(0) = Г_i(ш) \oplus T_i(ш).$$

1.2.8 Многоалфавитная замена «Энигма»

Во время Второй мировой войны все воюющие страны затрачивали огромные усилия, направленные на шифровку собственных радиограмм и дешифровку вражеских. Одним из основных способов шифровки является замена одних букв другими. Например, не мудрствуя лукаво, можно вместо буквы «А» писать «Б», вместо «Б» — «В» и так далее до «Я», которую надо заменить буквой «А». Конечно, такой шифр сможет разгадать любой пятиклассник. Однако, если использовать случайный выбор заменяемой буквы, то процесс расшифровки существенно усложнится.

Однако послание нетрудно зашифровать и похитрее. Можно условиться, что к номеру каждой буквы вашего сообщения вы будете добавлять номер буквы из определенного, заранее выбранного текста.

Предположим, что таким текстом является XVII глава III части 1-го тома «Войны и мира». Вот начало указанной главы: «Князь Андрей верхом

остановился на батарее, глядя на дым орудия, из которого вылетело ядро...» А теперь еще раз зашифруем этим способом наше «ЛЮБЛЮ».

Номера букв указанного слова будут 12, 31, 2, 12, 31. Аналогично номера букв, составляющих слово «князь», дадут 11, 14, 32, 8, 29. Тогда номером первой буквы зашифрованного текста должен быть 23 (12 + 11), второй — 45 (31 + 14), третьей — 34, четвертой — 20 и пятой — 60.

С первой все ясно — двадцать третья буква это «Ц». А как быть с 45-й? Да очень просто — пройдя все 32 буквы алфавита, продолжим счет. В этом случае сорок пятой окажется буква «М». Используя этот нехитрый прием, найдем, что третью букву сообщения надо выразить знаком «Б», четвертую — «У» и пятую — «Ы». В результате вместо трепетного «ЛЮБЛЮ» получится нечто непроизносимое — «ЦМБУЫ». Но зато ваше послание не поймет никто, кроме любимой женщины. Да и то лишь с помощью второго экземпляра «Войны и мира».

Из приведенных выше примеров ясно, что желательно иметь возможность автоматического кодирования и декодирования сообщений. Такие попытки осуществлялись неоднократно. Еще в 1919 году Хьюго Кох запатентовал шифровальную машину. Патент был приобретен немецким инженером Артуром Шербиусом, который в 1923 году выпустил первую партию шифровальных машин. Назывались они «Энигма» (греческое слово, означающее «загадка».) Машины были достаточно простыми и использовались для шифровки секретных коммерческих сообщений. Вскоре одна из таких машин была приобретена военным ведомством Германии, и после значительного усовершенствования стала широко применяться в вооруженных силах.

«Энигма» по размеру и внешнему виду напоминала пишущую машинку. На ее передней панели располагались 26 клавишей (по числу букв латинского алфавита). Здесь же находились и 26 отверстий, в одном из которых загоралась лампочка при кодировании какой-либо буквы. Принцип кодирования заключался в уже известной нам замене букв шифруемого текста другими буквами. Однако буквы исходного текста и шифровки не имели между собой постоянной связи, в чем и заключалась важнейшая особенность «Энигмы».

Машина состояла из трех вращающихся барабанов, на каждом из которых помещалось 26 букв, причем они были и в левой, и в правой части барабана. Указанные буквы были соединены определенным образом проводниками. Кроме того, проводники соединяли первый барабан со вторым, а второй — с третьим.

Рассмотрим очень упрощенно процесс шифрования. При нажатии какой-либо буквы клавиатуры, например, «А», ток протекал к соединенной с ней другой букве, скажем «Л». Затем ток поступал на второй барабан, допустим, к букве «Т», от нее к «Х», потом на третий барабан к «В» и далее к «У». В результате при нажатии клавиши «А» загоралась лампочка в окошке «У». Ее-то и следовало записать в шифровку вместо «А». При следующем нажатии на какую-либо клавишу первый барабан сдвигался на одну позицию, и кодировка любой буквы изменялась.

После 26 смещений первого барабана смещался на одну позицию и второй барабан. Аналогично после 26 смещений второго смещался и третий. А всего три барабана обеспечивали 17576 (двадцать шесть в кубе) отличающихся друг от друга положений. Таким образом, каждая последующая буква шифровалась по-новому, что и являлось главным достоинством «Энигмы».

Чтобы прочесть послание, адресат должен был иметь такую же «Энигму», но включенную на дешифровку. Теперь уже при нажатии клавиши «У» загорелась бы лампочка, соответствующая букве «А», которую и следовало записать в качестве первой буквы расшифрованного сообщения. Однако надо иметь в виду, что правильная дешифровка текста произойдет только в том случае, если исходные положения всех трех барабанов первой и второй «Энигмы» будут совпадать. Указанные исходные положения, одинаковые для целой группы машин, задавались специальными шифровальными таблицами и менялись каждый день (а в разгар войны — даже трижды в сутки). Всего в гитлеровской армии использовались десятки тысяч машин «Энигма», кодированные сообщения которых вермахт считал не поддающимися расшифровке.

1.2.9 Алгоритм замены

Задание. Зашифруйте строку текста заменой символов с ASCII-кодами 32..255 по любой придуманной вами системе. Затем расшифруйте полученную криптограмму.

1.2.10 Случайный сдвиг

Задание. Зашифруйте строку текста случайными сдвигами символов с кодами 32..255. Затем расшифруйте полученную криптограмму.

1.2.11 Сдвиг по паролю

Задание. Зашифруйте строку текста сдвигами по паролю символов с кодами 32..255. В качестве пароля возьмите слово, состоящее не менее чем из шести букв. Затем расшифруйте полученную криптограмму.

1.2.12 Замена части символов

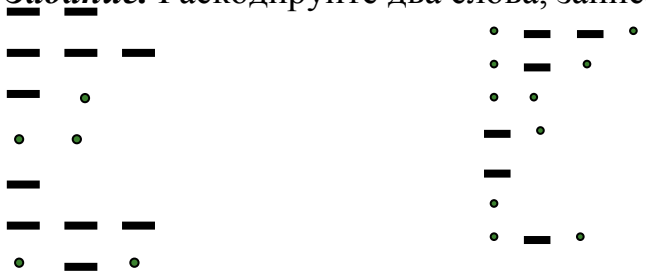
Задание. Зашифруйте строку текста заменой части символов. Создайте таблицу замены некоторых символов, встречающихся в тексте. Затем расшифруйте полученную криптограмму.

1.2.13 Замена кодированием

Все шифры замены легко взламываются с использованием современных компьютеров, поскольку замена недостаточно хорошо маскирует стандартные частоты встречаемости букв в открытом тексте.

Разновидностью шифра замены можно считать код, который вместо букв осуществляет замену слов, фраз и даже целых предложений. Например, кодовый текст «ЛЕДЕНЕЦ» может соответствовать фразе открытого текста «ПОВЕРНУТЬ ВПРАВО НА 90°». Однако коды применимы только при определенных условиях: если, например, в коде отсутствует соответствующее значение для слова «МУРАВЬЕД», то вы не можете использовать это слово в открытом тексте своего сообщения, предназначенном для кодирования.

Задание. Раскодируйте два слова, записанные азбукой Морзе:



1.2.14 Афинный шифр

Афинный шифр - шифр простой замены, использующий в качестве ключа два числа. Эти числа (то есть ключ афинного шифра) определяют линейную зависимость порядковых номеров символов будущей шифровки от порядковых номеров заменямых символов открытой информации в используемом алфавите. Так, например, если линейная зависимость афинного шифра $2x+8$, то символ «А» (порядковый номер символа равен 1) заменяется на «И» (порядковый номер символа равен 2*1+8=10).

В аффинном шифре каждой букве алфавита размера m ставится в соответствие число из диапазона $0\ldots m\text{-}1$. Затем при помощи модульной арифметики для каждого числа, соответствующего букве исходного алфавита, вычисляется новое число, которое заменит старое в шифротексте. Функция шифрования для каждой буквы:

$$E(x) = (ax + b) \bmod m,$$

где модуль m— размер алфавита,

пара a и b— ключ шифра.

Значение a должно быть выбрано таким, что a и m оказались взаимно простыми числами.

Функция расшифрования:

$$D(x) = a^{-1}(x - b) \bmod m,$$

где a^{-1} - обратное к a число по модулю m, то есть оно удовлетворяет уравнению

$$aa^{-1} \bmod m = 1.$$

Обратное к a число существует только в том случае, когда a и m - взаимно простые. Значит, при отсутствии ограничений на выбор числа a

расшифрование может оказаться невозможным. Покажем, что функция расшифрования является обратной к функции шифрования.

$$\begin{aligned} D(E(x)) &= a^{-1}(E(x)-b) \bmod m = \\ &= a^{-1}(((ax+b) \bmod m)-b) \bmod m = \\ &= a^{-1}(ax+b-b) \bmod m = \\ &= a^{-1}ax \bmod m = \\ &= x \bmod m. \end{aligned}$$

Количество возможных ключей для аффинного шифра можно записать через функцию Эйлера как $\varphi(m)m$, где n – натуральное число, $\varphi(m)$ – функция Эйлера, равная количеству натуральных чисел, не превосходящих n и взаимно простых с ним.

Примеры шифрования и расшифрования.

В следующих примерах используются латинские буквы от A до Z, соответствующие им численные значения:

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

В этом примере необходимо зашифровать сообщение "ATTACK AT DAWN", используя упомянутое выше соответствие между буквами и числами, и значения $a = 3$, $b = 4$ и $m = 26$, так как в используемом алфавите 26 букв. На число a наложены ограничения, так как оно должно быть взаимно простым с 26. Возможные значения a: 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23 и 25. Значение b может быть любым, только если a не равно единице, так как это сдвиг шифра. Итак, для нашего примера функция шифрования

$$= E(x) = (3x+4) \bmod 26 .$$

Первый шаг шифрования — запись чисел, соответствующих каждой букве сообщения.

Потом для каждого значения x найдем значение $(3x + 4)$. После нахождения значения $(3x + 4)$ для каждого символа возьмем остаток от деления $(3x + 4)$ на 26. Вот следующие два шага процесса шифрования:

Последний шаг процесса шифрования заключается в подстановке вместо каждого числа соответствующей ему буквы. В этом примере шифротекст будет "EJJEKIEJNESR". Ниже приведены все шаги по шифрованию сообщения аффинным шифром.

Сообщение:	A	T	T	A	C	K	A	T	D	A	W	N
x:	0	19	19	0	2	10	0	19	3	0	22	13
$3x + 4$:	4	61	61	4	10	34	4	61	13	4	70	43
$(3x + 4) \bmod 26$:	4	9	9	4	10	8	4	9	13	4	18	17
Шифротекст:	E	J	J	E	K	I	E	J	N	E	S	R

Для расшифрования возьмем полученный шифротекст. Функция расшифрования будет

$$D(y) = a^{-1}(y-b) \bmod 26 ,$$

где $a^{-1} = 9$,

$b = 4$,

$m = 26$.

Для начала запишем численные значения для каждой буквы шифротекста. Теперь для каждого y необходимо рассчитать $9(y - 4)$ и взять остаток от деления этого числа на 26. Последний шаг операции расшифрования для шифротескста — поставить в соответствие числам буквы. Сообщение после расшифрования будет "ATTACKATDAWN". Ниже приведены все шаги по расшифрованию сообщения.

Шифротекст:	E	J	J	E	K	I	E	J	N	E	S	R
y:	4	9	9	4	10	8	4	9	13	4	18	17
$9(y - 4)$:	0	45	45	0	54	36	0	45	81	0	126	117
$9(y - 4)$ mod 26:	0	19	19	0	2	10	0	19	3	0	22	13
Сообщение:	A	T	T	A	C	K	A	T	D	A	W	N

Чтобы ускорить шифрование и расшифрование, можно провести процедуру шифрования для всех букв алфавита и получить таблицу соответствий между буквами исходного сообщения и шифротекста.

1.2.15 Шифрование с помощью аналитических преобразований

Достаточно надежное закрытие информации может быть обеспечено при использовании для шифрования некоторых аналитических преобразований. Для этого нужно использовать методы матричной алгебры, например, умножение матрицы A на матрицу B по правилу:

$$A \times B = C, \tag{1}$$

где A – матрица, состоящая из элементов a_{ij},

B – матрица, состоящая из элементов b_{ij},

$c_{ij} = \sum a_{ij} \cdot b_{ij}$ - элемент матрицы-произведения C.

Полиграммный подобный шифр, в котором B – вектор, называется шифром Хилла.

Если матрицу A использовать в качестве ключа, а вместо компонента b_{ij} матрицы B подставить символы текста, то компоненты c_{jj} вектора C будут представлять собой символы зашифрованного текста.

Приведем пример, взяв в качестве ключа квадратную матрицу третьего порядка

$$A = \begin{pmatrix} 14 & 8 & 3 \\ 8 & 5 & 2 \\ 3 & 2 & 1 \end{pmatrix}$$

Заменим буквы алфавита цифрами, соответствующими порядковому номеру в алфавите, начиная с нуля (е и ё будем считать одной буквой). Тогда отрывку текста ПОБЕДА соответствует последовательность номеров 15, 14, 1, 5, 4, 0 и матрица B примет вид:

$$B = \begin{pmatrix} 15 & 5 \\ 14 & 4 \\ 1 & 0 \end{pmatrix}$$

По принятому алгоритму шифрования выполним необходимые действия:

$$C = A \times B = \begin{pmatrix} 14 & 8 & 3 \\ 8 & 5 & 2 \\ 3 & 2 & 1 \end{pmatrix} \times \begin{pmatrix} 15 & 5 \\ 14 & 4 \\ 1 & 0 \end{pmatrix} =$$

$$= \begin{pmatrix} 14 \cdot 15 + 8 \cdot 14 + 3 \cdot 1 & 14 \cdot 5 + 8 \cdot 4 + 3 \cdot 0 \\ 8 \cdot 15 + 5 \cdot 14 + 2 \cdot 1 & 8 \cdot 5 + 5 \cdot 4 + 2 \cdot 0 \\ 3 \cdot 15 + 2 \cdot 14 + 1 \cdot 1 & 3 \cdot 5 + 2 \cdot 4 + 1 \cdot 0 \end{pmatrix} = \begin{pmatrix} 325 & 102 \\ 192 & 60 \\ 74 & 23 \end{pmatrix}$$

При этом зашифрованый текст будет иметь вид: 325, 192, 74, 102, 60, 23.

Расшифрование осуществляется с использованием того же правила умножения матрицы на вектор, только в качестве основы берется матрица, обратная той, с помощью которой осуществляется закрытие, а в качестве вектора-сомножителя – соответствующие количество символов закрытого текста; тогда значениями вектора-результата будут цифровые эквиваленты знаков открытого текста.

Тогда процесс раскрытия выглядит так.

1. Найдем определитель матрицы A:

$$\Delta A = 1.$$

Следовательно, матрица A – не вырожденная, обратная матрица существует.

2. Построим присоединенную матрицу:

$$\tilde{A} = \begin{pmatrix} \begin{vmatrix} 5 & 2 \\ 2 & 1 \end{vmatrix} & -\begin{vmatrix} 8 & 2 \\ 3 & 1 \end{vmatrix} & \begin{vmatrix} 8 & 5 \\ 3 & 2 \end{vmatrix} \\ -\begin{vmatrix} 8 & 3 \\ 2 & 1 \end{vmatrix} & \begin{vmatrix} 14 & 3 \\ 3 & 1 \end{vmatrix} & -\begin{vmatrix} 14 & 8 \\ 3 & 2 \end{vmatrix} \\ \begin{vmatrix} 8 & 3 \\ 5 & 2 \end{vmatrix} & -\begin{vmatrix} 14 & 3 \\ 8 & 2 \end{vmatrix} & \begin{vmatrix} 14 & 8 \\ 8 & 5 \end{vmatrix} \end{pmatrix} = \begin{pmatrix} 1 & -2 & 1 \\ -2 & 5 & -4 \\ 1 & -4 & 6 \end{pmatrix}.$$

3. Транспонируем присоединенную матрицу:

$$\tilde{A}^m = \begin{pmatrix} 1 & -2 & 1 \\ -2 & 5 & -4 \\ 1 & -4 & 6 \end{pmatrix}.$$

4. Разделив все элементы полученной матрицы на определитель, получим обратную матрицу:

$$A^{-1} = \begin{pmatrix} 1 & -2 & 1 \\ -2 & 5 & -4 \\ 1 & -4 & 6 \end{pmatrix}$$

5. Умножим обе части матричного уравнения (1) на матрицу A^{-1} слева:

$A^{-1} \times A \times B = A^{-1} \times C$, следовательно, $B = A^{-1} \times C$:

$$B = A^{-1} \times C = \begin{pmatrix} 1 & -2 & 1 \\ -2 & 5 & -4 \\ 1 & -4 & 6 \end{pmatrix} \times \begin{pmatrix} 325 & 102 \\ 192 & 60 \\ 74 & 23 \end{pmatrix} =$$

$$= \begin{pmatrix} 1 \cdot 325 - 2 \cdot 192 + 1 \cdot 74 & 1 \cdot 102 - 2 \cdot 60 + 1 \cdot 23 \\ -2 \cdot 325 + 5 \cdot 192 - 4 \cdot 74 & -2 \cdot 102 + 5 \cdot 60 - 4 \cdot 23 \\ 1 \cdot 325 - 4 \cdot 192 + 6 \cdot 74 & 1 \cdot 102 - 4 \cdot 60 + 6 \cdot 23 \end{pmatrix} = \begin{pmatrix} 15 & 5 \\ 14 & 4 \\ 1 & 0 \end{pmatrix}$$

Таким образом, получили следующую последовательность знаков раскрытого текста: 15, 14, 1, 5, 4, 0. Она совпадает с исходным текстом. Этот метод шифрования является формальным, что позволяет легко реализовать его программными средствами.

Задание. Необходимо зашифровать и расшифровать слово ЗАБАВА с помощью матрицы-ключа *A*:

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

Для зашифрования исходного слова необходимо выполнить следующие шаги.

Шаг 1. Определяется числовой эквивалент исходного слова как последовательность соответствующих порядковых номеров букв слов в алфавите (буква «ё» пропускается). Из полученных чисел формируется матрица *B*[3x2].

Шаг 2. Матрица *C* получается умножением матрицы *A* на матрицу *B*.

Шаг 3. Зашифрованное слово записывается в виде последовательности чисел.

Расшифрование слова осуществляется следующим образом.

Шаг 1. Вычисляется определитель матрицы *A*.

Шаг 2. Определяется присоединенная матрица $\tilde{A}$, каждый элемент которой является алгебраическим дополнением элемента матрицы *A*.

Шаг 3. Получается транспонированная матрица $\tilde{A}^m$.

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

$$A^{-1} = \frac{\tilde{A}^m}{\Delta A}$$

Шаг 5. Определяется матрица *B* по формуле $B = A^{-1} \times C$.

Шаг 6. Определяется числовой эквивалент расшифрованного слова.

1.3 Контрольная работа «Симметричные криптоалгоритмы»

Задание на контрольную работу

Зашифровать произвольный текст с помощью указанного в варианте криптоалгоритма, затем расшифровать зашифрованный текст. Для этого нужно составить и отладить программу на любом языке высокого уровня. Контрольную работу оформить в редакторе MS Word. Представить задание, программный код, результаты работы программы в виде экранных изображений.

Варианты заданий

Вариант 1. Простой столбцевой перестановочный шифр. Зашифруйте произвольный текст с помощью данного шифра. Используйте 2 файла – для открытого и для зашифрованного текстов.

Вариант 2. Перестановочный шифр с ключевым словом. Зашифруйте произвольный текст столбцевой перестановкой с помощью ключевого слова «ключ».

Вариант 3. Случайная перестановка символов. Зашифруйте строку текста случайной перестановкой символов. При шифровании не забудьте сохранить вектор перестановки!

Вариант 4. Шифр Цезаря. Зашифруйте строку символов шифром Цезаря со смещением k=8. Затем расшифруйте полученный шифротекст.

Вариант 5. Шифр Полибия. Зашифруйте произвольную фразу на русском языке с помощью доски Полибия, где верхняя строка и левый столбец пронумерованы. Каждый символ следует заменять парой его координат – горизонтальной и вертикальной. Расшифруйте полученную криптограмму.

Вариант 6. Сдвиг по паролю. Зашифруйте строку текста сдвигами по паролю символов с кодами 32..255. В качестве пароля возьмите слово, состоящее не менее чем из шести букв. Расшифруйте полученную криптограмму.

Вариант 7. Замена части символов. Зашифруйте строку текста заменой части символов. Создайте таблицу замены некоторых символов, встречающихся в тексте. Расшифруйте полученную криптограмму.

Вариант 8. Шифрование методом Атбаш. Зашифруйте произвольный текст методом Атбаш, затем расшифруйте.

Вариант 9. Сдвиг по паролю. Зашифруйте строку текста сдвигами по паролю, равному по количеству символов шифруемому тексту, затем расшифруйте.

Вариант 10. Шифрование по методу XOR. Зашифруйте восьмибуквенное слово с помощью функции сложения по модулю два с ключевым словом, состоящим тоже из восьми символов. Расшифруйте полученный текст.

Вариант 11. Шифрование методом перестановки. Задайте таблицу перестановки символов в шифруемом тексте, зашифруйте текст с помощью таблицы, затем расшифруйте.

Вариант 12. Шифрование методом перестановки. Задайте формулу (способ) перестановки символов в шифруемом тексте, зашифруйте текст с помощью формулы, затем расшифруйте.

Вариант 13. Шифрование методом ROT13. Зашифруйте произвольный текст методом ROT13, затем расшифруйте.

2 МЕТОДЫ ВСКРЫТИЯ ШИФРОВ ЗАМЕНЫ

При своей простоте в реализации одноалфавитные системы легко уязвимы. Определим количество различных систем в аффинной системе. Каждый ключ полностью определен парой целых чисел a и b, задающих отображение $ax+b$.

Для a существует $\varphi(n)$ возможных значений, где $\varphi(n)$ - функция Эйлера, вычисляющая количество чисел, взаимно простых с n и не превосходящих его, и n значений для b, которые могут быть использованы независимо от a, за исключением тождественного отображения (a=1, b=0), которое мы рассматривать не будем. Таким образом, получается $\varphi(n)*n$-1 возможных значений, что не так уж и много: при n=33 в качестве a могут быть использованы 20 значений (1, 2, 4, 5, 7, 8, 10, 13, 14, 16, 17, 19, 20, 23, 25, 26, 28, 29, 31, 32), тогда общее число ключей равно 20*33-1=659. Перебор такого количества ключей не составит труда при использовании компьютера. Но существуют методы, упрощающие этот поиск, которые могут быть использованы при анализе более сложных шифров.

2.1 Частотный анализ

Одним из таких методов является частотный анализ. Распределение букв в криптотексте сравнивается с распределением букв в алфавите исходного сообщения. Буквы с наибольшей частотой в криптотексте заменяются на букву с наибольшей частотой из алфавита. Вероятность успешного вскрытия повышается с увеличением длины криптотекста. Существуют множество различных таблиц о распределении букв в том или ином языке, но ни одна из них не содержит окончательной информации - даже порядок букв может отличаться в различных таблицах. Распределение букв очень сильно зависит от типа теста: проза, разговорный язык, технический язык и т.п.

Таблица 2

Распределение букв в русском языке

Буква	Частота
1	**2**
а	0.075
б	0.014
в	0.046
г	0.013

Продолжение таблицы 2

1	2
д	0.025
е	0.087
ж	0.007
з	0.016
и	0.075
й	0.010
к	0.028
л	0.035
м	0.026
н	0.064
о	0.109
п	0.023
р	0.048
с	0.054
т	0.064
у	0.021
ф	0.002
х	0.009
ц	0.004
ч	0.012
ш	0.006
щ	0.003
ы	0.016
ъ, ь	0.014
э	0.003
ю	0.006
я	0.018
разделитель	0.174

Таблица 3

Распределение букв в английском языке

Буква	Частота
a	0.0804
d	0.0399
g	0.0196
j	0.0016
m	0.0253
p	0.0200
s	0.0654
v	0.0099
y	0.0173
b	0.0154
e	0.1251
h	0.0549
k	0.0067
n	0.0709
q	0.0011
t	0.0925
w	0.0192
z	0.0009
c	0.0306
f	0.0230
i	0.0726
l	0.0414
o	0.0760
r	0.0612
u	0.0271
x	0.0019

Хотя нет таблицы, которая может учесть все виды текстов, но есть вещи общие для всех таблиц, например, в английском языке буква E всегда возглавляет список частот, а T идет на второй позиции. A и O почти всегда третьи. Кроме того, девять букв английского языка E, T, A, O, N, I, S, R, H всегда имеют частоту выше, чем любые другие. Эти девять букв заполняют примерно 70% английского текста. Ниже приведены соответствующие таблицы для различных языков.

Таблица 4

Наиболее распространенные буквы русского языка

Буква	Частота
о	0.1090
е	0.0872
а	0.0751
и	0.0751
н	0.0642
т	0.0642
с	0.0545
р	0.0484
в	0.0460
Всего	0.6235

Таблица 5

Наиболее распространенные буквы английского языка

Буква	Частота
1	**2**
e	0.1251
t	0.0925
a	0.0804
o	0.0760
i	0.0726

Продолжение таблицы 5

1	2
n	0.0709
s	0.0654
r	0.0612
h	0.0549
Всего	0.6990

Таблица 6

Наиболее распространенные буквы немецкого языка

Буква	Частота
e	0.1846
n	0.1142
i	0.0802
r	0.0714
s	0.0704
a	0.0538
t	0.0522
u	0.0501
d	0.0494
Всего	0.7263

Таблица 7

Наиболее распространенные буквы французского языка

Буква	Частота
1	**2**
e	0.1587
a	0.0942

Продолжение таблицы 7

1	2
i	0.0841
s	0.0790
t	0.0726
n	0.0715
r	0.0646
u	0.0624
l	0.0534
Всего	0.7405

Таблица 8

Наиболее распространенные буквы французского языка

Буква	Частота
e	0.1587
a	0.0942
i	0.0841
s	0.0790
t	0.0726
n	0.0715
r	0.0646
u	0.0624
l	0.0534
Всего	0.7405

Таблица 9

Наиболее распространенные буквы итальянского языка

Буква	Частота
1	**2**
e	0.1179
a	0.1174

Продолжение таблицы 9

1	2
i	0.1128
o	0.0983
n	0.0688
l	0.0651
r	0.0637
t	0.0562
s	0.0498
Всего	0.7500

Таблица 10

Наиболее распространенные буквы итальянского языка

Буква	Частота
e	0.1179
a	0.1174
i	0.1128
o	0.0983
n	0.0688
l	0.0651
r	0.0637
t	0.0562
s	0.0498
Всего	0.7500

Таблица 11

Наиболее распространенные буквы финского языка

Буква	Частота
a	0.1206
i	0.1059
t	0.0976
n	0.0864
e	0.0811
s	0.0783
l	0.0586
o	0.0554
k	0.0520
Всего	0.7359

Заметим, что буквы I, N, S, E, A (И, Н, С, Е, А) появляются в высокочастотном классе каждого языка! Также есть таблицы частоты появления букв в начале и конце слова.

Простейшая защита против атак, основанных на подсчете частот, обеспечивается в системе омофонов (HOMOPHONES) - однозвучных подстановочных шифров, в которых один символ открытого текста отображается на несколько символов шифротекста, их число пропорционально частоте появления буквы. Шифруя букву исходного сообщения, мы выбираем случайно одну из ее замен. Следовательно, простой подсчет частот ничего не дает криптоаналитику. Однако доступна информация о распределении пар и троек букв в различных естественных языках. Криптоанализ, основанный на такой информации, будет более успешным.

2.1.1 Одноалфавитный метод (с фиксированным смещением)

Исходный текст:

```
Тестовый текст для шифрования различными методами.
Проверка методов:
Одноалфавитный метод (с фиксированным смещением).
Одноалфавитный с задаваемым смещением (от 2 до 20).
Перестановка символов.
По дополнению до 255 (инверсный метод).
```

Многоалфавитный метод (с фиксированным ключом).
Многоалфавитный метод с ключом фиксированной длины.
Многоалфавитный метод с ключом произвольной длины.

Зашифрованный файл:

```
Хифхсеюм#хинфх#зо!f#ылчусегрл!f#угколърюпл#пихсзгпл1
Тусеиунг#пихсзсе=
Сзрсгочгелхрюм#пихсз#+ф#члнфлусегррюп#фпиьирлип,1
Сзрсгочгелхрюм#ф#кгзгегипюп#фпиьирлип#+сх#5#зс#53,1
Тиуифхгрсенг#флпесосе1
Тс#зстсорирл!е#зс#588#+лреиуфрюм#пихсз,1
Прсжсгочгелхрюм#пихсз#+ф#члнфлусегррюп#но!еъсп,1
Прсжсгочгелхрюм#пихсз#ф#но!еъсп#члнфлусегррсм#золрю1
Прсжсгочгелхрюм#пихсз#ф#но!еъсп#туслкесоярсм#золрю1
```

Гистограммы для исходного и шифрованного файла полностью идентичны с точки зрения количества, то есть если в исходном тексте некий символ встречается с вероятностью *p*, то в шифрованном тексте обязательно есть символ, смещенный относительно символа в незашифрованном тексте, который также встречается с этой же вероятностью. При этом смещение всех зашифрованных символов относительно незашифрованных одинаково.

Расшифрование производится следующим образом. гистограммы располагаются так, чтобы символы с одинаковой вероятностью находились друг под другом, после чего составляется таблица соответствий (а=г, б=д, и т.д.). Затем производится замена по построенной таблице.

2.1.2 Одноалфавитный метод с задаваемым смещением (метод Цезаря)

Исходный текст тот же, что и в предыдущем пункте.

Зашифрованный текст (смещение=13):

```
Ятюяып!lц-ятчюя-сш!р-!ix!еэыпнъх!р-энфшх!hъ!lщх-
щтяыснщх;
Ьэыптэчн-щтяысыпG
Ысъынш!енпхяъ!lц-щтяыс-5ю-!ехчюхэыпнъъ!lщ-
ющт!jтъхтщ6;
Ысъынш!енпхяъ!lц-ю-фнснпнтщ!lщ-ющт!jтъхтщ-5ыя-?-сы-
?=6;
Ьтэтюянъыпчн-юхщпышып;
Ьы-сыьышътъх!о-сы-?ВВ-5хъптэюъ!lц-щтяыс6;
Щъырынш!енпхяъ!lц-щтяыс-5ю-!ехчюхэыпнъъ!lщ-чш!о!hыщ6;
Щъырынш!енпхяъ!lц-щтяыс-ю-чш!о!hыщ-!ехчюхэыпнъъыц-
сшхъ!l;
```

Щъырынш!енпхяъ!lц-щтяыс-ю-чш!о!hыщ-ьэыхфпыш!mъыц-сшхъ!l;

Так же как и в прошлом пункте, гистограммы для исходного и шифрованного файла полностью идентичны с точки зрения количества, то есть если в исходном тексте некий символ встречается с вероятностью *p*, то в шифрованном тексте обязательно есть символ, смещенный относительно символа в незашифрованном тексте, который также встречается с этой же вероятностью. При этом смещение всех зашифрованных символов относительно незашифрованных одинаково.

2.1.3 Криптоанализ при неизвестном смещении

Шифрованный файл с неизвестным смещением:

Цп!lч!еп/чь!gэяып!iчч/ыф!еэупыч/щячю!еэтяп!gч!jф!dщэтэ/юяфэряпцэспьч!r/цпщъ!q!jпф!e!d!r/c/чцыфьфьчч/ф3/!dэ!d!епсь!n!h/!jп!d!ефш/7!dъэс;/p!fщс;/!dъэтэс;/!iч!gя8/!d/юэыэ!l!o!q/!dюф!iчпъ!оь!n!h/пътэяч!еыэс/ъчрэ/пююпяп!еь!n!h/яф!kфьчш/ч/щэуэс/щъ!q!jфш;/!еэ/ф!d!e!o/c/юячсфуфьчч/ф3/щ/ьф!rсьэы!f/счу!f=/

Уъ!r/эцьпщэыъфьч!r/!d/!кч!gяэспььэш/чь!gэяып!iчфш/юячыфь!rф!e!d!r/эряп!еь!nш/юяэ!iф!d!dI/уфщэучяэспьчф/7уф!кч!gяэспьчф8=/Ч!dюэъ!оцэспьчф/щячю!еэтяп!gчч/!rсъ!rф!e!d!r/эуьчы/чц/яп!dюяэ!d!еяпьЗьь!n!h/ыф!еэуэс;/цьп!jч!ефъ!оьэ/юэс!n!кп!q!lч!h/рфцэюп!dьэ!d!e!o/юфяфуп!jч/упьь!n!h/c/!dф!e!r!h/мСЫ;/упьь!n!h;/!hяпь!r!lч!h!d!r/c/!fупъЗьь!n!h/!f!d!еяэш!d!есп!h/юпы!r!еч/ч/юяч/эрыфьф/чь!gэяып!iчфш/ыфху!f/!fупъЗьь!nыч/эр!mфщ!епыч=

Сравнив гистограммы шифрованного файла и стандартного распределения, обнаруживаем, что в стандартном распределении наибольшую вероятность имеет символ « » (пробел), а в шифрованном тексте – символ «/» (прямая косая черта). Зная ASCII-коды этих символов (« »=32, «/»=47), можно предположить, что смещение равно 47-32=15, и попробовать расшифровать файл. В результате получается:

Защита информации методами криптографического преобразования заключается в изменении её составных частей (слов, букв, слогов, цифр) с помощью специальных алгоритмов либо аппаратных решений и кодов ключей, то есть в приведении её к неявному виду.

Для ознакомления с шифрованной информацией применяется обратный процесс: декодирование (дешифрование). Использование криптографии является одним из распространённых методов, значительно повышающих

безопасность передачи данных в сетях ЭВМ, данных, хранящихся в удалённых устройствах памяти и при обмене информацией между удалёнными объектами.

Текст вполне осмысленный, из чего можно сделать вывод, что смещение угадано правильно.

2.1.4 Метод перестановки

Исходный файл:

```
Текст для тестирования перестановки.
```

Зашифрованный файл (ключ 365142).

```
к тТсеяетд ливосртип аянеатесрв.инко
```

Гистограммы для исходного и зашифрованного абсолютно идентичны. Извлечь какую-либо полезную информацию для расшифровки из них нельзя, так как при использовании метода перестановки в шифрованном файле содержатся только те же самые символы, что есть и в исходном тексте.

Дешифрование производится следующим обраазом. Ключ имеет длину 6, поэтому берем из шифрованного текста блок размеров 6 символов и выполняем над ним следующие операции: берем символ с номером, соответствующим номеру в первой позиции ключа (то есть символ с номером 3) и помещаем его в первую позицию расшифрованного текста. Затем то же самое делаем с символом, соотвествующим номеру во второй позиции, затем – в третьей, и т.д., после чего переходим к дешифрованию следующего блока.

Дешифрование первого блока текста из примера (ключ 365142, пробел заменен на _) приведено в таблице 4.

Таблица 11

Таблица для расшифрования

Зашифрованный текст	Действие	Расшифрованый текст
к_тТсе	Символ №1 записываем в 3-ую позицию	??**к**???
к_тТсе	Символ №2 записываем в 6-ую позицию	??к??**_**
к_**т**Тсе	Символ №3 записываем в 5-ую позицию	??к?**т**_
к_т**Т**се	Символ №4 записываем в 1-ую позицию	**Т**?к?т_
к_тТ**с**е	Символ №5 записываем в 4-ую позицию	Т?к**с**т_
к_тТс**е**	Символ №6 записываем в 2-ую позицию	Т**е**кст_

2.1.5 Метод инверсного кодирования

Исходный текст – см. пункт 2.1.1.

Шифрованный текст:

–

```
!~!r!q!u!Ґ!h!zЯ!q!~!y!r!qЯ!□!x!dЯ!k!{!o!s!u!Ґ!ґ!v!{!dЯ!s!
ґ!|!x!{!l!v!h!w!{Я!w!~!q!u!□!ґ!w!{C
0!s!u!Ґ!~!s!y!ґЯ!w!~!q!u!□!u!ҐE
1!□!v!u!ґ!x!o!ґ!Ґ!{!q!v!h!zЯ!w!~!q!u!□ЯЧ!rЯ!o!{!y!r!{!s!u
!Ґ!ґ!v!v!h!wЯ!r!w!~!j!~!v!{!~!wЦC
1!□!v!u!ґ!x!o!ґ!Ґ!{!q!v!h!zЯ!rЯ!|!ґ!□!ґ!Ґ!ґ!~!w!h!wЯ!r!w!
~!j!~!v!{!~!wЯЧ!u!qЯНЯ!□!uЯНПЦC
0!~!s!~!r!q!ґ!v!u!Ґ!y!ґЯ!r!{!w!Ґ!u!x!u!ҐC
0!uЯ!□!u!t!u!x!v!~!v!{!eЯ!□!uЯНККЯЧ!{!v!Ґ!~!s!r!v!h!zЯ!w!
~!q!u!□ЦC
3!v!u!Ъ!u!ґ!x!o!ґ!Ґ!{!q!v!h!zЯ!w!~!q!u!□ЯЧ!rЯ!o!{!y!r!{!s
!u!Ґ!ґ!v!v!h!wЯ!y!x!e!l!u!wЦC
3!v!u!Ъ!u!ґ!x!o!ґ!Ґ!{!q!v!h!zЯ!w!~!q!u!□Я!rЯ!y!x!e!l!u!wЯ
!o!{!y!r!{!s!u!Ґ!ґ!v!v!u!zЯ!□!x!{!v!hC
3!v!u!Ъ!u!ґ!x!o!ґ!Ґ!{!q!v!h!zЯ!w!~!q!u!□Я!rЯ!y!x!e!l!u!wЯ
!t!s!u!{!|!Ґ!u!x!g!v!u!zЯ!□!x!{!v!hC
```

Гистограммы шифрованного и расшифрованного файлов являются как бы зеркальным отражением друг друга, то есть если в исходной гистограмме есть несколько подряд идущих символов с вероятностями $p1$, $p2$, $p3$, то в гистограмме шифрованного текста будет находиться несколько идущих подряд символов с вероятностями $p3$, $p2$, $p1$.

Таблица 12

Смещение для некоторых символов

Символ в исходном тексте	Символ в конечном тексте	Смещение
пробел (32)	Я (223)	191
о (238)	(17)	221
т (242)	(13)	229

2.2 Метод полосок

Для шифра Цезаря имеется более простой способ расшифровки - так называемый метод полосок. На каждую полоску наносятся по порядку все буквы алфавита.

Рисунок 3 – Иллюстрация метода полосок.

В криптограмме берется некоторое слово. Полоски прикладываются друг к другу так, чтобы образовать данное слово. Двигаясь вдоль полосок, находим осмысленное словосочетание, которое и служит расшифровкой данного слова, одновременно находится и величина сдвига.

2.3 Криптоанализ при неизвестном методе шифрования

Имеется текст:

```
ЛРБОААНОРТАА РЯБ ТАО№ . 1
ПЕИМРНЕНИЕ ЛАЗРИХНЫЧ ОЕТМДЗВ ОАЫИТЩ
ТТКСЕО ОЙВИРФОНМИЦИА
```

Метод шифрования не известен. Известен только ключ: 15342.

В тексте есть только русские буквы и нет ни спецсимволов, ни латинских букв. Гистограмма шифрованного текста весьма похожа на гистограмму стандартного распределения. Поэтому можно предположить, что текст зашифрован методом перестановки. Проверим это предположение: попробуем расшифровать текст. В результате получается:

```
ЛАБОРАТОРНАЯ РАБОТА №1.
ПРИМЕНЕНИЕ РАЗЛИЧНЫХ МЕТОДОВ ЗАЩИТЫ
ТЕКСТОВОЙ ИНФОРМАЦИИ
```

Текст выглядит вполне осмысленным, из чего можно сделать вывод, что предположение было правильным.

2.4 Криптоанализ шифра XOR

Вспомним известный рассказ Эдгара По «Золотой жук». Его главный герой, Вильям Легран, нашел клочок пергамента, на котором имелась шифрованное послание пиратов о месте хранения сокровищ. Вместо букв в записке употреблялись цифры и значки, цифра 8 использовалась 34 раза, точка с запятой — 27 раз, скобка — 16 раз. Пытаясь расшифровать сообщение, Легран учел, что наиболее употребляемой буквой в английском языке является «E», за ней следуют «A», «O», «I», «H». Следовательно, можно было предположить, что цифра 8 — это и есть буква «E». А далее, используя

указанный принцип и еще некоторые лингвистические особенности английского языка, Легран успешно расшифровал послание пиратов и завладел традиционным сундуком с золотом.

Здесь следует подчеркнуть, что для такой расшифровки длина текста должна быть достаточно большой. В коротком сообщении статистические особенности языка могут не проявиться. К примеру, зашифровав описанным в начале статьи «детским» способом одно весьма распространенное послание из пяти букв, мы получим «МЯВМЯ». Герой Эдгара По, используя свой метод частоты букв, вряд ли бы догадался, что это мяукающее послание означает «ЛЮБЛЮ». Ведь буква «Л» употребляется не слишком часто, а буква «Ю» — еще реже.

В качестве примера рассмотрим криптоанализ алгоритма шифрования методом XOR. Шифруя таким способом, удается быстро зашифровать информацию от несведущего человека, но специалист её быстро взломает. И делается это следующим образом. Пусть текст будет написан на английском языке.

1) Необходимо определить длину ключа. Для этого шифрованный текст последовательно складывается по модулю 2 со своей копией, сдвинутой на различное число байтов. В полученном векторе *n* отсчитывается число совпадающих компонентов. Когда величина сдвига кратна длине ключа, это число совпадений превысит 6% от общей длины исследуемого шифрованного текста. Если не кратно, то совпадений будет меньше, чем 0,4%. Проанализировав полученные данные, можно сделать обоснованный вывод о длине ключа.
2) Затем надо сложить шифрованный текст по модулю 2 со своей копией, сдвинутой на величину длины ключа. Эта операция аннулирует ключ и оставит в наличии открытый текст сообщения, сложенный по модулю 2 со своей копией, сдвинутой на величину длины ключа.

2.5 Взлом шифра Гронсфельда

Для взлома шифра Гронсфельда необходимо найти длину повторения ключа (период), а после разбить шифровку на столбцы (количество которых должно быть равно периоду ключа), которые окажутся зашифрованными шифром Цезаря, а взломать шифр Цезаря несложно. Единственная сложность - найти период ключа (кодовой фразы). Существует несколько способов сделать это, однако в любом случае для этого необходимо, чтобы шифровка была достаточно длинной. Для этого используется метод Касиски - в шифровке ищутся повторяющиеся группы символов и из расстояния между ними делается вывод о длине периода ключа (кодовой фразы). Например, в следующей шифровке последовательность символов «4ХБ» встречается три раза:

!CZ.ЩQKF8D KWRP.TЩUZABII04-KIQOAW4O!Щ FOOЩ.(?CYY8Ъ8ABFBLYЩZЛIS! :MEWCTXЩO4?B!CWKXU5ZЩP7C9IYZX3?ZUNQËKPYPЯЩV(БН-PWH::ЩКЪJMHЗГ:?AA!CZ.4XЮЩ8Щ-U!JTAUIU?F+NCFIOUБ!EVV4OY92FHQ9!ZAQ!P5JVTFQD9LCRMIS!SGIQËY. B9ЭВМИ.X-ZG**4ХБ**Ы2N4PSVE)RQBG**4ХБ**ЩКЪ88ARKWHГTZKTMVD7MYЩ?)+DДPSCA AKBEFGR Л-LEMN8EXC2VCSK.WSQXË5C5ZMRN40F3ГИ3ГTZKTMEКЪ6ЭL.Ж.C БSIOALGPCЭ6X):VOVX96AJQIHZDCB(L:ZPЩW!4UBDЭJ.KЖL).EG5,GQPKG MRK:LVP6ЩVPEQJ9L8:Z-3,K,**4ХБ**ЩTЪ6G8ДKЖL).T6

Расстояние между повторениями составляют 16, 176 и 192 символов, наибольший общий делитель этих чисел 16 и будет искомым периодом ключа шифра Гронсфельда.

3 АЛГОРИТМЫ ШИФРОВАНИЯ ДАННЫХ С ОТКРЫТЫМ КЛЮЧОМ

Криптографические системы с открытым ключом (или асимметричное шифрование) – система шифрования и/или электронной цифровой подписи (ЭЦП), при которой открытый ключ передаётся по открытому (то есть незащищенному, доступному для наблюдения) каналу, и используется для проверки ЭЦП и для шифрования сообщения. Для генерации ЭЦП и для расшифровки сообщения используется секретный ключ.

3.1 Алгоритм RSA

Алгоритм шифрования данных с открытым ключом является наиболее перспективным в настоящий момент (RSA - Rivest, Shamir and Aldeman - его изобретатели).

Понятия.

Простое число – это такое целое число, которое делится только на 1 и на самого себя.

Взаимно простые числа не имеют ни одного общего делителя, кроме 1.

Чтобы использовать алгоритм RSA, надо сначала сгенерировать открытый и секретные ключи выполнив следующие шаги.

1) Выберем два очень больших простых числа p и q.

2) Определим n как результат умножения p на q ($n= p*q$).

3) Выберем большое случайное число, которое назовем d. Это число должно быть взаимно простым с функцией Эйлера $\varphi=(p-1)*(q-1)$.

4) Определим такое число e, для которого является истинным следующее соотношение $(e*d) \bmod \varphi =1$.

5) Назовем открытым ключом числа e и n, а секретным ключом - числа d и n.

Пример. Зашифруем и расшифруем сообщение "CAB" по алгоритму RSA. Для простоты буду использовать маленькие числа (на практике нужно брать намного большие).

1) Выберем p=3 и q=11.

2) Определим n= 3*11=33.

3) Найдем $\varphi =(p-1)*(q-1)=20$. Следовательно, d будет равно, например, 3: d=3.

4) Выберем число e по следующей формуле: $(e*3) \bmod 20=1$. Значит, e будет равно, например, 7: e=7.

5) Представим шифруемое сообщение как последовательность чисел в диапазоне от 0 до 32 (не забывайте, что диапазон кончается на n-1). Буква A =1, B=2, C=3.

6) Теперь зашифруем сообщение, используя открытый ключ {e,n}={7,33}.

C1 = $(3^7) \bmod 33 = 2187 \bmod 33 = 9$;

C2 = (1^7) mod 33 = 1 mod 33 = 1;

C3 = (2^7) mod 33 = 128 mod 33 = 29;

7) Теперь расшифруем эти данные, используя закрытый ключ {d,n}={3,33}.

M1 = (9^3) mod 33 =729 mod 33 = 3 (C);

M 2= (1^3) mod 33 =1 mod 33 = 1 (A);

M3 = (29^3) mod 33 = 24389 mod 33 = 2 (B);

Данные расшифрованы.

3.2 Контрольная работа «Алгоритмы шифрования с открытым ключом»

Задание на контрольную работу

Зашифровать указанный в варианте текст с помощью алгоритма RSA, затем расшифровать зашифрованный текст. Для этого нужно составить и отладить программу на любом языке высокого уровня. Контрольную работу оформить в редакторе MS Word. Представить задание, программный код, результаты работы программы.

Варианты заданий

Вариант 1. Зашифровать первые четыре строки из «Евгения Онегина».

Вариант 2. Зашифровать условие задачи коммивояжера.

Вариант 3. Зашифровать постановку задачи линейного программирования (без формул).

Вариант 4. Зашифровать фамилии и имена авторов криптосистемы RSA.

Вариант 5. С помощью алгоритма RSA зашифровать фразу: «В отличие от симметричного кодирования, при котором процедура расшифровки легко восстанавливается по процедуре шифрования и обратно, в схеме кодирования с открытым ключом невозможно вычислить процедуру расшифровки, зная процедуру шифрования».

Вариант 6. С помощью алгоритма RSA зашифровать текст: «Для генерации ключей нам надо уметь генерировать большие простые числа. Близкой задачей является проверка простоты целого числа».

Вариант 7. С помощью алгоритма RSA зашифровать предложение: «Для взламывания ключа в RSA нужно уметь раскладывать целое число на

множители (или, что практически то же самое, уметь вычислять функцию Эйлера)».

Вариант 8. С помощью алгоритма RSA зашифровать фразу: «Взлом ключа может интересовать только преступников, но, с другой стороны, те, кто пытаются защитить информацию, должны быть уверены, что задача разложения на множители достаточно сложна».

3.3 Криптосистема Эль-Гамаля

Схема Эль-Гамаля - криптосистема с открытым ключом, основанная на трудности вычисления дискретных логарифмов в конечном поле. Криптосистема включает в себя алгоритм шифрования и алгоритм цифровой подписи. Схема Эль-Гамаля лежит в основе стандартов электронной цифровой подписи.

Алгоритм работы схемы Эль-гамаля следующий.

1. Генерируется случайное простое число p длины n битов.
2. Выбирается произвольное целое число g, являющееся первообразным корнем по модулю p. Первообразным корнем по модулю p называется такое целое число g ($g < p$), для которого: а) все степени $g^1 \ldots g^{p-1}$ по модулю p различны; б) для любого целого числа x, такого что $1 \le x \le p-1$, найдется n, при котором $a = g^n \bmod p$.
3. Выбирается случайное целое число x такое, что $1 < x < p$.
4. Вычисляется $y = g^x \bmod p$.
5. Открытым ключом является тройка (p, g, y), закрытым – число x.

3.4 Процедура открытого распределения ключей Диффи-Хеллмана

Асимметричные криптографические системы позволяют распределять секретные ключи по открытым каналам, то есть каналам, которые потенциально могут быть прослушаны противником. Такая процедура открытого распределения ключей была впервые опубликована в 1976 году в работе У. Диффи и М.Э. Хеллмана «Новые направления в криптографии».

В основе процедуры Диффи–Хеллмана лежит использование односторонней функции дискретного возведения в степень:

$$F(x) = g^x \bmod p,$$

где x - целое число ($1 \le x \le p-1$),

p - простое число,

g - первообразный корень по модулю p.

Процедура Диффи–Хеллмана для открытого распределения ключей заключается в следующем. Для начала выбирается большое простое число p и число g - первообразный корень по модулю p. Для обеспечения стойкости число p должно иметь длину, большую или равную 512 бит (количество бит в двоичной записи этого числа), и разложение числа $p-1$ на множители должно

содержать хотя бы один большой простой множитель (например, $p-1 = 2q$, где q - простое число). При таком выборе числа p в настоящее время не существует эффективного алгоритма для решения задачи инвертирования функции $F(x)$.

Каждый абонент в качестве своего секретного ключа выбирает некоторое случайное число x, по которому вычисляет свой открытый ключ $y = g^x \bmod p$.

Все абоненты помещают свои открытые ключи в общедоступный справочник.

После этого, если два абонента, А и В, захотят обменяться секретным сообщением, они берут из общедоступного справочника открытые ключи друг друга (соответственно, y_A и y_B) и вычисляют общий секретный ключ:

1) абонент А вычисляет $Z_A = (y_B)^{x_A} = (g^{x_B})^{x_A} \bmod p = g^{x_A x_B} \bmod p$,

2) абонент В вычисляет $Z_B = (y_A)^{x_B} = (g^{x_A})^{x_B} \bmod p = g^{x_A x_B} \bmod p$.

Таким образом, после выполнения описанной процедуры у абонентов А и В есть общее число $z_A = z_B$. Это число они при обмене сообщениями могут использовать в качестве ключа для шифрования (например, методом гаммирования). Противник знает числа $y_A = g^{x_A} \bmod p$ и $y_B = g^{x_B} \bmod p$, но для того чтобы определить секретный ключ, ему необходимо решить задачу дискретного логарифмирования (по известным y_A и y_B вычислить x_A и x_B). Для этой задачи в настоящее время не существует эффективного алгоритма.

КРИПТОГРАММЫ ДЛЯ РАСШИФРОВКИ

Криптограмма 1

Дана криптограмма:

```
CO *  N  = CPC
 +    *    -
II  +  I   = OY
 =    =    =
EDP + TR  = ETO
```

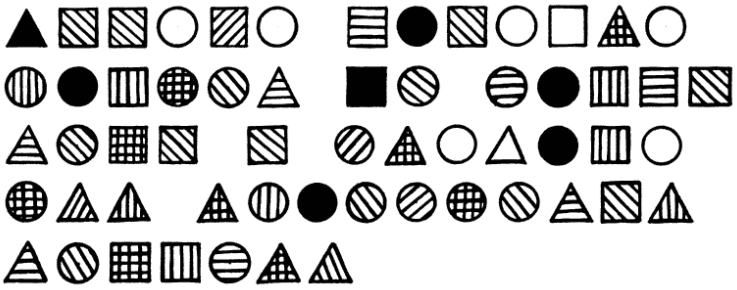
Восстановите цифровые значения букв, при которых справедливы все указанные равенства, если разным буквам соответствуют различные цифры. Расставьте буквы в порядке возрастания их цифровых значений и получите искомое слово.

Криптограмма 2

Каждая буква фрагмента известного стихотворения Ф.И. Тютчева заменена некоторой буквой так, что разным буквам соответствуют разные буквы, а одинаковым - одинаковые. Пробелы и знаки препинания сохранены. Восстановите этот фрагмент стихотворения:

Гьюь Фюббшн эй яюэовл,
Пфзшэюь юришь эй шчьйфшвл:
Г эйщ юбюрйээпо бвпвл —
С Фюббшн ьюцэю вюылъю сйфшвл.

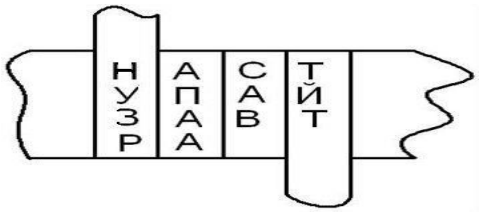
Криптограмма 3. Пользуясь ключом, разгадай головоломку и прочти стих из Библии.



КЛЮЧ

ОТВЕТЫ НА ЗАДАНИЯ

Страница 6.



Страница 13. Пришел, увидел, победил!

Страница 14. Я умею работать с шифром! А ты?

Страница 19. Эта наука интересная и перспективная

Страница 20. Криптография

Страница 26. монитор, принтер

Страница 53.

Криптограмма 1. DECRYPTION

Криптограмма 2. *Умом Россию не понять,*
Аршином общим не измерить:
У ней особенная стать –
В Россию можно только верить.

ВОПРОСЫ ДЛЯ САМОПРОВЕРКИ

1. Понятие криптологии.
2. Криптография. Определение. Основные понятия.
3. Криптоанализ. Определение. Основные понятия.
4. Криптографические методы защиты информации.
5. Классификация криптосистем.
6. Симметричные и ассиметричные криптосистемы.
7. Симметричные криптосистемы.
8. Шифры замены и перестановки.
9. Шифрование простой заменой.
10. Шифрование омофонной заменой.
11. Шифрование блочной заменой.
12. Шифрование многоалфавитной заменой.
13. Шифрование перестановкой.
14. Шифрование с помощью одноразового блокнота.
15. Роторные машины для шифрования.
16. Операция сложения по модулю 2. Возможность применения в криптографии.
17. Потоковые шифры.
18. Основные идеи цифровой подписи.
19. Ассиметричные криптосистемы.
20. Система шифрования RSA.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

Основная литература

Полянская О. Ю. Инфраструктуры открытых ключей: учебное пособие. – М.: Изд. БИНОМ, 2007

Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. – Изд. Наука и техника, 2004

Запечников С.В., Милославская Н.Г., Толстой А.И., Ушаков Д.В. Информационная безопасность открытых систем. – Изд. Горячая Линия-Телеком, 2006

Шанкин Г.П., Бабаш А.В. Криптография. – Изд. Солон, 2007

Хорев П.Б. Методы и средства защиты информации в компьютерных системах: учебное пособие. – Изд. Academia, 2007

Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие. – Изд. Форум Инфра-М, 2008

Дополнительная литература

Нильс Фергюсон, Брюс Шнайер Практическая криптография. Пер. с англ. – Изд. Вильямс, 2005

Мао В. Современная криптография: теория и практика. Пер. с англ. – Изд. Вильямс, 2005

Макнамара Д. Секреты компьютерного шпионажа: Тактика и контрмеры. Пер. с англ. – М.: Изд. БИНОМ, 2006

Запечников С.В. Криптографические протоколы и их применение в финансовой и коммерческой деятельности: учебное пособие. – Изд. Горячая Линия-Телеком, 2007

Молдовян Н.А. Практикум по криптосистемам с открытым ключом. – Изд. BHV, 2007

Смарт Н. Криптография. Пер. с англ. – Изд. Техносфера, 2006