ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ
Северо-Кавказский филиал
ордена Трудового Красного Знамени федерального государственного
бюджетного образовательного учреждения высшего образования
«Московский технический университет связи и информатики»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ
по проведению практических занятий
для дисциплины «Основы криптографии»

Направление подготовки: **11.03.02 Инфокоммуникационные технологии и системы связи**

Профиль: Защищенные системы и сети связи

Ростов на Дону
2019

Рыбалко И.П.

Методические указания по проведению практических занятий по дисциплине «Основы криптографии»/ Рыбалко И.П. – Ростов-на -Дону: Изд-во СКФ МТУСИ, 2019. – 49 с.: ил.

Методические указания соответствуют направлению подготовки: 11.03.02 Инфокоммуникационные технологии и системы связи, профилю: защищенные системы и сети связи.

В указаниях приведены общие сведения о криптографии. Рассмотрены основные методы симметричного и асимметричного шифрования. Приведены задания на выполнение лабораторных работ и даны рекомендации по их выполнению.

Указания предназначены для студентов любых форм обучения, изучающих информационную безопасность и защиту информации, а также специалистов, ведущим проектирование, разработку и эксплуатацию информационных систем.

Оглавление

Введение

Тема «Криптографические методы защиты информации» является базовым при подготовке специалистов по защите информации. На основе знаний криптографии выстраивается система подготовки специалистов. При этом изучение методов защиты неразрывно связано с изучением возможных атак на алгоритмы и на их реализации. Хорошо известно, что для усвоения материала необходима активная самостоятельная работа студентов. Поэтому представляется целесообразным проведение лабораторных работ по криптоанализу. Работы по анализу таких шифров, как DES, ГОСТ 28147-89, IDEA требуют большого ресурса и для начинающего являются чрезвычайно сложными. В то же время на примерах классических шифров можно проиллюстрировать некоторые важные приемы и методы криптоанализа. Как показывает практика работы, студенты после анализа шифров перестановки, простой замены и Виженера уверенно и достаточно быстро входят в круг идей современной криптографии. Таким образом, настоящее пособие выполняет пропедевтическую функцию. После анализа классических шифров учащиеся успешно изучают современные блочные алгоритмы шифрования, им становятся доступными идеи линейного и дифференциального криптоанализа.

Авторы сочли необходимым теоретические сведения дополнить подробно изложенными примерами выполнения заданий. После изучения теории и ознакомления с образцами решений заданий студент должен выполнить свой вариант лабораторной работы. Мы не приводим ответы к задачам, дабы не лишать обучающихся удовольствия от самостоятельного решения.

1. Классические шифры

Разработкой методов преобразования *(шифрования)* информации с целью ее защиты от незаконных пользователей занимается *криптография.* Такие методы и способы преобразования информации называются *шифрами.*

Шифрование (зашифрование) - процесс применения шифра к защищаемой информации, т. е. преобразование защищаемой информации *(открытого текста)* в шифрованное сообщение *(шифртекст, криптограмму)* с помощью определенных правил, содержащихся в шифре.

Дешифрование - процесс, обратный шифрованию, т. е. преобразование шифрованного сообщения в защищаемую информацию с помощью определенных правил, содержащихся в шифре.

Криптография - прикладная наука, она использует самые последние достижения фундаментальных наук и, в первую очередь, математики. С другой стороны, все конкретные задачи криптографии существенно зависят от уровня развития техники и технологии, от применяемых средств связи и способов передачи информации.

Современная *криптография* является областью знаний, связанной с решением таких проблем безопасности информации, как конфиденциальность, целостность, аутентификация и невозможность отказа сторон от авторства. Достижение этих требований безопасности информационного взаимодействия и составляет основные цели криптографии. Они определяются следующим образом.

Обеспечение *конфиденциальности* - решение проблемы защиты информации от ознакомления с ее содержанием со стороны лиц, не имеющих права доступа к ней. В зависимости от контекста вместо термина "конфиденциальная" информация могут выступать термины "секретная", "частная", "ограниченного доступа" информация.

Обеспечение *целостности* - гарантирование невозможности несанкционированного изменения информации. Для гарантии целостности необходим

простой и надежный критерий обнаружения любых манипуляций с данными. Манипуляции с данными включают вставку, удаление и замену.

Обеспечение *аутентификации* - разработка методов подтверждения подлинности сторон *(идентификация)* и самой информации в процессе информационного взаимодействия. Информация, передаваемая по каналу связи, должна быть аутентифицирована по источнику, времени создания, содержанию данных, времени пересылки и т. д.

Обеспечение *невозможности отказа от авторства* - предотвращение возможности отказа субъектов от некоторых из совершенных ими действий. Рассмотрим средства для достижения этих целей более подробно.

Традиционной задачей криптографии является проблема обеспечения конфиденциальности информации при передаче сообщений по контролируемому противником каналу связи. В простейшем случае эта задача описывается взаимодействием трех субъектов (сторон). Владелец информации, называемый обычно *отправителем,* осуществляет преобразование исходной *(открытой)* информации (сам процесс преобразования называется *шифрованием)* в форму передаваемых *получателю* по открытому каналу связи *шифрованных* сообщений с целью ее защиты от противника.

Под *противником* понимается любой субъект, не имеющий права ознакомления с содержанием передаваемой информации. В качестве противника может выступать *криптоаналитик,* владеющий методами раскрытия шифров. Законный получатель информации осуществляет *расшифрование* полученных сообщений. Противник пытается овладеть защищаемой информацией (его действия обычно называют *атаками).* При этом он может совершать как пассивные, так и активные действия. *Пассивные* атаки связаны с прослушиванием, анализом трафика, перехватом, записью передаваемых шифрованных сообщений, *дешифрованием,* то есть попытками "взломать" защиту с целью овладения информацией.

При проведении *активных* атак противник может прерывать процесс передачи сообщений, создавать поддельные (сфабрикованные) или модифи-

цировать передаваемые шифрованные сообщения. Эти активные действия называют попытками *имитации* и *подмены* соответственно.

Под *шифром* обычно понимается семейство обратимых преобразований, каждое из которых определяется некоторым параметром, называемым ключом, а также порядком применения данного преобразования, называемым *режимом шифрования*.

Ключ - это важнейший компонент шифра, отвечающий за выбор преобразования, применяемого для зашифрования конкретного сообщения. Обычно ключ представляет собой некоторую буквенную или числовую последовательность. Эта последовательность как бы "настраивает" алгоритм шифрования.

Каждое преобразование однозначно определяется ключом и описывается некоторым *криптографическим алгоритмом.* Один и тот же криптографический алгоритм может применяться для шифрования в различных режимах. Тем самым реализуются различные способы шифрования (простая замена, гаммирование и т. п.). Каждый режим шифрования имеет как свои преимущества, так и недостатки. Поэтому выбор режима зависит от конкретной ситуации. При расшифровании используется криптографический алгоритм, который в общем случае может отличаться от алгоритма, применяемого для зашифрования сообщения. Соответственно могут различаться ключи зашифрования и расшифрования. Пару алгоритмов зашифрования и расшифрования обычно называют *криптосистемой (шифрсистемой),* а реализующие их устройства - *шифртехникой.*

Если обозначить через *M* открытое, а через *C* шифрованное сообщения, то процессы зашифрования и расшифрования можно записать в виде равенств

$E_{k1}(M)=C$

$D_{k2}(C)=M$

в которых алгоритмы зашифрования *E* и расшифрования *D* должны удовлетворять равенству

$D_{k2}(E_{k1}(M))=M$

Наряду с конфиденциальностью не менее важной задачей является обеспечение *целостности* информации, другими словами, - неизменности ее в процессе передачи или хранении. Решение этой задачи предполагает разработку средств, позволяющих обнаруживать не столько случайные искажения (для этой цели вполне подходят методы теории кодирования с обнаружением и исправлением ошибок), сколько целенаправленное навязывание противником ложной информации. Для этого в передаваемую информацию вносится избыточность. Как правило, это достигается добавлением к сообщению некоторой проверочной комбинации, вычисляемой с помощью специального алгоритма и играющей роль контрольной суммы для проверки целостности полученного сообщения. Главное отличие такого метода от методов теории кодирования состоит в том, что алгоритм выработки проверочной комбинации является "криптографическим", то есть зависящим от секретного ключа. Без знания секретного ключа вероятность успешного навязывания противником искаженной или ложной информации мала. Такая вероятность служит мерой *имитостойкости* шифра, то есть способности самого шифра противостоять активным атакам со стороны противника.

Итак, для проверки целостности к сообщению *M* добавляется проверочная комбинация *S,* называемая *кодом аутентификации сообщения* (сокращенно - КАС) или *имитовставкой.* В этом случае по каналу связи передается пара *C = (M, S).* При получении сообщения *M* пользователь вычисляет значение проверочной комбинации и сравнивает его с полученным контрольным значением *S* Несовпадение говорит о том, что данные были изменены.

Как правило, код аутентификации является значением некоторой (зависящей от секретного ключа) криптографической *хеш-функции* от данного сообщения: $h_k(M) = S$ К кодам аутентификации предъявляются определенные требования. К ним относятся:

- невозможность вычисления значения $h_k(M) = S$ для заданного сообщения M без знания ключа k,

- невозможность подбора для заданного сообщения M с известным значением $h_k(M)=S$ другого сообщения M_1 с известным значением h_k (M_1) = S_1, без знания ключа k.

Первое требование направлено против создания поддельных (сфабрикованных) сообщений при атаках типа *имитация;* второе - против модификации передаваемых сообщений при атаках типа *подмена.*

Аутентификация - установление подлинности. В общем случае этот термин может относиться ко всем аспектам информационного взаимодействия: сеансу связи, сторонам, передаваемым сообщениям и т. д.

Установление подлинности (то есть проверка и подтверждение) всех аспектов информационного взаимодействия является важной составной частью проблемы обеспечения достоверности получаемой информации. Особенно остро эта проблема стоит в случае не доверяющих друг другу сторон, когда источником угроз может служить не только третья сторона (противник), но и сторона, с которой осуществляется взаимодействие.

Применительно к сеансу связи аутентификация означает проверку: целостности соединения, невозможности повторной передачи данных противником и своевременности передачи данных. Для этого, как правило, используют дополнительные параметры, позволяющие "сцепить" передаваемые данные в легко проверяемую последовательность. Это достигается, например, путем вставки в сообщения некоторых специальных чисел или *меток времени.* Они позволяют предотвратить попытки повторной передачи, изменения порядка следования или обратной отсылки части переданных сообщений. При этом такие вставки в передаваемом сообщении необходимо защищать (например, с помощью шифрования) от возможных подделок и искажений.

Применительно к сторонам взаимодействия аутентификация означает проверку одной из сторон того, что взаимодействующая с ней сторона -

именно та, за которую она себя выдает. Часто аутентификацию сторон называют также *идентификацией*.

Основным средством для проведения идентификации являются *протоколы идентификации,* позволяющие осуществлять идентификацию (и аутентификацию) каждой из участвующих во взаимодействии и не доверяющих друг другу сторон. Различают *протоколы односторонней* и *взаимной идентификации.*

Протокол - это распределенный алгоритм, определяющий последовательность действий каждой из сторон. В процессе выполнения протокола идентификации каждая из сторон не передает никакой информации о своем секретном ключе, а хранит его у себя и использует для формирования ответных сообщений на запросы, поступающие при выполнении протокола.

Наконец, применительно к самой информации аутентификация означает проверку того, что информация, передаваемая по каналу, является подлинной по содержанию, источнику, времени создания, времени пересылки и т. д.

Проверка подлинности содержания информации сводится, по сути, к проверке ее неизменности (с момента создания) в процессе передачи или хранения, то есть проверке целостности.

Аутентификация источника данных означает подтверждение того, что исходный документ был создан именно заявленным источником.

Заметим, что если стороны доверяют друг другу и обладают общим секретным ключом, то аутентификацию сторон можно обеспечить применением кода аутентификации. Действительно, каждое успешно декодированное получателем сообщение может быть создано только отправителем, так как только он знает их общий секретный ключ. Для не доверяющих друг другу сторон решение подобных задач с использованием общего секретного ключа становится невозможным. Поэтому при аутентификации источника данных нужен механизм цифровой подписи, который будет рассмотрен ниже.

В целом, аутентификация источника данных выполняет ту же роль, что и протокол идентификации. Отличие заключается только в том, что в первом случае имеется некоторая передаваемая информация, авторство которой требуется установить, а во втором требуется просто установить сторону, с шторой осуществляется взаимодействие.

2. Математические модели открытого текста

Потребность в математических моделях открытого текста продиктована, прежде всего, следующими соображениями. Во-первых, даже при отсутствии ограничений на временные и материальные затраты по выявлению закономерностей, имеющих место в открытых текстах, нельзя гарантировать того, что такие свойства указаны с достаточной полнотой. Например, хорошо известно, что частотные свойства текстов в значительной степени зависят от их характера. Поэтому при математических исследованиях свойств шифров прибегают к упрощающему моделированию, в частности, реальный открытый текст заменяется его моделью, отражающей наиболее важные его свойства. Во-вторых, при автоматизации методов криптоанализа, связанных с перебором ключей, требуется "научить" ЭВМ отличать открытый текст от случайной последовательности знаков. Ясно, что соответствующий критерий может выявить лишь адекватность последовательности знаков некоторой модели открытого текста.

Один из естественных подходов к моделированию открытых текстов связан с учетом их частотных характеристик, приближения для которых можно вычислить с нужной точностью, исследуя тексты достаточной длины. Основанием для такого подхода является устойчивость частот *к* - грамм или целых словоформ реальных языков человеческого общения (то есть отдельных букв, слогов, слов и некоторых словосочетаний). Основанием для построения модели может служить также и теоретико-информационный подход, развитый в работах К. Шеннона.

Учет частот k-грамм приводит к следующей модели открытого текста. Пусть $P^{(k)}(A)$ представляет собой массив, состоящий из приближений для вероятностей $p(b_1,b_2,...,b_k)$ появления k - грамм $b_1 b_2 ... b_k$ в открытом тексте, $k \in N$,

$A = (a_1 ,...,a_n)$ - алфавит открытого текста, $b_i \in A$, $i = 1,k$.

Тогда источник "открытого текста" генерирует последовательность $c_1,c_2,...,c_k,c_{k+1},...$ знаков алфавита A, в которой k-грамма $c_1 c_2 ... c_k$ появляется с

вероятностью $p(c_1c_2...c_k) \in P^{(k)}(A)$, следующая k-грамма $c_1c_2...c_{k+1}$ появляется с вероятность $p(c_2c_3...c_{k+1}) \in P^{(k)}(A)$ и т. д. Назовем построенную модель открытого текста *вероятностной моделью k-го приближения.*

Таким образом, простейшая модель открытого текста - *вероятностная модель первого приближения* – представляет собой последовательность знаков $c_1, c_2, ...$, в которой каждый знак ci, $i = 1,2,...$, появляется с вероятностью $p(c_i) \in P^{(1)}(A)$, независимо от других знаков. Будем называть также эту модель *позначной моделью открытого текста.* В такой модели открытый текст $c_1c_2...c_1$ имеет вероятность

$$p(c_1c_2...c_l) = \prod_{i=1}^{l} p(c_i) .$$

В вероятностной модели второго приближения первый знак c_1 имеет вероятность $p(c_{1)} \in P^{(1)}(A)$, а каждый следующий знак c_i зависит от предыдущего и появляется с вероятностью

$$p(c_i / c_{i-1}) = \frac{p(c_{i-1}c)}{p(c_{i-1})} ,$$

где $p(c_{i-1}c_i) \in P^{(2)}(A)$, $p(c_{i-1}) \in P^{(1)}(A)$, $i = 2,3,...$. Другими словами, модель открытого текста второго приближения представляет собой *простую однородную цепь Маркова.* В такой модели открытый текст $c_1c_2...c_l$ имеет вероятность

$$p(c_1c_2...c_l) = p(c_1) \cdot \prod_{i=2}^{l} p(c_i / c_{i-1}) .$$

Модели открытого текста более высоких приближений учитывают зависимость каждого знака от большего числа предыдущих знаков. Ясно, что чем выше степень приближения, тем более "читаемыми" являются соответствующие модели. Проводились эксперименты по моделированию открытых текстов с помощью ЭВМ.

Отметим, что с более общих позиций открытый текст может рассматриваться как реализация *стационарного эргодического случайного процесса с дискретным временем и конечным числом состояний*.

Критерии распознавания открытого текста

Заменив реальный открытый текст его моделью, мы можем теперь построить критерий распознавания открытого текста. При этом можно воспользоваться либо стандартными методами различения статистических гипотез, либо наличием в открытых текстах некоторых запретов, таких, например, как биграмма ЪЪ в русском тексте. Проиллюстрируем первый подход при распознавании позначной модели открытого текста.

Итак, согласно нашей договоренности, открытый текст представляет собой реализацию независимых испытаний случайной величины, значениями которой являются буквы алфавита $A = \{a_1,...,a_n\}$, появляющиеся в соответствии с распределением вероятностей $P^{(1)}(A) = (p(a_1),...,p(a_n))$. Требуется определить, является ли случайная последовательность $c_1c_2...c_l$ букв алфавита A открытым текстом или нет.

Пусть H_0 - гипотеза, состоящая в том, что данная последовательность - открытый текст, H_1 - альтернативная гипотеза. В простейшем случае последовательность $c_1c_2...c_l$ можно рассматривать при гипотезе H_1 как случайную и равновероятную. Эта альтернатива отвечает субъективному представлению о том, что при расшифровании криптограммы с помощью ложного ключа получается "бессмысленная" последовательность знаков. В более общем случае можно считать, что при гипотезе H1 последовательность $c_1c_2...c_l$ представляет собой реализацию независимых испытаний некоторой случайной величины, значениями которой являются буквы алфавита $A = \{a_1,...,a_n\}$, появляющиеся в соответствии с распределением вероятностей $Q^{(1)}(A)= (q(a_l),...,q(a_n))$. При таких договоренностях можно применить, например, *наиболее мощный критерий* различения двух простых гипотез, который дает *лемма Неймана—Пирсона*.

В силу своего вероятностного характера такой критерий может совершать ошибки двух родов. Критерий может принять открытый текст за случайный набор знаков. Такая ошибка обычно называется *ошибкой первого ро-*

да, ее вероятность равна $\alpha = p\{H_1/H_0\}$. Аналогично вводится *ошибка второго рода* и ее вероятность $\beta = p\{H_0/H_1\}$. Эти ошибки определяют качество работы критерия. В криптографических исследованиях естественно минимизировать вероятность ошибки первого рода, чтобы не "пропустить" открытый текст. Лемма Неймана - Пирсона при заданной вероятности первого рода минимизирует также вероятность ошибки второго рода.

Критерии на открытый текст, использующие запретные сочетания знаков, например *к* - граммы подряд идущих букв, будем называть *критериями запретных k-грамм.* Они устроены чрезвычайно просто. Отбирается некоторое число *s* редких *k*-грамм, которые объявляются запретными. Теперь, просматривая последовательно *k*-грамму за *k*-граммой анализируемой последовательности $c_1c_2...c_l$, мы объявляем ее случайной, как только в ней встретится одна из запретных *k*-грамм, и открытым текстом в противном случае. Такие критерии также могут совершать ошибки в принятии решения. В простейших случаях их можно рассчитать. Несмотря на свою простоту, критерии запретных *k*-грамм являются весьма эффективными.

3. Классификация шифров

В качестве первичного признака, по которому производится классификация шифров, используется тип преобразования, осуществляемого с открытым текстом при шифровании. Если фрагменты открытого текста (отдельные буквы или группы букв) заменяются некоторыми их эквивалентами в шифртексте, то соответствующий шифр относится к классу *шифров замены.* Если буквы открытого текста при шифровании лишь меняются местами друг с другом, то мы имеем дело с *шифром перестановки.* С целью повышения надежности шифрования шифрованный текст, полученный применением некоторого шифра, может быть еще раз зашифрован с помощью другого шифра. Всевозможные такие композиции различных шифров приводят к третьему классу шифров, которые обычно называют *композиционными шифрами.* Заметим, что композиционный шифр может не входить ни в класс шифров замены, ни в класс шифров перестановки (рис. 1).

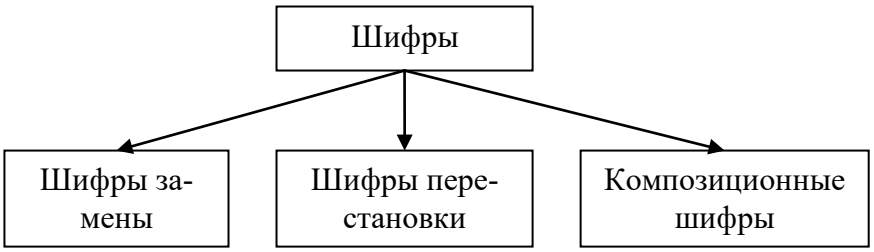


Рисунок 1. Классификация шифров

Шифры перестановки

Шифры перестановки, или транспозиции, изменяют только порядок следования символов или других элементов исходного текста. Классическим примером такого шифра является система, использующая карточку с отверстиями – *решетку Кардано,* которая при наложении на лист бумаги оставляет открытыми лишь некоторые его части. При зашифровке буквы сообщения вписываются в эти отверстия. При расшифровке сообщение вписывается в диаграмму нужных размеров, затем накладывается решетка, после чего на виду оказываются только буквы открытого текста.

Решетки можно использовать двумя различными способами. В первом случае зашифрованный текст состоит только из букв исходного сообщения. Решетка изготавливается таким образом, чтобы при ее последовательном использовании в различных положениях каждая клетка лежащего под ней листа бумаги оказалась занятой. Примером такой решетки является *поворотная решетка,* показанная на рис.1. Если такую решетку последовательно поворачивать на 90° после заполнения всех открытых при данном положении клеток, то при возврате решетки в исходное положение все клетки окажутся заполненными. Числа, стоящие в клетках, облегчают изготовление решетки. В каждом из концентрических окаймлений должна быть вырезана только одна клетка из тех, которые имеют одинаковый номер. Второй, стеганографический метод использования решетки позволяет скрыть факт передачи секретного сообщения. В этом случае заполняется только часть листа бумаги, лежащего под решеткой, после чего буквы или слова исходного текста окружаются ложным текстом.

1	2	3	4	5	1
5	1	2	3	1	2
4	3	1	1	2	3
3	2	1	1	3	4
2	1	3	2	1	5
1	5	4	3	2	1

Рисунок 2. Пример поворотной решетки

Рассмотрим усложненную перестановку по таблице. Пример таблицы для реализации этого метода шифрования показан на рис.3. Таблица представляет собой матрицу размерностью 6 х 6, в которую построчно вписывается искомое сообщение. При считывании информации по столбцам в соответствии с последовательностью чисел ключа получается шифротекст. Усложнение заключается в том, что некоторые ячейки таблицы не использу-

ются. При зашифровании сообщения

КОМАНДОВАТЬ ПАРАДОМ БУДУ Я

получим:

ОЬБНАОДКДМУМВ АУ ОТР ААПДЯ,

Ключ					
2	4	0	3	5	1
К	О		М	А	Н
Д		О	В	А	
	Т	Ь		П	А
	Р		А	Д	О
М		Б	У		Д
У				Я	

Рисунок 3. Пример шифрования методом усложненной перестановки по таблице

При расшифровании буквы шифротекста записываются по столбцам в соответствии с последовательностью чисел ключа, после чего исходный текст считывается по строкам. Для удобства запоминания ключа применяют перестановку столбцов таблицы по ключевому слову или фразе, всем символам которых ставятся в соответствие номера, определяемые порядком соответствующих букв в алфавите. Например, при выборе в качестве ключа слова ИНГОДА последовательность использования столбцов будет иметь вид 462531.

Также возможны и другие варианты шифра перестановки, например, шифры столбцовой и двойной перестановки.

Шифры замены

Большое влияние на развитие криптографии оказали появившиеся в середине XX века работы американского математика Клода Шеннона. В этих работах были заложены основы теории информации, а также был разработан математический аппарат для исследований во многих областях науки, связанных с информацией. Более того, принято считать, что теория информации как наука родилась в 1948 году после публикации работы К. Шеннона «Математическая теория связи» (см. приложение).

В своей работе «Теория связи в секретных системах» Клод Шеннон обобщил накопленный до него опыт разработки шифров. Оказалось, что даже в очень сложных шифрах в качестве типичных компонентов можно выделить такие простые шифры как *шифры замены, шифры перестановки* или их сочетания.

Шифр замены является простейшим, наиболее популярным шифром. Типичными примерами являются шифр Цезаря, «цифирная азбука» Петра Великого и «пляшущие человечки» А. Конан Дойла. Как видно из самого названия, шифр замены осуществляет преобразование замены букв или других «частей» открытого текста на аналогичные «части» шифрованного текста. Легко дать математическое описание шифра замены. Пусть X *и* Y – два алфавита (открытого и шифрованного текстов соответственно), состоящие из одинакового числа символов. Пусть также $g: X \longrightarrow Y$ - взаимнооднозначное отображение X в Y. Тогда шифр замены действует так: открытый текст $x_1x_2...x_n$ преобразуется в шифрованный текст $g(x_1)g(x_2)... g(x_n)$.

Шифр перестановки, как видно из названия, осуществляет преобразование перестановки букв в открытом тексте. Типичным примером шифра перестановки является шифр «Сцитала». Обычно открытый текст разбивается на отрезки равной длины и каждый отрезок шифруется независимо. Пусть, например, длина отрезков равна n и σ - взаимнооднозначное отображение множества $\{1,2,..., n\}$ в себя. Тогда шифр перестановки действует так: отрезок открытого текста $x_1...x_n$ преобразуется в отрезок шифрованного текста

Математическая модель шифра замены

Определим модель Σ_A =*(X, K ,Y, E, D)* произвольного шифра замены. Будем считать, что открытые и шифрованные тексты являются словами в алфавитах *A и B* соответственно: $X \subset A^*$, $Y \subset B^*$, $|A|=n$, $|B| = m$. Здесь и далее C* обозначает множество слов конечной длины в алфавите C.

Перед зашифрованием открытый текст предварительно представляется в виде последовательности подслов, называемых *шифрвеличинами.* При зашифровании шифрвеличины заменяются некоторыми их эквивалентами в шифртексте, которые назовем *шифробозначениями.* Как шифрвеличины, так и шифробозначения представляют собой слова из A^* и B^* соответственно.

Пусть $U = \{u_1,..,u_N\}$ — множество возможных шифрвеличин, $V = \{v_1,...,v_M\}$ - множество возможных шифробозначений. Эти множества должны быть такими, чтобы любые тексты $x \in X$, $y \in Y$ можно было представить словами из U^*, V^* соответственно. Требование однозначности расшифрования влечет неравенства $N \geq n$, $M \geq m$, $M \geq N$. Для определения правила зашифрования $E_k(x)$ в общем случае нам понадобится ряд обозначений и понятие *распределителя,* который, по сути, и будет выбирать в каждом такте шифрования замену соответствующей шифрвеличине.

Поскольку $M \geq N$, множество V можно представить в виде объединения $V = \bigcup_{i=1}^{N} V_\alpha^{(i)}$ непересекающихся непустых подмножеств $V^{(i)}$. Рассмотрим произвольное семейство, состоящее из r таких разбиений множества V:

$$V = \bigcup_{i=1}^{N} V_\alpha^{(i)},\ \alpha = \overline{1,r},\ r \in N,$$

и соответствующее семейство биекций

$$\varphi_\alpha : U \to \{V_\alpha^{(1)},...,V_\alpha^{N}\},$$

для которых $\varphi_\alpha(u_i) = V_\alpha^{(i)},\ i = \overline{1,N}$.

Рассмотрим также произвольное отображение $\psi : K \times N \to N_r^*$, где $N_r = \{1,2,...,r\}$, такое, что для любых $k \in K, l \in N$

$\psi(k,l) = \alpha_1^{(k)}...\alpha_l^{(k)}, \alpha_j^{(k)} \in N_r, \quad j = \overline{1,l}.$

Назовем последовательность $\psi(к,1)$ *распределителем,* отвечающим данным значениям $к \in K$, $l \in$ N.

Теперь мы сможем определить правило зашифрования произвольного шифра замены. Пусть

$x \in X$, $x = x_1...x_l$, $x_i \in U$, $i = 1,l$; $k \in K$

и $\psi(к,I) = a_1^{(k)}...a_1^{(k)}$. Тогда $E_к(x) = y$, где $y = y_1...y_l$,

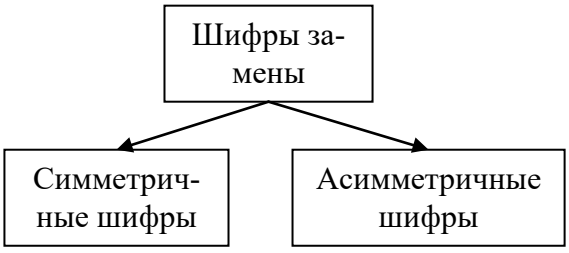
$y_j = \varphi_{\alpha_j^{(k)}}(x), \ j = \overline{1,l}.$

В качестве y_j можно выбрать любой элемент множества m $\varphi_{\alpha_j^{(k)}}(x_j)$. Всякий раз при шифровании этот выбор можно производить случайно, например, с помощью некоторого *рандомизатора* типа игровой рулетки. Подчеркнем, что такая многозначность при зашифровании не препятствует расшифрованию, так как $V_\alpha^{(i)} \bigcap V_\alpha^{(j)} = \emptyset$ при $i \neq j$.

Классификация шифров замены

Если ключ зашифрования совпадает с ключом расшифрования: $k_3 = k_p$, то такие шифры называют *симметричными,* если же $k_3 \neq k_p$ — *асимметричными.*

В связи с указанным различием в использовании ключей сделаем еще один шаг в классификации:



Отметим также, что в приведенном определении правило зашифрования E_k(x) является, вообще говоря, *многозначной функцией.* Выбор ее значе-

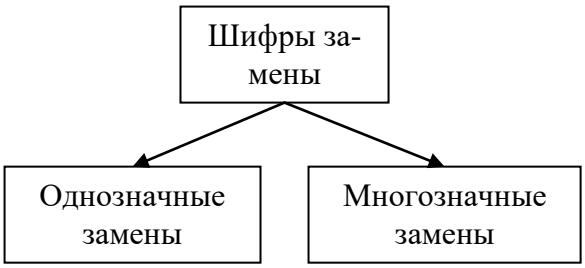
ний представляет собой некоторую проблему, которая делает многозначные функции $E_k(x)$ не слишком удобными для использования. Избавиться от этой проблемы позволяет использование однозначных функций, что приводит к естественному разделению всех шифров замены на *однозначные* и *многозначные замены* (называемых также в литературе *омофонами).*

Для однозначных шифров замены справедливо свойство:

$$\forall \alpha, i : \left|V_\alpha^{(i)}\right| = 1;$$

для многозначных шифров замены:

$$\exists \alpha, i : \left|V_\alpha^{(i)}\right| > 1;$$



Исторически известный шифр - *пропорциональной замены* представляет собой пример шифра многозначной замены, *шифр гаммирования* - пример шифра однозначной замены. Далее мы будем заниматься в основном изучением однозначных замен, получивших наибольшее практическое применение. Итак, далее $M = N$ и $\varphi_\alpha(u_i) = v_{\alpha,i}$, $i = \overline{1,M}$.

Заметим, что правило зашифрования E_k естественным образом индуцирует отображение $\tilde{E}_k : U \to V$, которое в свою очередь продолжается до отображения $\tilde{E}_k : U^* \to V^*$. Для упрощения записи будем использовать одно обозначение E_k для каждого из трех указанных отображений.

В силу инъективности (по k) отображения E_k и того, что $|U| = |V|$, введенные в общем случае отображения φ_α являются биекциями $\varphi_\alpha : U \leftrightarrow V$, определенными равенствами

$$\varphi_\alpha(u_i) = v_\alpha^{(i)},\ i = \overline{1,N},\ \alpha = \overline{1,r}.$$

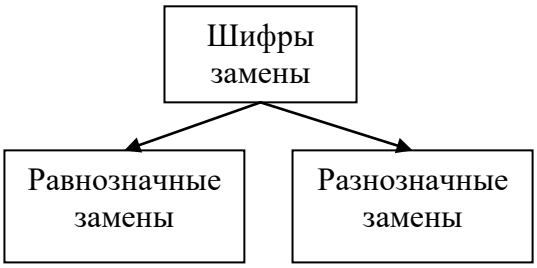
Число таких биекций не превосходит $N!$.

Для шифра однозначной замены определение правила зашифрования можно уточнить: в формуле включение следует заменить равенством

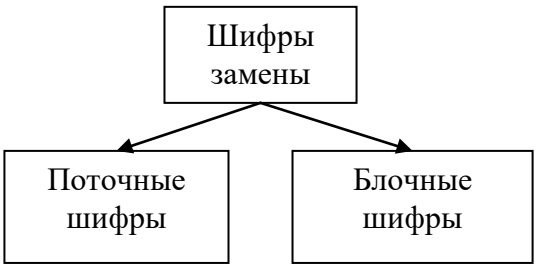
$$y_j = \varphi_{\alpha_j^{(k)}}(x_j), \quad j = \overline{1,l}.$$

Введем еще ряд определений.

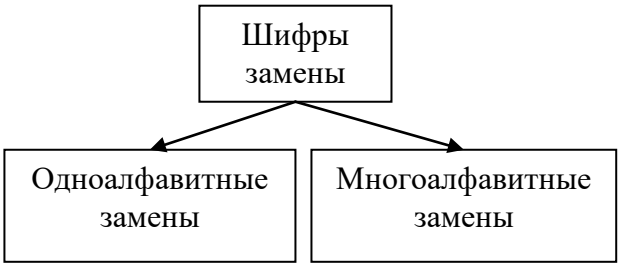
Если для некоторого числа $q \in \mathrm{N}$ выполняются включения $v_i \in B^q$, $i=1,N$, то соответствующий шифр замены будем называть *шифром равнозначной замены.* В противном случае - *шифром разнозначной замены:*



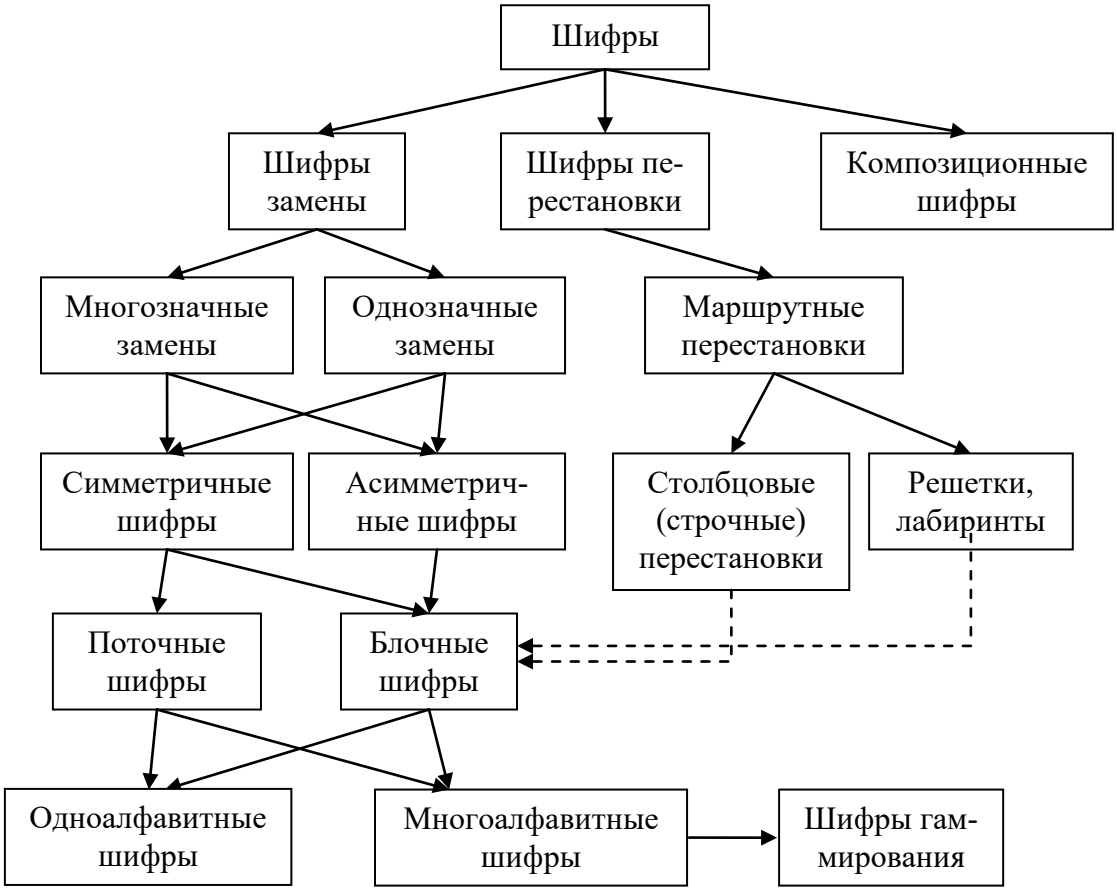
В подавляющем большинстве случаев используются шифры замены, для которых $U \in A^p$, для некоторого $p \in \mathrm{N}$. При p = 1 говорят о *поточных шифрах замены,* при $p > 1$ - о *блочных шифрах замены:*



Следующее определение. В случае r = 1 шифр замены называют *одноалфавитным шифром замены* или *шифром простой замены.* В противном случае – *многоалфавитным шифром замены:*



Ограничиваясь наиболее важными классами шифров замены и исторически известными классами шифров перестановки, сведем результаты классификации в схему, изображенную на рисунке.



Следует подчеркнуть, что стрелки, выходящие из любого прямоугольника схемы, указывают лишь на наиболее значимые частные подклассы шифров. Пунктирные стрелки, ведущие из подклассов шифров перестановки, означают, что эти шифры можно рассматривать и как блочные шифры замены в соответствии с тем, что открытый текст делится при шифровании на блоки фиксированной длины, в каждом из которых производится некоторая перестановка букв. Одноалфавитные и многоалфавитные шифры могут быть как поточными, так и блочными. В то же время шифры гаммирования, образующие подкласс многоалфавитных шифров, относятся к поточным, а не к блочным шифрам. Кроме того, они являются симметричными, а не асимметричными шифрами.

Шифр Виженера

Наиболее известными являются шифры замены, или подстановки, особенностью которых является замена символов (или слов, или других частей

сообщения) открытого текста соответствующими символами, принадлежащими алфавиту шифротекста. Различают *одноалфавитную* и *многоалфавитную* замену. Вскрытие одноалфавитных шифров основано на учете частоты появления отдельных букв или их сочетаний (биграмм, триграмм и т. п.) в данном языке. Классические примеры вскрытия таких шифров содержатся в рассказах Э. По "Золотой жук" и А. Конан Дойля "Пляшущие человечки".

Примером многоалфавитного шифра замены является так называемая система Виженера. Шифрование осуществляется по таблице, представляющей собой квадратную матрицу размерностью n X n, где n - число символов используемого алфавита. На рис.4 показана таблица Виженера для русского языка (алфавит Z_{32}- 32 буквы и пробел). Первая строка содержит все символы алфавита. Каждая следующая строка получается из предыдущей циклическим сдвигом последней на символ влево.

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

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**	**Ъ**	**Ы**	**Ь**	Э
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**	**Ъ**	**Ы**	**Ь**	**Э**	Ю
	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	Ъ	Ы	Ь	Э	Ю	Я

Рисунок 4. Таблица Виженера для алфавита Z_{32}

Выбирается ключ или ключевая фраза. После чего процесс зашифрования осуществляется следующим образом. Под каждой буквой исходного сообщения последовательно записываются буквы ключа; если ключ оказался короче сообщения, его используют несколько раз. Каждая буква шифротекста находится на пересечении столбца таблицы, определяемого буквой открытого текста, и строки, определяемой буквой ключа. Пусть, например, требуется зашифровать сообщение:

ГРУЗИТЕ АПЕЛЬСИНЫ БОЧКАМИ ТЧК БРАТЬЯ КАРАМАЗОВЫ ТЧК

С помощью ключа ВЕНТИЛЬ запишем строку исходного текста с расположенной под ней строкой с циклически повторяемым ключом:

ГРУЗИТЕ АПЕЛЬСИНЫ БОЧКАМИ ТЧК БРАТЬЯ КАРАМАЗОВЫ ТЧК

ВЕНТИЛЬВЕНТИЛЬВЕНТИЛЬВЕНТИЛЬВЕНТИЛЬВЕНТИЛЬВЕН-ТИЛЬВЕ

В результате зашифрования, начальный этап которого показан на рисунке 5, получим шифротекст:

ЕХЩРЭАБЕЫЧУДККТИСЙЩРМЕЩЬЗЭРМДО-БИЭУАДЧТШЛЕВМЪФГК ЛЩП

Расшифрование осуществляется следующим образом. Под буквами шифро-текста последовательно записываются буквы ключа; в строке таблицы, соответствующей очередной букве ключа, происходит поиск соответствующей буквы шифротекста. Находящаяся над ней в первой строке таблицы буква является соответствующей буквой исходного текста.

Для увеличения надежности шифра можно рекомендовать его использование после предварительной псевдослучайной перестановки букв в каж-

дой строке таблицы. Возможны и другие модификации метода.

Рисунок 5. Принцип шифрования по таблице Виженера

4. Задания на криптоанализ классических шифров

4.1 Шифр столбцовой перестановки

При решении заданий на криптоанализ шифров перестановки необходимо восстановить начальный порядок следования букв текста. Для этого используется анализ совместимости символов, в чем может помочь таблица сочетаемости.

Таблица 1. Сочетаемость букв русского языка

Г	С	Слева		Справа	Г	С
3	97	л, д, к, т, в, р, н	А	л, н, с, т, р, в, к, м	12	88
80	20	я, е, у, и, а, о	Б	о, ы, е, а, р, у	81	19
68	32	я, т, а, е, и, о	В	о, а, и, ы, с, н, л, р	60	40
78	22	р, у, а, и, е, о	Г	о, а, р, л, и, в	69	31
72	28	р, я, у, а, и, е, о	Д	е, а, и, о, н, у, р, в	68	32
19	81	м, и, л, д, т, р, н	Е	н, т, р, с, л, в, м, и	12	88
83	17	р, е, и, а, у, о	Ж	е, и, д, а, н	71	29
89	11	о, е, а, и	З	а, н, в, о, м, д	51	49
27	73	р, т, м, и, о, л, н	И	с, н, в, и, е, м, к, з	25	75
55	45	ь, в, е, о, а, и, с	К	о, а, и, р, у, т, л, е	73	27
77	23	г, в, ы, и, е, о, а	Л	и, е, о, а, ь, я, ю, у	75	25
80	20	я, ы, а, и, е, о	М	и, е, о, у, а, н, п, ы	73	27
55	45	д, ь, н, о, а, и, е	Н	о, а, и, е, ы, н, у	80	20
11	89	р, п, к, в, т, н	О	в, с, т, р, и, д, н, м	15	85
65	35	в, с, у, а, и, е, о	П	о, р, е, а, у, и, л	68	32
55	45	и, к, т, а, п, о, е	Р	а, е, о, и, у, я ,ы, н	80	20
69	31	с, т, в, а, е, и, о	С	т, к, о, я, е, ь, с, н	32	68
57	43	ч, у, и, а, е, о, с	Т	о, а, е, и, ь, в, р, с	63	37
15	85	п, т, к, д, н, м, р	У	т, п, с, д, н, ю, ж	16	84
70	30	н, а, е, о, и	Ф	и, е, о, а, е, о, а	81	19
90	10	у, е, о, а, ы, и	Х	о, и, с, н, в, п, р	43	57
69	31	е, ю, н, а, и	Ц	и, е, а, ы	93	7
82	18	е, а, у, и, о	Ч	е, и, т, н	66	34
67	33	ь, у, ы, е, о, а, и, в	Ш	е, и, н, а, о, л	68	32
84	16	е, б, а, я, ю	Щ	е, и, а	97	3
0	100	м, р, т, с, б, в, н	Ы	л, х, е, м, и, в, с, н	56	44
0	100	н, с, т, л	Ь	н, к, в, п, с, е, о, и	24	76
14	86	с, ы, м, л, д, т, р, н	Э	н, т, р, с, к	0	100
58	42	ь, о, а, и, л, у	Ю	д, т, щ, ц, н, п	11	89
43	57	о, н, р, л, а, и, с	Я	в, с, т, п, д, к, м, л	16	84

При анализе сочетаемости букв друг с другом следует иметь в виду зависимость появления букв в открытом тексте от значительного числа предшествующих букв. Для анализа этих закономерностей используют понятие условной вероятности.

Систематически вопрос о зависимости букв алфавита в открытом тексте от предыдущих букв исследовался известным русским математиком А.А. Марковым (1856 - 1922). Он доказал, что появления букв в открытом тексте нельзя считать независимыми друг от друга. В связи с этим А. А. Марковым отмечена еще одна устойчивая закономерность открытых текстов, связанная с чередованием гласных и согласных букв. Им были подсчитаны частоты встречаемости биграмм вида гласная - гласная (*г, г*), гласная - согласная (*г, с*), согласная - гласная (*с, г*), согласная - согласная (*с, с*) в русском тексте длиной в 10^5 знаков. Результаты подсчета отражены в следующей таблице:

Таблица 3. Чередование гласных и согласных

	Г	С	Всего
Г	6588	38310	44898
С	38296	16806	55102

Пример решения:

Дан шифр-текст: СВПООЗЛУЙЬСТЬ_ЕДПСОКОКАЙЗО

Текст содержит 25 символов, что позволяет записать его в квадратную матрицу 5х5. Известно, что шифрование производилось по столбцам, следовательно, расшифрование следует проводить, меняя порядок столбцов.

С	**В**	**П**	**О**	**О**
З	**Л**	**У**	**Й**	**Ь**
С	**Т**	**Ь**	**_**	**Е**
Д	**П**	**С**	**О**	**К**
К	**А**	**Й**	**З**	**О**

Необходимо произвести анализ совместимости символов (Таблица сочетаемости букв русского и английского алфавита, а также таблицы частот

биграмм представлена выше). В первом и третьем столбце сочетание СП является крайне маловероятным для русского языка, следовательно, такая последовательность столбцов быть не может. Рассмотрим другие запрещенные и маловероятные сочетания букв: ВП (2,3 столбцы), ПС (3,1 столбцы), ПВ (3,2 столбцы). Перебрав их все, получаем наиболее вероятные сочетания биграмм по столбцам:

В	**О**	**С**	**П**	**О**
Л	**Ь**	**З**	**У**	**Й**
Т	**Е**	**С**	**Ь**	**_**
П	**О**	**Д**	**С**	**К**
А	**З**	**К**	**О**	**Й**

Получаем осмысленный текст: ВОСПОЛЬЗУЙТЕСЬ_ПОДСКАЗКОЙ

Задание: Расшифровать фразу, зашифрованную столбцовой перестановкой.

1. ОКЕСНВРП_ЫРЕАДЕЫН_В_РСИКО
2. ДСЛИЕЗТЕА_Ь_ЛЬЮВМИ_ _АОЧХК
3. НМВИАИ_НЕВЕ_СМСТУОРДИАНКМ
4. ЕДСЗЬНДЕ_МУБД_УЭ_КРЗЕМНАЫ
5. СОНРЧОУО_ХДТ_ИЕИ_ВЗКАТРРИ
6. _ОНКА_БНЫЕЦВЛЕ_К_ТГОАНЕИР
7. НЗМАЕЕАА_Г_НОТВОССОТЬЯАЛС
8. РППОЕААДТВЛ_ЕБЬЛНЫЕ_ПА_ВР
9. ОПЗДЕП_ИХРДОТ_И_ВРИТЧ_САА
10. ВКЫОСИРЙУ_ОЬВНЕ_СОАПНИОТС
11. ПКТИРАОЛНАОИЧ_З_ЕСЬНЕЛНЖО
12. ИПКСОЕ_ТСМНАЧИ_ОЕН_ГДЕЛА_
13. АМВИННЬТЛЕАНЕ_ЙОВ_ОПХАРТО
14. АРЫКЗЫ_КЙТНЛ_ААЫ_ОЛБКЫТРТ
15. _ПАРИИВИАРЗ_БРА_ИСТЬЛТОЕК
16. П_ЛНАЭУВКАА_ЦИИВР_ОКЧЕДРО
17. ЖВНОАН_АТЗОЬСН_ЫО_ФВИИКИЗ
18. ОТВГОСЕЬЬТАДВ_С_ЬЗАТТЕЫАЧ
19. ЯАМРИТ_ДЖЕХ_СВЕД_ТСУВЕТНО
20. УЬБДТ_ОЕГТВ_ОЫКЭА_ВКАИУЦИ
21. ЛТБЕЧЛЖЫЕ_ _ОАПТЖРДУ_ЛМНОА
22. ИТПРКРФАГО_АВЯИА_ЯНЖУАКАН
23. ПКЕЕРРПО_ЙУСТ_ИТПСУТЛЯЕИН
24. ИЬЖЗНСД_ТДН_ЕТ_НУВЕУРЫГОЫ
25. ЕОУРВА_НЬРИАДИЦЕПИ_РНШВЫЕ

Задание: Расшифровать фразу, зашифрованную двойной перестановкой (сначала были переставлены столбцы, затем строки)

1. СЯСЕ_ _ЛУНЫИАККННОГЯДУЧАТН
2. МСЕЫ_ЛЫВЕНТОСАНТУЕИ_РЛПОБ
3. АМНРИД_УЕБСЫ_ЕЙРСООКОТНВ_
4. ОПЧУЛС_БООНЕВ_ОЖАЕОНЕЩЕИН
5. ЕШИАНИРЛПГЕЧАВРВ_СЕЫНА_ЛО
6. АРАВНРСВЕЕОАВ_ЗАНЯА_КМРЕИ
7. А_ЛТАВЙООЛСО_ТВ_ШЕЕНЕСТ_Ь
8. ФИ_ЗИММУЫНУУБК_Е_ДЬШЫИВЧУ
9. ВР_ЕСДЕИ_ТПХРОИ_ЗБУАДНУА_
10. ЦТААЙПЕЕ_ТБГУРРСВЬЕ_ОРЗВВ
11. АВАРНСЧАА_НЕДВЕДЕРПЕОЙ_ИС
12. ДОПК_СОПАЛЕЧНЛ_ГИНЙОИЖЕ_Т
13. ЛУАЗИЯНСА_ДТДЕАИ_ШРФЕОНГ_
14. С_ОЯНВ_СЬСЛААВРЧЕАРТОГДЕС
15. ЗШАФИПРАЛОЕНЖ_ОЬН_ДАРВОНА
16. КЭЕ_ТДУМБ_ЬСЗЕДНЕЗМАОР_ТУ
17. _ЕАЛЯРАНВЯАЧДА_ЕРПЕСАНВ_Ч
18. _И_ЕНТРЗИ_ОКЕВНОДЛЕША_ИМП
19. РОБДОЕВПС_МСХЬА_ _ИВПСНИОТ
20. ЕСДНОГТЕАНН_НЕОВМР_ЕУНПТЕ
21. _ЙЕСТОВО_НИИНЛАЕТИЖДСОПВ_
22. НДИАЕОЫЛПНЕ_ _НВЕАНГТ_ИЗЛА
23. П_БИРДЛЬНЕВ_ОП_ОПЗДЕВЫГЕА
24. МДООИТЕЬ_СМТ_НАДТЕСУБЕХНО
25. АИНАЛЖНОЛЕШФ_ЗИ_УАРОЬСНЕ_

4.2 Шифр двойной перестановки

Пример решения:

Дан шифр-текст: ЫОЕЧТТОУ_СНСОРЧТРНАИДЬН_Е

Текст содержит 25 символов, что позволяет записать его в квадратную матрицу 5х5. известно, что шифрование производилось сначала по столбцам, а затем по строкам, следовательно, расшифрование следует проводить тем же способом.

Ы	О	Е	Ч	Т
Т	О	У	_	С
Н	С	О	Р	Ч
Т	Р	Н	А	И

Д	Ь	Н	_	Е

Производим анализ совместимости символов. Если в примере столбцовой перестановки можно было легко подобрать нужную комбинацию путем перебора, то здесь лучше воспользоваться таблицей частот букв русского языка (см. приложение). Для оптимизации скорости выполнения задания можно проверить все комбинации букв только в первой строке. Получаем ОЕ-15, ОЧ-12, ЕТ-33, ТЕ-31, ЧО-х, ЕО-7, ЧЫ-х, ОЫ-х, ТЫ-11, ТЧ-1, ЧЕ-23 (где х - запрещенная комбинация).

Из полученных результатов можно предположить следующую комбинацию замены столбцов **2 4 3 5 1:**

О	Ч	Е	Т	Ы
О	_	У	С	Т
С	Р	О	Ч	Н
Р	А	Н	И	Т
Ь	_	Н	Е	Д

Теперь необходимо переставить строки в нужном порядке. **3 2 4 5 1:**

С	Р	О	Ч	Н
О	_	У	С	Т
Р	А	Н	И	Т
Ь	_	Н	Е	Д
О	Ч	Е	Т	Ы

Получаем осмысленный текст: СРОЧНО_УСТРАНИТЬ_НЕДОЧЕТЫ

Задание: Расшифровать фразу, зашифрованную двойной перестановкой (сначала были переставлены столбцы, затем строки)

1. СЯСЕ_ _ЛУНЫИАККННОГЯДУЧАТН
2. МСЕЫ_ЛЫВЕНТОСАНТУЕИ_РЛПОБ
3. АМНРИД_УЕБСЫ_ЕЙРСООКОТНВ_
4. ОПЧУЛС_БООНЕВ_ОЖАЕОНЕЩЕИН
5. ЕШИАНИРЛПГЕЧАВРВ_СЕЫНА_ЛО
6. АРАВНРСВЕЕОАВ_ЗАНЯА_КМРЕИ
7. А_ЛТАВЙООЛСО_ТВ_ШЕЕНЕСТ_Ь
8. ФИ_ЗИММУЫНУУБК_Е_ДЬШЫИВЧУ
9. ВР_ЕСДЕИ_ТПХРОИ_ЗБУАДНУА_
10. ЦТААЙПЕЕ_ТБГУРРСВЬЕ_ОРЗВВ
11. АВАРНСЧАА_НЕДВЕДЕРПЕОЙ_ИС
12. ДОПК_СОПАЛЕЧНЛ_ГИНЙОИЖЕ_Т
13. ЛУАЗИЯНСА_ДТДЕАИ_ШРФЕОНГ_

14. С_ОЯНВ_СЬСЛААВРЧЕАРТОГДЕС
15. ЗШАФИПРАЛОЕНЖ_ОЬН_ДАРВОНА
16. КЭЕ_ТДУМБ_ЬСЗЕДНЕЗМАОР_ТУ
17. _ЕАЛЯРАНВЯАЧДА_ЕРПЕСАНВ_Ч
18. _И_ЕНТРЗИ_ОКЕВНОДЛЕША_ИМП
19. РОБДОЕВПС_МСХЬА_ _ИВПСНИОТ
20. ЕСДНОГТЕАНН_НЕОВМР_ЕУНПТЕ
21. _ЙЕСТОВО_НИИНЛАЕТИЖДСОПВ_
22. НДИАЕОЫЛППНЕ_ _НВЕАНГТ_ИЗЛА
23. П_БИРДЛЬНЕВ_ОП_ОПЗДЕВЫГЕА
24. МДООИТЕЬ_СМТ_НАДТЕСУБЕХНО
25. АИНАЛЖНОЛЕШФ_ЗИ_УАРОЬСНЕ_

4.3 ШИФР ПРОСТОЙ ЗАМЕНЫ

Криптоанализ шифра простой замены основан на использовании статистических закономерностей языка. Так, например, известно, что в русском языке частоты букв распределены следующим образом:

Таблица 4. Частоты букв русского языка (в 32-буквенном алфавите со знаком пробела)

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

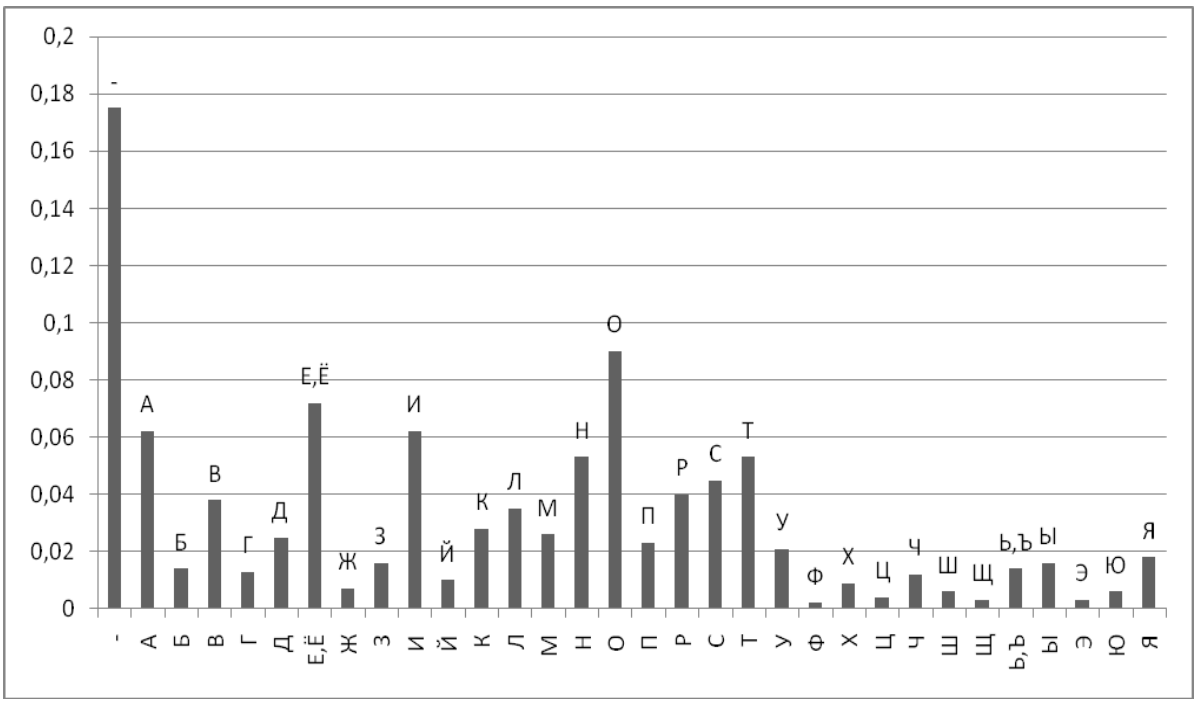


Рисунок 6. Диаграмма частот букв русского языка

Для получения более точных сведений об открытых текстах можно строить и анализировать таблицы k-грамм при k>2, однако для учебных целей вполне достаточно ограничиться биграммами. Неравновероятность k - грамм (и даже слов) тесно связана с характерной особенностью открытого текста – наличием в нем большого числа повторений отдельных фрагментов текста: корней, окончаний, суффиксов, слов и фраз. Так, для русского языка такими привычными фрагментами являются наиболее частые биграммы и триграммы:

СТ, НО, ЕН, ТО, НА, ОВ, НИ, РА, ВО, КО,

СТО, ЕНО, НОВ, ТОВ, ОВО, ОВА

Полезной является информация о сочетаемости букв, то есть о предпочтительных связях букв друг с другом, которую легко извлечь из таблиц частот биграмм.

Имеется в виду таблица, в которой слева и справа от каждой буквы расположены наиболее предпочтительные "соседи" (в порядке убывания частоты соответствующих биграмм). В таких таблицах обычно указывается

также доля гласных и согласных букв (в процентах), предшествующих (или следующих за) данной букве.

Таблица 5. Таблица частот биграмм русского языка

ЧАСТЬ 1

	А	Б	В	Г	Д	Е	Ж	З	И	И	К	Л	М	Н	О	П
А	2	12	35	8	14	7	6	15	7	7	19	27	19	45	3	11
Б	5					9	1		6			6		2	21	
В	35	1	5	3	3	32		2	17		7	10	3	9	58	6
Г	7				3	3			5		1	5		1	50	
Д	25		3	1	1	29	1	1	13		1	5	1	13	22	3
Е	2	9	18	11	27	7	5	10	6	15	13	35	24	63	7	16
Ж	5	1			6	12			5					6		
З	35	1	7	1	5	3			4		2	1	2	9	9	1
И	4	6	22	5	10	21	2	23	19	11	19	21	20	32	8	13
И	1	1	4	1	3		1	2	4		5	1	2	7	9	7
К	24	1	4	1		4	1	1	26		1	4	1	2	66	2
Л	25	1	1	1	1	33	2	1	36		1	2	1	8	30	2
М	18	2	4	1	1	21	1	2	23		3	1	3	7	19	5
Н	54	1	2	3	3	34			58		3		1	24	67	2
О	1	28	84	32	47	15	7	18	12	29	19	41	38	30	9	18
П	7					15			4			9		1	46	

ЧАСТЬ 2

	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь	Э	Ю	Я
А	26	31	27	3	1	10	6	7	10	1			2	6	9
Б	8	1		6						1	11				2
В	6	19	6	7		1	1	2	4	1	18	1	2		3
Г	7			2											
Д	6	8	1	10			1	1	1		5	1			1
Е	39	37	33	3	1	8	3	7	3	3			1	1	2
Ж		1													
З	3	1		2							4				4
И	11	29	29	3	1	17	3	11	1	1			1	3	17
И	3	10	2				1	3	2						
К	10	3	7	10			1								
Л		3	1	6		4		1			2	30		4	9
М	2	5	3	9	1			2			5	1	1		3
Н	1	9	9	7	1		5	2			36	3			5
О	43	50	39	3	2	5	2	12	4	3			2	3	2

П	41	1		6							2				2

ЧАСТЬ 3

	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П
Р	55	1	4	4	3	37	3	1	24		3	1	3	7	56	2
С	8	1	7	1	2	25			6		40	13	3	9	27	11
Т	35	1	27	1	3	31		1	28		5	1	1	11	56	4
У	1	4	4	4	11	2	6	3	2		8	5	5	5	1	5
Ф	2					2			2						1	
Х	4	I	4	1	3	1		2	3		4	3	3	4	18	5
Ц	3					7			10		2				1	
Ч	12					23			13		2			6		
Ш	5					11			14		1	2		2	2	
Щ	3					8			6					1		
Ы		1	9	1	3	12		2	4	7	-3	6	6	3	2	10
Ь		2	4	1	1	2		2	2		6		3	13	2	4
Э											1			1		
Ю		2	1	2	1			3	1		1		1	1	1	3
Я	1	3	9	1	3	3	1	5	3	2	3	3	4	6	3	6

ЧАСТЬ 4

	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь	Э	Ю	Я
Р	1	5	9	16		1	1	1	2		8	3			5
С	4	11	82	6		1	1	2	2		1	8			17
Т	26	18	2	10				1			И	21			4
У	7	14	7			1		8	3	2				9	1
Ф	1	1													
Х	3	4	2	2	1			1							
Ц				1							1				
Ч			7	1					1			1			
Ш				1								1			
Щ				1											
Ы	3	9	4	1		16		1	2						
Ь	1	11	3					1	4				1	3	1
Э		1	9												
Ю	1	1	7				1	1		4					
Я	3	6	10			2	1	4	1	1			1	1	1

Пример криптоанализа шифра замены

Известно, что зашифровано стихотворение Р. Киплинга в переводе С.Я. Маршака. Шифрование заключалось в замене каждой буквы на двузначное число. Отдельные слова разделены несколькими пробелами, знаки препинания сохранены. Таблица частот букв русского языка приведена выше.

29 15 10 17 29 22 25 31 15 33 35 41 43 45 35 57 45 25 17 59 15 10 25 41 25 69, 59 78 29 82 25 78 25 17 15 10 88 90 78 25 62 25 22 10 57 73 79 35 67 78 90 88 29 45 35 29, 54 57 90 31 90 73 22 88 15 88 29 15 17 69 41 25 15, 70 17 90 57 43 59 15 78 15 62 22 25 17 57 25 69 88 15 82 17 25 88 29 45 35…

Подсчитаем частоты шифрообразований:

Обозначение	29	15	10	17	22	25	31	33	35	41	43	45	57
Количество	7	10	4	7	4	12	2	1	5	3	2	4	5

Обозначение	59	69	78	82	88	90	62	73	79	67	54	70
Количество	3	3	4	2	6	5	1	2	1	1	1	1

Из таблица частот букв русского языка видно, что чаще всего встречается буква О, на втором месте Е. В нашем шифр-тексте чаще всего встречается обозначение 25 (12 раз), на втором месте идет обозначение 15 (10 раз), остальные обозначения им существенно уступают. Поэтому можем выдвинуть гипотезу: 25=О, 15=Е. Однако, текст у нас не очень большой, поэтому закономерности русского языка проявляются в нем не обязательно в строгом соответствии с таблицей частот букв русского языка. Поэтому возможен и вариант: 25=Е, 15=О. Но тогда последнее слово в третьей строке имеет окончание ЕО, что возможно, но все же более вероятный вариант ОЕ. Итак, будем работать с текстом, считая, что 25=О, 15=Е.

Теперь нам поможет знак препинания: «29, …». Крайне маловероятно, чтобы запятая стояла после согласной. Итак, 29 – гласная, причем вероятнее всего 29=И или 29=А, т.к. гласные Я, Ю, Э, У встречаются в осмысленных текстах на русском языке намного реже, чем И и А, что не противоречит таблице частот шифр-текста.

В последней строке: 88 15, но 15=Е, следовательно, 88 – согласная, причем наиболее вероятные значения – это Н и Т. Итак, 25=О, 15=Е, 29=А $\begin{pmatrix} А \\ И \end{pmatrix}$, 88=$\begin{pmatrix} Н \\ Т \end{pmatrix}$. Теперь третье слово в третьей строке имеет 4 варианта:

- 29=И, 88=Н: 22 Н Е Н И Е
- 29=И, 88=Т: 22 Т Е Т И Е
- 29=А, 88=Н: 22 Н Е Н А Е
- 29=А, 88=Т: 22 Т Е Т А Е

Из рассмотренных вариантов лишь один является осмысленным, и он позволяет найти значение 22. Имеем: 22=М и третье слово в третье строке М Н Е Н И Е.

Теперь рассмотрим второе слово в первой строке. Е 10 17 И, причем 10 и 17 – согласные, и это не М и не Н. Наиболее вероятное слово Е С Л И, т.е. 10=С, 17=Л. Конечно, если мы, продолжая работать с текстом, вдруг получим «нечитаемое» слово, то придется вернуться к этому этапу и рассмотреть другие варианты. Однако, это маловероятно, поскольку вряд ли в стихотворении были слова наподобие Е Р Т И, Е В Л И и т.п.

Далее, первое слово второй строки: 59 78 И, причем 59 и 78 – согласные, и это не С, не Л, не М и не Н. Так что это слово П Р И, т.е. 59=П, 78=Р. Тогда шестое слово первой строки 45 О Л П Е, что дает значение 45=Т и тогда при 57=В получаем фрагмент «…В Т О Л П Е…». Также второе слово последней строки П Е Р Е 62 дает нам значение 62=Д.

Далее рассмотрим начало второй строки: «П Р И 82 О Р О Л Е С Н 90 Р О Д О М …». Из него следует, что 82=К и 90=А.

Зная, что 82=К, посмотрим на самое последнее слово К Л О Н И Т 35, откуда станет ясно, что 35=Ь.

Перед последней атакой выпишем текст, заменяя известные обозначения буквами.

И Е С Л И М О 31 Е 33 Ь 41 43 Т Ь В Т О Л П Е С О 41 О 69,
П Р И К О Р О Л Е С Н А Р О Д О М С В 73 79 Ь 67 Р А Н И Т Ь
И, 54 В А 31 А 73 М Н Е Н И Е Л 69 41 О Е,
70 Л А В 43 П Е Р Е Д М О Л В О 69 Н Е К Л О Н И Т Ь…

Из последней строки: 69=Ю, тогда слова Л Ю 41 О Е и С О 41 О Ю определяют 41: 41=Б. Теперь из четвертого слова первой строки Б 43 Т Ь получаем, что 43=Ы. А первое слово из последней строки 70 Л А В Ы – это Г Л А В Ы. Слово в первой строке М О 31 Е 33 Ь угадывается из контекста: М О Ж Е Ш Ь, т.е. 31=Ж, 33=Ш. Теперь второе слово в третьей строке запишется как 54 В А Ж А 73, откуда, с учетом контекста: 54=У, 73=Я. После этого окончание второй строки имеет вид «… С В Я 79 Ь 67 Р А Н И Т Ь». Легко определяются буквы 79=З, 67=Х.

Ответ: И ЕСЛИ МОЖЕШЬ БЫТЬ В ТОЛПЕ СОБОЮ, ПРИ КОРОЛЕ С НАРОДОМ СВЯЗЬ ХРАНИТЬ И, УВАЖАЯ МНЕНИЕ ЛЮБОЕ, ГЛАВЫ ПЕРЕД МОЛВОЮ НЕ КЛОНИТЬ…

Задания: Расшифровать текст. Каждой букве алфавита соответствует двузначное число.

1. 58 62 32 39 99 31 29 58 72 62 99 58 13 54 15 56 31 63 39 72 84 15 13 56 77 15 82 56 56 56 58 54 29 77 56 – 39 99 56 31 56 7732 12 15 54 31 48 7663 15 52 13 39 72 39 5416 72 39 32 72 62 58 58 15,37 62 7752 39 13 39 72 39 32 3931 62 54 39 77 84 39 21 31 3916 72 62 99 58 13 15 54 56 13 4616 39 58 13 95 16 15 13 62 12 46 31 39 6272 15 77 54 56 13 56 6284 31 39 32 56 7658 63 62 7233 62 12 39 54 62 33 62 58 52 39 9199 62 29 13 62 12 46 31 39 58 13 56.56 31 63 39 72 84 15 82 56 39 31 31 48 6213 62 76 31 39 12 39 32 56 5616 72 39 33 31 3954 39 53 12 565437 56 77 31 62 58,39 37 72 15 77 39 54 15 31 56 62,16 72 39 56 77 54 39 99 58 13 54 39,39 13 52 72 48 5433 62 12 39 54 62 52 9531 62 37 48 54 15 12 48 6254 39 77 84 39 21 31 39 58 13 5616 3958 52 39 72 39 58 13 5616 39 12 95 33 62 31 56 295639 37 72 15 37 39 13 52 6256 31 63 39 72 84 15 82 56 56,1513 15 52 21 6216 3915 54 13 39 84 15 13 56 77 15 82 56 5616 72 39 56 77 54 39 99 58 13 54 62 31 31 48 76,95 16 72 15 54 12 62 31 33 62 58 52 56 765656 31 48 76 16 72 39 82 62 58 58 39 54.

2. 3925 20 34 82 6366 46 35 20 25 828639 51 74 35 51 66 20 4437 25 27 51 35 44 20 90 37 51 25 25 51 6391 20 11 37 46 4825 20 37 61 51 14 82 8266 82 35 29 82 91 25 5174 51 24 78 51 24 59 46 86 51 44 74 20 25 37 37,37 44 82 31 11 37 82 51 46 25 51 34 82 25 37 828637 25 27 51 35 44 20 90 37 51 25 25 48 4446 82 78 25 51 14 51 18 37 59 44,51 74 82 35 20 90 37 59 446690 82 25 25 48 44 3761 10 44 20 18 20 44 37,8661 20 25 86 51 39 66 86 51 44 1066 82 86 46 51 35 10 3766 51 46 51 39 51 6366 39 59 91 37.56 46 51 86 20 66 20 82 46 66 5924 35 10 18 37 7851 35 18 20 25 37 91 20 90 37 63,4651,66 51 18 14 20 66 25 5135 82 91 10 14 29 46 20 46 20 4435 20 91 14 37 56 25 48 7837

66 66 14 82 24 51 39 20 25 37 63, 35 10 86 51 39 51 24 37 46 82 14 3744 25 51 18 37 7837 9125 37 7891 25 20 31 4651 61 51 66 25 51 39 25 48 7839 37 24 20 78 10 18 35 51 91,25 5125 82 10 24 82 14 59 31 4624 51 14 42 25 51 18 5139 25 37 44 20 25 37 5924 20 25 25 48 4439 51 74 35 5166 20 44,66 56 37 46 20 59,56 46 5151 61 82 66 74 82 56 82 25 37 8237 25 27 51 35 44 20 90 37 51 25 25 51 6361 82 91 51 74 20 66 25 51 66 46 3725 8237 44 82 82 4666 44 48 66 14 20,82 66 14 3751 46 66 10 46 66 46 39 10 82 4639 37 24 37 44 20 5910 18 35 51 91 20.

3. 74 29 23 27 17 99 71 254932 29 34 27 63 32 25 17 99 60 62 25 34 95 29 53 59 82 27 71 29 77 99 34 27 91 17 99 71 49 99 27 15 60 32 25 50 27 17 62 27 95 27 50 25 91 32 59 77 95 29 50 25 99 59,25 99 74 29 53 25 59 17 99 25 91 23 49 71 25 17 99 604925 34 32 25 71 95 27 82 27 32 32 2529 50 17 25 15 77 99 32 59 7762 95 25 53 95 29 23 32 25 17 99 60 34 15 35 17 27 99 27 71 25 12 2599 95 29 45 49 74 29. 62 95 27 63 34 2771 17 27 12 25,50 27 17 62 27 95 27 50 25 91 32 29 3595 29 50 25 99 29 17 29 82 49 8362 2517 27 50 2762 95 25 34 59 74 99 25 7150 27 53 25 62 29 17 32 25 17 99 4917 71 35 53 29 32 2917 32 29 15 49 23 49 27 8232 29 34 27 63 32 2595 29 50 25 99 29 77 10 27 12 2525 50 25 95 59 34 25 71 29 32 49 3549 95 27 53 27 95 71 49 95 25 71 29 32 49 27 8274 95 49 99 49 23 32 89 837425 99 74 29 53 5950 15 25 74 25 7162 49 99 29 32 49 354953 29 62 25 82 49 32 29 77 10 49 8359 17 99 95 25 91 17 99 71.34 15 3562 25 17 15 27 34 32 49 8325 62 99 49 82 29 15 60 32 2562 95 49 82 27 32 27 32 49 2734 49 17 74 25 71 89 8382 29 17 17 49 71 25 7112 25 95 35 23 27 9153 29 82 27 32 89.74 29 23 27 17 99 71 25 49 32 29 34 27 63 32 25 17 99 60 95 29 50 25 99 8934 25 17 99 49 12 29 27 99 17 3525 62 99 49 82 49 53 29 67 49 27 9162 95 25 12 95 29 82 82 32 25 12 2525 50 27 17 62 27 23 27 32 49 35.

4. 48 2318 40 94 35 62 53 94 25 53 15 3591 35 40 35, 52 23 5253 40 3594 35 40 2394 23 91 52 94 49 24 23 84 8994 23 64 55 53 15 18 53 91, 24 53 88 23 62 12 25 7694 2364 35 24 49, 35 9449 88 5348 94 23 24,41 91 3591 23 5231 49 15 53 91. 47 91 3541 49 62 84 91 62 3535 91 41 23 84 91 2531 29 24 3564 35 27 35 88 5394 2391 35,52 35 91 35 55 35 5335 9425 84 64 29 91 23 24,52 35 40 15 2348 23 62 53 55 94 49 2448 2349 40 35 242541 49 91 8994 5394 23 24 53 91 53 24 94 2315 53 62 49 12 52 49,12 53 15 12 49 6053 18 4994 23 62 84 91 55 53 41 49.53 40 3594 35 40 23,62 29 48 62 23 6284 62 35 25 1815 62 25 88 53 94 25 53 18 52 35 24 53 31 23 94 25 53 62 35 48 15 49 27 23,64 35 24 49 41 25 24 23 35 91 55 23 88 53 94 94 29 7684 25 40 94 23 243564 55 53 64 38 91 84 91 62 25 2594 2364 49 91 25 2564 35 41 91 256291 4988 5384 53 52 49 94 15 4949 15 23 55 25 24 23 84 8935 31 3541 91 35 – 91 35.52 23 52 35 76-91 3564 55 53 15 18 53 918440 24 49 27 25 1884 91 49 52 35 1835 91 24 53 91 53 246291 53 18 94 35 91 49.

5. 79 6131 96 28 35 85 5226 30 24 21 52 85 59 49 79 30 88 7949 30 52 79 59 85 26 30 24 21 59 85 42 79 88 61 28 35 86 5096 28 52 30 50,24 30 96 74 21 59 9059 30 96 30 24 85 61 8626 96 85 88 79 96 79 24 61 79 1128 52 79 78 31 85, - 21 50 30 96 85 31 21 61 59 31 85 1126 79 24 96 79 59 35 79 31 5996 30 31 52 21 50 61 79 1131 21 96 35 85 61 31 85,2126 79 78 30 50 2867 868561 30 35:35 79 24 2467 79 28 24 30 61,35 96 85 61 21 24 69 21 35 9052 30 35,61 79 96 50 21 52 90 61 86 1196 79 59 35,42 24 79 96 79 49 86 1149 30 59,49 79 52 79 59 8669 49 30 35 2159 26 30 52 79 1126 46 30 61 85 69 86,88 79 52 28 67 86 3088 52 21 42 21,96 79 49 61 86 3067 30 52 86 3042 28 67 86,42 21 88 79 96 30 52 79 3052 85 69 79,61 3085 59 26 79 96 78 30 61 61 79 3024 21 74 3061 21 50 30 31 79 5061 2149 79 42 96 21 59 35 61 86 30 26 96 86 29 85 31 85..

6. 56 27 54 54 27 56 51 32 82 16 63 49 27 63 11 30 73 35 23 54 89 70 27 63 27 493270 35 16 97 82 16 67 73 27 51 30 56 32 6370 29 63 27 49 32 73 29 5473 2748 29 13 29 82 56 82 27 9554 27 35 27 18 51 29,97 56 2770 29 63 305151 35 15 63 89 48 16.16 63 15 11 51 3082 2949 65 27 54 32 63 304929 61 2763 32 48 30-27 56 51 35 15 56 30 233227 11 70 27 35 27 18 32 56 29 63 89 82 30 23,27 82 3051 30 5111 1573 35 29 54 70 27 49 65 32 38 30 63 3073 35 32 23 56 82 16 6770 49 56 35 29 97 16.82 27 49 51 27 1351 29 54 3027 8227 73 16 49 56 32 6370

29 63 27 49 32 73 29 54 82 15 9516 73 27 353270 15 56 30 38 32 6332 92-73 27 5411 30 61 30 18 82 32 51 3049 63 27 18 29 82 82 16 67 61 30 92 29 56 16.27 8249 16 82 16 6361 30 92 29 56 1673 27 5413 15 24 51 163270 92 27 24 29 6373 2749 56 16 73 29 82 89 51 30 13.

7. 3428 68 91 1383 10 65 27 6849 10 26 65 27 68 75 26 39 785375 83 53 18 26 36 62 91.26 10 74 53 1349 10 83 10 65 5353 36 68 72 28 1028 13 18 86 10 27 53 75 3983 6857 26 18 10 91535736 53 6528 68 91 10,83 68 75 27 1334 13 24 13 18 53 36 74 5336 10 74 10 36 57 36 13,83 68 74 1091 10 91 1036 1368 26 74 18 62 34 10 27 1036 10 75 26 13 86 3968 74 36 10.83 18 10 34 28 10,26 57 2650 62 27 6883 68 65 57 86 13.26 57 2649 10 83 10 65 5334 19 13 27 53 75 395334 75 1375 68 50 68 1583 18 68 83 53 26 10 27 53.49 10 83 10 65 5310 27 74 68 72 68 27 44,83 68 28 72 68 18 13 34 80 13 72 6891 10 75 27 10,83 68 26 10,75 26 10 18 68 1568 28 13 86 28 625313 96 1327 13 74 10 18 75 26 34-91 13 36 26 68 27 1053,74 10 86 13 26 75 44,34 10 27 13 18 39 44 36 74 53.3483 18 53 65 68 86 13 15 26 13 91 36 68 26 53 96 10,5318 44 28 68 9123 26 68 2628 78 75 75 10 36 28 13 18-34 26 44 36 57 2772 68 27 68 34 573434 68 18 68 26,23 26 10 74 53 1572 18 53 47 – 75 26 13 18 34 44 26 36 53 74,86 28 57 96 53 15,74 68 72 28 1018 10 36 13 36 68 1386 53 34 68 26 36 68 1353 75 83 57 75 26 53 2628 57 65.

8. 45 34 26 34 9777 34 47 49 67 14 22 49 6747 34 49 39 77 6953 89 26 1097 10 49 10 77 45 53 31 10 14 10 47 22.17 90 56 14 34 77 67 49,49 67 75 49 1053 14 5349 26 90 47 10,77 3439 47 56 34 3156 26 67 52 34 13 10 84 22 5377 34 47 49 67 14 22 49 67 28 34 84 26 67 31,67 49 10 97 90 31 10 14 53 47 223128 70 89 49 53 9314 10 56 10 9356 47 10,5345 34 84 90 26 34 93 69 58 37 28 67 31 10 7047 84 10 14 22 77 10 7053 89 14 10,31 90 47 39 77 39 31 75 53 47 22,47 14 67 31 77 6713 10 14 67,53 9734 89 6728 67 26 69 90,31 56 26 90 47 49 53 31 10 14 1013 34 26 84 31 3453 97 26 70 69 77 39 5869 67 97 39 28 67 26 24 53 70,53 14 5356 26 67 49 10 53 77 10.97 10 84 34 2839 52 53 84 67 89 6797 31 34 26 22 49 1052 26 67 47 10 14 533156 34 45 2269 14 7047 13 53 89 10 77 53 7028 39 47 67 26 10,5353 89 26 1077 10 45 53 77 10 14 10 47 2247 77 67 31 10.

9. 81 49 86 49 1273 92 5081 50 15 5062 47 4915 56 50 51 7673 33 94 7615 94 65 81 47 76.94 76 47 49 81 47 76,15 7662 47 76 2628 16 5162 76 2628 76 51 70 58 76 2673 86 65 84 76 94,47 7615 94 65 81 47 7615 56 50 51 76.24 16 51 7062 76 49 2694 76 86 76 28 94 3362 49 47 1765 84 4915 76 92 15 49 6247 4924 86 49 51 70 96 50 51 50.56 76 31 73 5047 49 62 47 76 31 7624 76 73 65 62 50 513386 49 58 33 5115 56 50 567 065 62 47 16 62.47 65,47 50 73 7684 4943 76 56 7081 56 76-56 7673 49 51 50 56 70…1724 76 58 49 519294 76 51 51 49 73 84.76 94 50 12 50 92 58 33 15 709294 50 28 33 47 49 56 496586 49 94 56 76 86 50,1773 49 86 84 50 51 15 1765 92 49 86 49 47 47 76.86 49 94 56 76 86 76 6228 16 51 5062 76 51 76 73 50 1784 49 47 96 33 47 5028 50 51 70 12 50 94 76 92 15 94 76 31 7692 76 12 86 50 15 56 50.94 76 31 73 501792 76 58 49 51,76 47 5081 56 76-56 7615 76 15 86 49 73 76 56 76 81 49 47 47 7624 33 15 50 51 50,62 76 84 49 5647 76 92 16 2665 94 50 12.

10. 2043 40 13 15 91 31 5475 31 91 12.88 56,88 40 29 1571 3113 15 91 1249 91 15 – 91 1529 31 54 40 91 12…1715 61 69 31 44,2075 15 36 31 546275 25 15 29 84 65 31 25 56.90 4415 62 40 43 40 54 65 2088 31 17 58 65 15 62 90 2690,75 15-17 90 29 90 44 15 44 56,88 31 29 40 54 31 62 90 2649 31 54 15 17 31 621791 31 44 88 58 1315 49 62 40 13901725 15 43 15 17 15 4436 40 25 34 90 62 3188 4036 31 31.15 8862 56 25 90 5449 91 15-91 1515 49 31 88 1275 25 15 91 90 17 88 1575 40 13 88 56 69 31 31.29 40 71 3117 15 88 20 84 69 31 31.56 17 90 29 31 1744 31 88 20,75 25 15 29 84 65 31 2588 31 65 62 15 54 12 62 1544 90 88 56 9175 15 44 56 49 40 54 65 20,17 65 91 40 17 54 20 2015 91 17 90 65 36 56 8449 31 54 84 65 91 1288 4044 31 65 91 15,88 1517 65 3171 3117 43 20 5465 31 61 201725 56 62 90,43 40 91 56 36 90 5465 90 52 40 25 31 91 569043 40 52 15 17 15 25 90 54.

11. 65 27,67 40 58 34 11 4727 4227 45 82 34 11 14 4914 89 95 47.65 14 90 36 89 3434 67 36 90 36 45 67 11 36 65 65 34 89 34,11 17 82 34 67 1924 3495 40 45 17 34 45 82 36 24 65 14 7025 36 82 34 90 36 73.70 34 67 4945 67 95 40 65 40,17 34 45 95 36 24 1458 34 67 34 95 34 7334 65 1445 36 73 90 40 4517 95 36 59 47 11 40 82 14,24 40 11 65 341465 40 24 36 42 65 3417 34 24 25 49 67 4040 25 36 95 14 58 34 45 40 25 14,69 67 3411 45 3642 3645 27 11 36 95 36 65 65 40 4924 36 95 42 40 11 40,90 82 36 6534 34 65,4558 34 36 7345 34 11 36 67 45 58 14 7345 34 31 6317 34 24 24 36 95 42 14 11 40 36 6765 34 95 25 40 82 19 65 47 3624 14 17 82 34 25 40 67 14 90 36 45 58 14 3634 67 65 34 32 36 65 14 49,17 34 65 36 25 65 34 89 2765 40 82 40 42 14 11 40 36 6767 34 95 89 34 11 82 31,17 95 14 45 47 82 40 36 6765 4089 40 45 67 95 34 82 1459 40 82 36 67 65 47 3667 95 27 17 17 471434 59 25 36 65 14 11 40 36 67 45 4917 95 34 18 45 34 31 63 65 47 25 1424 36 82 36 89 40 56 14 49 25 14.4017 34 67 34 25 2763 24 36 45 1965 14 58 40 5865 3617 34 82 40 89 40 36 67 45 4965 36 82 36 89 40 82 19 65 3417 95 36 59 47 11 40 67 1945 34 11 36 67 45 58 14 2559 34 36 11 47 2517 82 34 11 56 40 25,“25 34 95 45 58 14 2524 19 49 11 34 82 40 25”.36 42 36 82 1490 67 34-45 58 40 65 24 40 8295 40 63 89 34 95 14 67 45 4917 3417 34 82 65 34 73…

12. 14 701465 3659 47 82 34,4058 40 5842 36.17 95 34 45 67 34-65 40 17 95 34 45 67 3432 36 45 67 36 95 3425 27 42 14 58 34 11,65 4011 14 24-45 67 40 65 24 40 95 67 65 47 3636 11 95 34 17 36 34 14 24 47,4563 40 17 40 24 65 34 89 36 95 25 40 65 45 58 14 25 1440 11 67 34 25 40 67 40 25 14,14 67 40 82 19 49 65 45 58 14 25 1440 58 11 40 82 40 65 89 40 25 14,32 11 36 24 45 58 14 25 1459 40 63 27 58 40 25 14,59 36 82 19 89 14 73 45 58 14 25 1425 14 65 40 25 14,18 95 40 65 56 27 63 45 58 14 25 1445 14 89 40 95 36 67 40 25 141432 11 36 73 56 40 95 45 58 14 25 1490 40 45 40 25 14.17 95 36 24 25 36 67 4745 65 40 95 49 42 36 65 14 49,11 63 49 67 47 3617 3434 67 24 36 82 19 65 34 45 67 14,25 34 42 65 3459 36 6334 45 34 59 47 7070 82 34 17 34 6717 95 14 34 59 95 36 45 67 141195 40 63 65 47 7058 34 65 56 40 7036 11 95 34 17 4758 40 5882 36 89 40 82 19 65 34,67 40 581465 4090 36 95 65 34 2595 47 65 58 36-58 40 58,45 34 59 45 67 11 36 65 65 34,1417 95 34 14 63 34 32 82 3467 95 27 24 40 25 1465 36 11 36 24 34 25 47 7025 40 63 27 95 27“14 65 67 36 65 24 40 65 67 34 11”.

13. 60 46 5746 52,28 15 57 3912 32 60 32 3246 5752 55 30 12 61 11 55 57 32 12 41,37 46 60 37 32 9152 32 11 55 12 32 75 4646 5730 32 20 15 75 46 25 99 20 52 32 52 52 4667 55 25 55 12 12 32 12 39 52 19 63“52 99 57 32 36”75 46 12 61 28 75 99(18 32 37 57 3952 99 57 32 3667 46 60 32 25 63 159991 32 57 25 46 60 46 3660 19 37 46 57 19“37 67 99 25 55 12 3930 25 15 52 46 ”67 4620 32 91 12 32).57 5537 55 91 55 4167 57 99 28 75 55.75 25 55 37 55 60 32 74,37 57 46 99 5767 25 99 20 52 55 57 39,99 20 41 45 52 19 36,11 12 99 52 52 46 75 25 19 12 19 36,37 15 67 32 25 55 29 25 46 11 99 52 55 91 99 28 32 37 75 99 36,60 19 37 46 57 52 19 36.“11 48 99 – 29 25 – 11 60 32 52 55 11 74 55 57 39”,52 46 60 32 36 18 99 3637 55 91 46 12 32 5729 12 32 75 57 25 46 52 52 46 3625 55 20 60 32 11 75 99,46 37 52 55 45 32 52 52 19 3655 67 67 55 25 55 57 15 25 46 36,78 46 25 11 4699 91 32 52 15 32 91 46 36“57 32 63 52 99 75 46 3611 60 55 11 74 55 57 3967 32 25 60 46 78 4660 32 75 55”(63 46 57 4111 4675 46 52 74 5511 60 55 11 74 55 57 46 78 4637 57 46 12 32 57 99 41,37 46 78 12 55 37 52 4663 25 46 52 46 12 46 78 99 99,46 37 57 55 12 46 37 3932 45 3267 41 57 52 55 11 74 55 57 393712 99 18 52 99 9112 32 57)…

14. 15 48 3252 326067 32 25 60 19 3625 55 2091 55 20 15 25 1567 25 99 63 46 11 99 12 466078 46 12 46 60 15,28 57 4628 99 52,46 57 60 32 28 55 60 18 99 3620 5530 32 20 46 67 55 37 52 46 37 57 3930 55 20 19,30 19 12 75 12 55 37 37 99 28 32 37 75 99 9137 15 63 46 67 15 57 28 99 75 46 91. 60 37 60 46 3260 25 32 91 4146 52 67 46 25 55 30 46 57 55 12 52 55 37 46 60 32 37 57 39,46 30 46 25 15 11 46 60 55 60 37 15 63 46 67 15 57 52 19 3267 46 11 37 57 15 67 197530 55 20 3232 91 75 46 37 57 52 19 91 9911 55 57 28 99 75 55 91 99,37 99 78 52 55 12 39 52 19 91 9925 55 75 32 57 55 91 99,67 25 9991 55 12 32 36 18 32 9167 25 99 75 46 37 52 46 60 32 52 99 997557 46 52 61 37 32 52 39 75 46 3652 99 57 9960 20 12 32 57 55 60 18 99 91 996052 32 30 32 37 5537 4637 60 99 37 57 46 91,25 55 37 37 19 67 55 4160 46 25 46 63 5525 55 20 52 46 74 60 32 57 52 19 6346 37 12 32 67 99 57 32 12 39 52 19 6399 37 75 25-9911 55 48 3267 46 12 46 37 55 91 9967 25 46 57 99 60 46 67 32 63 46 57 52 19

6391 99 52.28 57 46 75 55 37 55 32 57 37 4167 46 11 37 57 15 67 46 6060 46 11 52 19 63,28 99 5230 19 1252 3257 55 7525 32 57 99 60. 46 11 52 9957 46 12 39 75 4637 57 46 12 30 193775 46 12 61 28 75 46 369967 25 32 37 12 46 60 15 57 19 32“37 67 99 25 55 12 39 75 99”-75 46 57 46 25 19 3252 32 20 60 55 52 19 3278 46 37 57 99,6046 57 12 99 28 99 3246 5720 11 32 18 52 99 6367 55 25 57 99 20 55 52,15 91 32 12 9967 25 32 46 11 46 12 32 60 55 57 3930 19 37 57 25 469930 32 2091 55 12 32 36 18 32 78 4660 25 32 11 5511 12 4137 46 30 37 57 60 32 52 52 46 78 4646 25 78 55 52 99 20 91 55.9960 37 32.

15. 45 74 5431 10 26 38 23 74,86 74 5425 89 26 38 16 74 7475 1645 56 90 25 86 90 75 90 10 2616 74 23 56 86 75 45 16 75 7495 10 13 31 95 10 51 74 16 89 74,36 75 95 75 5936 74 95 74 91 75 31 89 90 23 74 749036 95 89 26 89 90 8313 26 75 25 86 89-75 86 86 75 47 75,45 86 7575 16 8945 74 86 90 74 95 7525 56 86 75 33,75 29 95 10 86 89 90 23 89 25 389013 95 74 16 89 748925 26 56 91,86 75 95 45 10 26 899045 10 19 75 29 74,33 10 3331 89 33 89 7475 29 74 13 38 42 16 8389 1329 95 10 13 89 26 89 89,75 86 86 75 47 75,45 86 7536 75 31 90 74 95 16 56 26 25 4286 56 36 75 4633 10 46 54 10 16,2575 31 89 16 10 33 75 90 83 5456 25 74 95 31 89 74 5416 10 36 10 31 10 90 23 89 468916 1026 74 25 16 56 5925 90 89 16 38 59,8916 1075 86 26 89 45 16 75 47 7536 10 95 16 422531 95 56 47 75 47 7533 75 16 86 89 16 74 16 86 10.109021 86 7590 95 74 54 4286 74,16 1029 10 13 74,51 89 26 899025 90 75 7456 31 75 90 75 26 38 25 86 90 89 74,25 36 10 26 8916 1045 89 25 86 74 16 38 33 89 9136 95 75 25 86 83 16 33 10 919033 75 16 31 89 17 89 75 16 89 95 75 90 10 16 16 75 4636 95 75 91 26 10 31 74,36 95 89 16 89 54 10 26 8931 56 23,51 95 10 26 8916 1013 10 90 86 95 10 3367 95 56 33 86 83,31 51 74 548929 89 67 23 86 74 33 25 839086 95 8936 10 26 38 17 1086 75 26 19 89 16 75 46-8975 33 16 1086 10 3356 59 86 16 7525 90 74 86 89 26 89 25 38,8954 56 13 83 33 1089 47 95 10 26 10,8967 56 86 29 75 26 36 75 86 74 26 74 90 89 13 75 95 56…

16 89 45 74 47 75 9021 86 75 4 613 26 75 25 86 8916 7429 83 26 7536 26 75 91 75 47 75,16 10 75 29 75 95 75 86-86 10 33 75 4616 10 25 86 95 75 4633 10 3395 10 138936 95 89 31 10 74 8629 75 74 90 75 47 7533 56 95 10 51 10…

1036 75 86 75 5436 95 89 23 74 2633 75 16 74 178936 75 25 86 75 95 75 16 16 89 5454 83 25 26 42 548929 74 13 31 74 26 38 59.54 75 95 25 33 75 46 13 54 74 4616 10 33 75 16 74 17-86 7536 75 31 10 2613 16 10 33,33 75 86 75 95 75 47 7575 16 8951 31 10 26 8945 74 86 90 74 95 7525 56 86 75 33,8921 86 7529 83 26 7525 26 75 90 16 7554 74 31 16 83 4695 74 9029 75 74 90 75 4686 95 56 29 83,21 86 7575 13 16 10 45 10 26 75,45 86 7516 10 45 10 26 10 25 3895 10 29 75 86 83,8916 89 45 74 47 7556 51 7416 7489 13 54 74 16 89 86 38,16 7475 25 86 10 16 75 90 89 86 38,16 7436 74 95 74 89 47 95 10 86 38…

16. 15 22 67 30 93 4922 94 65 94 44 49,4939 51 22 75 49 411115 22 4911 53 51 75 51 78 94,44 4927 51 22 67 44 86 51,26 49 39 51 75“78 45 94 – 62 75 – 78 11 51 44 49 78 91 49 22 72 14”,9411 67 26 93 5 144 51 90 6793 51 44 94 11 6753 75 67 41 49 45 94 11 49 93 15 3035 49 15 67 11 67 14,44 5145 78 49 11 65 94 1444 94 86 49 86 94 4115 20 75 53 75 94 26 67 11,44 5153 67 78 67 26 75 51 11 49 11 65 94 14,35 22 6751 90 6715 39 51 75 22 5853 75 51 27 72 11 49 51 2215 67 11 15 51 3944 51 53 67 78 49 93 51 86 881167 27 75 49 26 5127 51 15 53 93 67 22 44 67 90 6735 51 75 44 67 90 6753 75 94 26 75 49 86 49,44 5126 44 49 20 18 51 90 6745 49 93 67 15 22 94.

67 35 51 75 51 78 44 67 1445 51 15 2286 67 39 49 44 78 94 75 49-9439 49 26 88 751511 94 86 94 44 90 67 399415 22 75 49 65 94 93 67 1453 51 75 51 27 51 45 86 49 39 9478 11 94 44 88 93 94 15 5811 53 51 75 51 78.26 78 51 15 5841 11 49 22 49 93 6753 75 67 45 51 86 22 67 75 67 11,36 67 44 49 75 51 149486 75 67 44 65 22 51 14 44 67 111590 94 75 93 30 44 78 49 39 9493 49 39 53,44 6744 51 75 51 49 93 58 44 67 1426 49 78 49 35 51 1427 72 93 6727 7267 15 11 51 22 94 22 5811 15 2027 49 26 88.67 15 22 49 11 49 93 67 15 5844 51 39 49 93 6753 67 93 67 159453 30 22 51 4422 51 39 44 67 22 72,86 67 22 67 75 88 20 44 51 26 11 49 44 72 5190 67 15 22 9494 15 53 67 93 58 26 67 11 49 93 9439 49 15 22 51 75 15 86 94.11 15 5127 93 94 45 518615 49 39 67 93 51 22 88,27 93 94 45 51,27 93 94 45 51,67 4411 72 75 49 15 22 49 51 2244 4990 93 49 26 49 41,44 49 11 94 15 49 51 2244 49 7890 67 93 67 11 67 14,88 45

5153 75 51 86 75 49 15 44 6715 93 72 65 44 67,86 49 8635 49 15 67 11 67 1467 2215 86 88 86 9444 88 78 94 2253 67 7844 67 1544 51 26 44 49 86 67 39 88 2039 51 93 67 78 94 20,53 67 15 93 51 78 44 20 201115 11 67 51 1445 94 26 44 94…

22 94 41 67 44 58 86 6718 51 93 86 44 88 9327 51 15 65 88 39 44 72 1453 94 15 22 67 93 51 22-9439 51 93 67 78 94 3067 27 67 75 11 49 93 49 15 58,35 49 15 67 11 67 1453 67 78 93 67 39 94 93 15 301186 67 93 51 44 86 49 41,44 6788 53 49 15 22 5844 5188 15 53 51 93,9415 11 67 2049 11 22 67 39 49 22 94 35 51 15 86 88 2011 94 44 22 67 11 86 8844 5111 72 75 67 44 94 93.78 11 5122 51 44 94,27 51 15 65 88 39 44 6711 72 44 72 75 44 88 1194 26 -53 67 7836 20 26 51 93 30 45 49,53 67 78 41 11 49 22 94 93 9451 90 679488 11 67 93 67 86 93 94 44 4978 75 88 90 88 2015 22 67 75 67 44 88,1122 51 39 44 67 22 88.

17. 56 67 9218 58 39 99 27 87 67 5625 56 80 67 10 17 92 39 6225 5627 24 95 56 3195 46 27 73 56 3117 58 39 58 67 95 589256 95 40 24 40 17 92 39 626939 40 17 56 67 58-56 18 99 92 46 67 56 87,69 5669 39 3680 17 92 67 2739 40 87 56 17 58 73 40.25 56 39 73 56 10 17 92,56 43 92 80 40 10,95 56 23 80 4023 17 40 24 4025 46 92 69 14 95 67 27 739573 58 87 67 56 73 58.69 39 5869 56 95 46 27 2325 46 92 67 10 17 5638 58 73 95 92 5856 38 58 46 73 40 67 92 10.25 46 92 18 56 46 56 699225 27 17 62 73 56 6924 80 58 39 6218 14 17 5625 46 58 69 58 17 92 95 56 5887 67 56 43 58 39 73 69 56,23 17 40 24 4046 40 24 18 58 23 40 17 92 39 62.56 80 67 40 95 5618 17 40 23 56 80 40 46 1073 58 8743 58 80 69 27 8767 58 80 58 17 10 8773 46 58 67 92 46 56 69 56 9567 4087 40 95 58 73 58 9273 14 39 10 38 58 95 46 40 73 67 56 25 56 69 73 56 46 58 67 67 14 8767 40 39 73 40 69 17 58 67 92 10 8792 67 39 73 46 27 95 73 56 46 4056 67 9239 56 69 58 46 99 58 67 67 5673 56 38 67 5624 67 40 17 92,24 4038 58 8725 46 92 99 17 92.25 56 67 10 73 92 1067 5892 87 58 17 92,80 17 1038 58 23 5695 56 67 95 46 58 73 67 5625 46 58 80 67 40 24 67 40 38 58 67 1469 39 5871 73 9299 73 27 95 92-67 5656 7367 92 8271 73 56 23 56 9267 5873 46 58 18 56 69 40 17 56 39 62.

67 5825 46 56 99 17 569287 92 67 27 73 14,95 40 9556 6727 69 92 80 58 1751 58 17 6292 8267 58 17 58 23 95 56 23 569271 95 24 56 73 92 38 58 39 95 56 23 5625 27 73 58 99 58 39 73 69 92 10-73 46 9225 27 17 62 73 4025 5625 46 40 69 56 87 2718 56 46 73 27,27 39 14 25 40 67 67 14 5838 58 46 73 56 69 56 3127 31 87 56 3173 27 87 18 17 58 46 56 69,17 40 87 25 56 38 58 95,25 58 46 58 95 17 36 38 40 73 58 17 58 319295 67 56 25 56 95.73 46 9269 14 25 27 95 17 14 8271 95 46 40 67 406969 92 80 5869 58 46 73 92 95 40 17 62 67 14 8225 46 10 87 56 27 23 56 17 62 67 92 95 56 69-56 67 9239 40 87 14 58,67 92 95 40 95 56 3156 99 92 18 95 92…

18 56 80 46 56 39 73 9246 40 80 92,56 6725 56 69 73 56 46 92 1725 46 5639 58 18 1025 56 17 36 18 92 69 99 27 36 39 1051 92 73 40 73 27:“38 73 5656 80 92 6738 58 17 56 69 58 9525 56 39 73 46 56 92 17,80 46 27 23 56 3124 40 69 39 58 23 80 4046 40 24 17 56 87 40 73 6239 87 56 43 58 73”.92,25 56 82 17 56 25 40 6925 5625 17 58 38 27 39 73 46 40 99 92 17 276924 67 40 9573 56 23 56,38 73 5667 40 25 40 46 67 92 9580 56 17 43 58 6718 80 92 73 58 17 62 67 5639 73 56 10 73 6267 4099 27 82 58 46 58,80 56 39 73 40 1795 92 67 43 40 1792 2425 46 92 99 92 73 14 8267 40 8095 56 17 58 67 56 8767 56 43 58 67.

18. 67 58 26 19 88 2332 37 15 23 90 63 7146 63 26-63 2658 2463 23 3732 956763 15 32 88 58 26-6726 58 6741 16 24 90 63 52 30 2449 63 2688 26 37 23 38 23 16 6758 2390 26 41 90 63 68 24 58 58 26 7685 15 67 76 24 15 24.19 26 15 23 38 88 2663 15 32 88 58 24 2490 88 24 16 23 63 7163 23 37,46 63 26 41 5437 15 23 95 676758 2438 23 76 24 63 67 16 6768 26 68 90 24,67 58 23 46 2437 63 26 – 63 2658 24 19 16 32 85 54 4426 46 24 58 7141 54 90 63 15 2690 88 24 16 23 24 6390 26 26 63 68 24 63 90 63 68 32 11 30 67 2468 54 68 26 88 546724 30 24,46 24 19 2688 26 41 15 26 19 26,85 15 67 76 24 63 90 5237 16 24 68 24 63 23 63 71,68 15 23 95 67 58 2367 88 24 26 16 26 19 67 46 24 90 37 23 52,85 32 90 63 7188 23 95 243258 24 19 266758 2441 32 88 24 6388 26 37 23 38 23 63 24 16 71 90 63 68,58 263746 24 76 3258 23 7616 67 83 58 52 5237 16 24 68 24 63 23?63 26-63 26…49 63 26 6356 67 58 23 1685 26 38 68 26 16 52 1626 88 58 67 7676 23 73 26 7615 24 83 67 63 7158 24 90 37 26 16 71 37 2638 23 88

23 46.58 2441 54 16 2658 67 37 23 37 26 4437 15 23 95 67,90 26 68 24 15 83 24 58 58 26 4473 68 23 63 37 67 76 6763 15 24 58 67 15 26 68 23 58 58 54 76 6715 24 41 52 63 23 76 67-85 15 26 90 63 26-58 23 85 15 26 90 63 2626 37 15 24 90 63 58 54 2485 23 15 63 67 38 23 58 54,88 23 68 58 54 76-88 23 68 58 2619 15 26 38 67 68 83 67 2488 26 41 15 23 63 71 90 5268 90 2495 2488 2626 85 16 26 63 2367 76 85 24 15 67 23 16 67 38 76 23,90 67 15 24 46 7188 23 58 58 26 4441 23 38 54,90 68 26 1132 19 15 26 38 326837 26 58 29 2437 26 58 29 26 6868 54 85 26 16 58 67 16 67.58 23 19 15 52 58 32 16 6758 26 46 58 26 4485 26 15 26 44,85 26 15 24 38 23 16 6737 26 16 11 46 37 32,85 15 26 58 67 37 16 6758 2341 23 38 3285 26 8885 26 37 15 26 68 26 7676 15 23 37 23,38 23 16 26 95 67 16 679085 26 16 88 11 95 67 58 5476 67 58,85 26 90 63 15 24 16 52 16 6767 3819 15 23 58 23 63 26 76 24 63 26 6867,90 85 15 23 68 24 88 16 67 68 2615 24 83 67 68,46 63 2688 26 90 63 23 63 26 46 58 2658 23 85 23 37 26 90 63 67 16 67,38 16 26 15 23 88 58 2685 26 16 11 41 26 68 23 16 67 90 7188 24 16 26 7615 32 3790 68 26 67 736732 41 15 23 16 67 90 7168 26 90 68 26 52 90 6741 24 3876 23 16 24 44 83 24 19 2688 16 5290 24 41 5232 15 26 58 23.

19. 3492 45 25 90 30 25 7116 62 37 7155 7189 18 96 6255 85 22 71 11 6262 24 62 89 71 55 55 6285 55 16 71 92 71 24 55 62 11 62-90 30 49 30 24 55 18 7124 16 85 92 30 55 18 7152 37 85 55 24 18,49 30 92 62 22 25 3022 85 24 16 18 7392 58 89 30 67 71 25,90 58 89 55 30 2086 71 16 25 302416 45 89 85 25 62 1449 30 24 16 18-89 92 62 52 20 11 7168 16 6249 62 96 62 37 71 55 62,25 62 96 8562 5530 34 24 16 92 30 96 85 71 4692 62 52 62 14,49 30 92 3089 30 55 62 2525 62 55 24 71 92 34 62 34,49 62 22 30 16 18 9439 96 30 25 62 552462 89 71 90 90 30 92 30 37 85 34 30 45 86 85 14 8534 62 52 5816 30 89 96 71 16 25 30 14 85,24 16 30 92 18 9425 62 14 49 30 24,62 89 67 30 92 49 30 55 55 18 9439 62 55 30 92 85 258549 92 62 22 30 2052 92 71 89 71 52 71 55 19,85 90 62 89 96 85 22 30 34 67 30 203452 37 62 55 7124 16 19 45 -25 30 25 -71 11 62-16 30 1452 62 24 16 30 16 62 22 55 6262 49 18 16 55 62 11 6249 58 16 71 67 71 24 16 34 71 55 55 85 25 30,14 30 16 92 62 24 302455 71 14 30 96 18 1424 16 30 37 71 14,3462 52 85 5549 92 71 25 92 30 24 55 18 9452 71 55 1992 71 67 85 34 67 71 11 6249 62 85 24 25 30 16 1924 22 30 24 16 19 2055 3089 71 92 71 11 58.49 92 71 52 71 96 19 55 6224 25 92 62 14 55 18 7149 62 37 85 16 25 85,55 7124 49 62 24 62 89 55 18 7149 92 85 34 96 71 22 1934 55 85 14 30 55 85 7124 71 92 19 71 90 55 18 7311 92 30 89 85 16 71 96 71 94.

85 14 71 96 62 24 198562 92 58 37 85 71,3025 30 2537 71.49 92 85 96 85 22 55 18 7392 30 90 14 71 92 62 3462 73 62 16 55 85 22 85 9455 62 37,34 16 62 92 62 94,25 30 92 14 30 55 55 18 9467 34 71 94 46 30 92 24 25 85 9449 71 92 62 22 85 55 55 85 252452 34 58 14 2052 71 24 20 16 25 30 14 8549 92 85 22 85 55 52 30 96 62 34,3016 30 25 37 7149 62 16 71 92 16 18 9449 85 24 16 62 96 71 16-25 62 96 19 1689 62 96 71 7122 71 1452 34 30 52 46 30 16 85 96 71 16 55 71 11 6234 62 90 92 30 24 16 30,55 6258 73 62 37 71 55 55 18 948524 14 30 90 30 55 55 18 94-85 14 71 55 55 6216 30 25 62 7162 92 58 37 85 7114 62 37 55 6289 71 9062 24 62 89 18 7349 92 62 89 96 71 1449 92 85 62 89 92 71 24 16853449 62 92 16 62 34 18 7316 92 58 86 62 89 30 73.34 24 7149 92 62 52 58 14 30 55 62.90 52 71 67 55 85 7149 62 96 85 46 30 852489 62 96 19 67 85 1449 62 52 62 90 92 71 55 85 71 1462 16 55 62 24 20 16 24 202524 58 89 10 71 25 16 30 142430 34 16 62 14 30 16 85 22 71 24 25 85 1462 92 58 37 85 71 1455 3049 96 71 22 71,90 30 16 6255 7162 24 62 89 6255 30 34 62 92 62 22 71 55 55 18 9425 30 92 30 89 85 5585 96 8549 92 62 24 16 71 55 19 25 85 9449 85 24 16 62 96 71 163425 30 92 14 30 55 713490 52 71 67 55 85 7314 71 24 16 30 7324 22 85 16 30 45 16 24 2055 71 49 92 71 14 71 55 55 18 1430 16 92 85 89 58 16 62 1458 34 30 37 30 45 86 71 11 6224 71 89 2025 30 89 30 96 19 71 92 62,49 85 24 19 14 71 55 55 62 11 6292 30 90 92 71 67 71 55 85 2055 7116 92 71 89 58 45 1685,3462 89 86 71 14,49 62 52 62 90 92 71 55 85 9455 71 34 18 90 18 34 30 45 16,49 62 25 302485 7349 62 14 62 86 19 4555 7124 62 16 34 62 92 20 1622 71 11 62-16 62 55 71 90 30 25 62 55 55 62 11 62.

20. 16 7453 74 47 47 8531 85 66 74 29 58 55 7416 96 74 66 85 55 11 66 5896 11 12 91 74 74 50 96 11 12 91 85 49 53 58 8547 11 33 74 26 74 31 2329 47 85 2645 29 85 55 74 29,96

11 12 33 85 96 74 29,33 11 96 74 285829 74 12 96 11 47 55 11-66 85 68 28 74 29 35 53 28 5847 35 16 85 96 47 74 29 96 85 33 85 91 91 23 85,47 29 85 96 28 11 21 18 58 8591 74 29 85 91 61 28 58 3366 11 28 74 33,66 85 68 28 74 29 35 53 28 5829 96 85 33 85 9188 35 55 6166 5891 8529 55 74 96 74 4933 58 96 74 29 74 49,47 55 11 96 85 91 61 28 58 8511 29 55 74 50 35 47 23,68 96 74 33 11 31 91 23 8568 96 35 12 74 29 58 28 58-55 96 11 28 58,91 85 29 85 47 55 6174 55 28 35 31 1129 12 43 29 53 11 43 47 435891 85 29 85 31 74 33 7428 35 31 1147 16 85 53 58 29 53 11 4316 74 79 11 96 91 11 4333 11 53 58 91 11…31 74 29 74 66 61 91 7447 28 74 96 7474 9174 55 33 85 55 58 66,88 55 7447 96 85 31 5829 47 85 68 7438 55 74 68 7496 11 12 91 74 74 50 96 11 12 58 4391 8516 74 16 11 31 11 85 55 47 4391 5829 74 85 91 91 23 26,91 5816 74 66 58 45 85 49 47 28 58 2633 11 53 58 91,29 74 74 50 18 852974 28 96 85 47 55 91 74 47 55 43 26,91 11 47 28 74 66 61 28 7433 74 79 91 7447 35 31 58 55 6116 7455 74 33 35,88 55 7474 9129 58 31 85 664729 85 96 26 74 55 35 96 23,91 8591 11 50 66 21 31 11 85 55 47 4391 5833 11 66 85 49 53 58 2616 96 58 12 91 11 28 74 2988 96 85 12 29 23 88 11 49 18 58 91 23,28 11 28-55 74:33 74 50 58 66 61 91 23 2616 11 55 96 35 66 85 49,16 74 47 55 74 2991 1174 50 74 88 58 91 85,16 96 74 29 85 96 28 5831 74 28 35 33 85 91 55 74 29,12 11 47 55 11 29,50 66 74 28 16 74 47 55 74 29…91 58 88 85 68 7416 74 31 74 50 91 74 68 74.47 58 8545 85 91 91 74 8591 11 50 66 21 31 85 91 58 8591 8591 1153 35 55 28 3516 96 58 50 11 29 66 43 66 7474 16 55 58 33 58 12 33 11.

74 9116 74 47 33 74 55 96 85 6666 85 29 85 85-55 11 3374 5516 11 91 11 33 85 96 58 28 11 91 23 74 55 26 74 31 58 66 1111 47 62 11 66 61 55 58 96 74 29 11 91 91 11 4331 74 96 74 68 11,91 852916 96 58 33 85 9635 79 85,31 11 66 85 28 7491 8555 11 28 11 4374 79 58 29 66 85 91 91 11 43.5835 55 23 28 11 66 11 47 6174 91 1116 96 43 33 85 26 74 91 61 28 742955 74 55 47 11 33 23 4968 74 96 74 31 74 28,68 31 8558 2653 85 47 55 85 96 28 1131 74 66 79 91 1150 23 66 1129 23 49 55 58 91 1133 85 47 55 91 74 68 7491 85 66 85 68 11 66 11.

21. 40 77 40,29 75 5875 28 75!15 61 75 23 40 52 672929 54 52 1115 75 65 58 5415 84 40 29 54 61 67 28 75 77 7558 84 11 18 77 75 61 67 28 54 35 40,77 52 1115 75 37 11 84 11 52 54 28 11,28 4028 11 29 49 37 75 35 75 13,35 29 40 52 84 40 58 28 75 1335 54 84 15 54 65 28 75 1315 75 37 58 40 13 11 28 58 1129 75 90 29 49 72 40 11 58 37 8015 18 72 35 4029 84 11 13 11 2815 11 84 29 75 4113 54 84 75 29 75 41,5415 75 5211 1137 58 29 75 61 75 1337 61 75 82 11 28 4015 54 84 40 13 54 52 35 4054 9029 75 29 37 1118 8237 58 40 84 54 28 28 49 4680 52 11 84,35 40 35 54 13 5415 40 61 54 61 5461 11 5890 4037 58 7552 7515 75 80 29 61 11 28 54 8028 4035 75 28 29 11 41 11 84 1158 40 35 54 4629 75 5858 84 11 46 52 20 41 13 75 29 75 35-37 20 84 84 11 40 61 54 37 58 54 65 11 37 35 75 1137 75 65 11 58 40 28 54 11,11 37 61 5429 52 18 13 40 58 67 37 80,28 7513 11 37 58 28 49 46,28 40 52 7515 75 61 40 77 40 58 67,29 15 75 61 28 1118 37 58 84 40 54 29 40 11 58.54 33 7528 40 77 61 80 52 28 7515 75 35 40 90 49 29 40 11 5852 75 33 61 11 37 58 67,15 84 75 80 29 61 11 28 28 18 2054 4652 11 84 82 40 29 75 412915 11 84 29 18 2013 54 84 75 29 18 20:28 1835 40 3582 11,75 28 4075 58 15 84 40 29 54 61 4028 4011 29 84 75 15 11 41 37 35 54 4192 84 75 28 5826 11 61 49 4137 58 84 11 61 35 75 29 49 4133 40 58 40 61 67 75 285458 75 84 82 11 37 58 29 11 28 28 7515 75 84 29 40 61 4075 58 28 75 72 11 28 54 803777 11 84 13 40 28 37 35 75 4154 13 15 11 84 54 11 41,4029 52 75 33 40 29 75 3575 52 182972 11 37 58 28 40 52 26 40 58 75 1333 11 84 11 77 75 29 49 1133 40 58 40 84 11 5475 52 28 75 77 7554 9029 75 11 28 28 49 4615 75 84 58 75 2926 11 61 49 4652 29 4065 40 37 4015 40 61 54 61 5415 7558 75 4158 75 65 35 111877 75 84 54 90 75 28 58 40,77 52 1135 40 35 75 13 18 -58 7533 52 54 58 11 61 67 28 75 13 1829 75 80 35 1115 75 65 18 52 54 61 37 8077 11 84 13 40 28 37 35 54 4135 84 11 41 37 11 84…75 33 19 11 35 58 54 29 28 75 37 58 5484 40 52 5437 58 75 54 5818 58 75 65 28 54 58 67,65 58 7529 7529 58 75 84 18 2013 54 84 75 29 18 2090 52 11 72 28 54 41,15 18 37 58 675428 11 29 11 61 54 35 54 4129 75 11 28 28 75-13 75 84 37 35 75 4192 61 75 5829 13 11 37 58 113737 75 20 90 28 54 35 40 13 5415 40 58 84 18 61 54 84 75 29 40 6115 84 54 61 11 77 40 20 23 54 1129 75 52 495415 40 84 1884 40 9029 84 75 52 1133 4952 40 82 1137 58 84 11 61 80 6115 7528 40 37 58 75 80 23 54

13,4028 1115 84 54 29 54 52 11 29 72 54 13 37 8015 75 52 29 75 52 28 49 1361 75 52 35 40 1335 84 54 77 37-13 40 84 54 28 11.

22. 56 9631 57 87 3756 7584 77 87 24 96 73 68 75,56 7550 37 16 42 68 77,7720 73 3737 49 56 77 39 77 87 37,39 73 3712 84 9616 91 64 56 91 87 37.75 56 84 73 16 91 68 94 75 7531 57 87 7544 16 37 84 73 577556 96 49 77 73 96 14 87 75 12 57:96 84 87 7556 7744 37 28 37 68 37 56 56 75 68 9656 96 7356 7550 37 16 42 68 77,56 7584 77 87 24 96 73 68 75,96 84 87 7573 77 2673 37 87 41 68 3784 77 87 24 96 73 68 7731 96 4950 37 16 42 68 7775 87 7550 37 16 42 37 6831 96 4984 77 87 24 96 73 68 75-56 9673 3739 73 3756 9612 64 37 28 75 73 41,56 3728 77 35 9656 9644 16 75 31 87 75 35 77 73 41 84 61.12 84 9644 16 96 35 56 75 9616 77 84 68 87 77 28 5787 96 73 61 736839 96 16 73 91,1235 75 49 56 4184 87 96 28 91 96 7356 96 26 96 28 87 96 56 56 3744 16 96 73 12 37 16 61 73 4149 77 44 77 84 56 37 1412 77 16 75 77 56 73.56 91 35 56 3768 77 6826 37 35 56 3731 57 84 73 16 96 9637 73 84 82 28 7784 26 77 73 57 12 77 73 41 84 61,91 31 75 16 77 73 41 84 616839 96 16 73 37 12 37 1426 77 73 96 16 7575 4950 37 16 37 28 68 77,12 84 73 91 44 77 96 731284 75 87 9149 77 44 77 84 56 37 1412 77 16 75 77 56 7337 73 64 37 28 77…

12 96 84 4137 68 16 91 35 77 82 22 75 1426 75 1612 56 96 49 77 44 56 3784 73 77 8756 9644 16 37 84 73 3739 91 35 75 26-12 16 77 35 28 96 31 56 57 26.44 37 28 37 49 16 96 12 77 73 4184 87 96 28 37 12 77 87 3712 84 96 647512 84 61.44 41 82 22 75 6444 75 12 3784 37 87 28 77 73 75 68 37 12-1273 37 26,39 73 3737 56 7556 9684 37 87 28 77 73 75 68 7512 37 12 84 96,7750 16 91 44 44 7749 77 64 12 77 73 7775 4912 37 96 56 56 37 1468 37 56 73 16 16 77 49 12 96 28 68 75,44 16 96 84 73 77 16 96 87 37 50 3750 37 84 73 75 56 75 39 56 37 50 3764 26 57 16 61-1273 37 26,39 73 3737 5612 37 12 84 9656 9644 37 16 73 41 9675 87 7512 87 77 28 96 87 96 94,75 87 7573 377528 16 91 50 37 961237 28 56 37 2687 75 94 96,7744 37 87 68 37 12 56 75 6849 28 96 42 56 96 1473 77 14 56 37 1444 37 87 75 94 75 75.12 84 9612 37 49 26 37 35 56 37,68 37 50 28 7791 84 87 37 12 87 96 56 56 37 50 3784 75 50 56 77 87 7756 96 7356 7791 84 87 37 12 87 96 56 56 37 2626 96 84 73 96.

23. 22 10 75 6247 1074 10 24 88 47 39 35 66 15 75 58 10 47 64 53 5385 66 35 10 69 62 28 10 24 5366 49 53 47 47 10 49 64 10 58 3928 22 88 17 10 79 47 88 1547 66 22 53.4447 10 85 17 10 28 53 24 75 443551 66 75 58 53 47 53 64 88.35 10 3572 62 28 10 24 6647 8817 10 69,4466 80 37 80 10 2469 49 88 75 3937 74 53 17 66 58 28 66 17 88 47 53 885385 66 35 66 15,22 37 28 75 58 28 10,35 66 58 66 17 62 8853 75 85 62 58 62 28 10 88 79 39,66 35 10 69 10 28 79 53 75 392849 10 28 47 6669 47 10 35 66 74 62 4274 88 75 58 10 42.79 53 17 66 35 53 8828 66 17 66 58 1072 62 24 5317 10 75 85 10 42 47 37 58 62,37 75 10 49 39 72 1037 58 66 47 37 24 102875 37 74 88 17 35 10 42.4428 66 79 88 242842 66 24 24,51 49 8858 37 74 10 47 47 62 8869 88 17 35 10 24 1069 62 72 35 6666 58 17 10 31 10 24 5364 28 88 58 625349 88 58 10 24 5353 47 58 88 17 39 88 17 10.37 49 53 28 53 58 88 24 39 47 66,47 6642 66 69 44 53 4747 8837 69 47 10 2474 88 47 44.66 4785 17 66 58 44 47 37 2417 88 51 53 75 58 17 10 64 53 66 47 47 37 9735 47 53 51 37.4428 69 44 2417 37 22 35 37,66 72 7 41 03 54 73 7 2485 88 17 662872 17 66 47 69 66 28 37 9722 88 17 47 53 24 39 47 53 64 3753,75 35 24 66 47 53 28 79 53 75 3947 10 49 17 10 75 35 17 62 58 62 74 5375 58 17 10 47 53 64 10 74 53,75 58 66 24 35 47 37 24 75 447585 88 17 28 66 1553 6974 47 66 31 88 75 58 28 1047 88 66 31 53 49 10 47 47 66 75 58 88 15,35 66 58 66 17 62 8885 66 49 75 58 88 17 88 51 10 24 5374 88 47 4425 58 66 1547 66 22 39 97.74 66 8853 74 44,42 66 17 42 8824 37 53 7572 66 17 42 88 75,72 62 24 6647 10 22 88 17 58 10 47 662835 47 53 51 88,5322 88 17 47 53 24 1088 80 8847 8837 75 85 88 24 5328 62 75 66 42 47 37 58 39.

24. 6152 16 36 26 14 5416 45 24 29 4595 1129 36 95 86 36 16 29 451452 49 75 36 4797 36 93 95 61 54 26 6197 3626 86 45 97 49 95 41 29 11 47.93 49 30 61 86 95 11 93 56 11 86 83 8995 36 47 49 1695 11 37 36 93 14 54 26 6195 1130 86 36 16 36 4721 86 11 33 49,2636 29 95 11 47 1495 1130 95 45 86 16 49 95 95 14 8993 30 36 16 14 29,33 11 54 29 14 891471 11 52 16

36 19 49 95 95 83 89,36 52 95 49 26 49 95 95 83 8952 11 54 98 26 86 16 11 93 36 89;75 93 49,29 11 2997 36 47 95 14 54 36 26 4147 95 49,26 86 36 61 54 1197 54 61 33 95 11 6126 29 11 47 49 89 29 11.21 86 3652 83 54 1126 11 47 11 6152 36 54 41 19 11 6129 36 47 95 11 86 1130 75 36 26 86 14 95 14 56 49.6186 36 54 29 95 45 5493 30 49 16 41,36 95 1197 36 93 93 11 54 11 26 41.97 36 93 97 36 86 36 54 29 36 4775 36 16 49 54 1154 98 26 86 16 11.3049 4952 49 71 33 11 54 36 26 86 95 36 4726 30 49 86 496145 71 95 11 5426 49 52 61.95 1145 71 29 36 8933 49 54 49 71 95 36 8929 16 36 30 11 86 1454 49 33 11 5461,97 36 26 86 11 16 49 30 19 14 891436 52 16 98 71 75 19 14 89,1416 11 71 75 54 61 93 83 30 11 5454 49 97 95 14 95 4595 1197 36 86 36 54 29 49.6145 26 54 83 19 11 5475 36 54 36 26.95 4926 36 30 26 49 4747 36 89-52 49 7136 52 49 16 86 36 95 36 30,95 49 97 16 14 61 86 95 83 89,97 36 37 36 33 14 8995 1147 11 75 95 14 86 36 78 36 95 95 45 9871 11 97 14 26 41.

-45 93 14 30 14 86 49 54 41 95 36,-26 29 11 71 11 5436 95,-95 11 2693 30 36 491447 8336 93 95 36.30 97 16 36 24 49 47,30 3626 95 4995 14 24 86 3695 4926 97 36 26 36 52 95 3630 83 71 30 11 86 4145 93 14 30 54 49 95 14 49.6116 36 52 29 3626 97 16 36 26 14 54:

-71 95 11 24 14 86,30 26 4921 86 3626 36 95?

-97 16 14 24 49 4797 36 26 54 49 93 95 14 8926 36 95.-33 49 26 86 36 4736 9597 36 29 11 71 11 5495 1197 45 26 86 36 89 97 45 71 83 16 49 29,

26 86 36 61 30 19 14 8995 1147 16 11 47 36 16 95 36 8929 16 83 19 29 4995 36 24 95 36 75 3626 86 36 54 14 29 11.-86 49 52 49 97 16 14 93 49 86 26 61,95 11 30 49 16 95 36 49,45 30 14 93 49 86 4147 95 36 33 49 26 86 30 3626 95 36 30,97 16 49 33 93 4924 49 4793 36 52 49 16 49 19 41 26 6193 3621 86 36 8995 36 24 14.29 11 29 36 4926 49 75 36 93 95 6124 14 26 54 3697 3686 30 36 49 47 4529 11 54 49 95 93 11 16 98?

25. 48 84 13 3394 13 48 42 33 46 82,84 13 82 4894 82 46 84 33 4213 88 82 84 16 46 1625 8250 17 481342 61 37 78 50 511682 42 13 82 84 16 46 1650 48 17 341376 82 25 82 1672 82 46 48 69 17 82 28 82,28 84 4851 75 4875 84 33 46 1646 33 84 33 17,75 33 37 82 13 17 341638 48 37 17 16 46 33.82 1713 58 94 25 33 69 58 13 33 4676 82 75 48 46 33 17 16 34,163476 82 25 33 69 58 13 33 4648 50 5113 94 48,38 42 8217 1648 94 42 781350 16 37 48.1376 37 16 28 82 37 64 17 4817 48 17 33 13 16 94 42 17 82 28 8272 58 46 8294 82 72 37 33 17 8213 94 48,38 42 8284 82 13 48 46 82 94 78 76 82 13 16 84 33 42 7851 75 4851 94 82 76 64 16 501638 42 8269 37 34 4217 58 17 4869 84 37 33 13 94 42 13 51 61 21 16 48:28 82 37 82 84 33,75 33 37 25 16 481688 82 46 82 84 17 58 4894 42 37 33 17 58,94 82 25 37 82 13 16 21 33,94 25 37 58 42 58 481369 48 50 17 58 8828 46 51 72 16 17 33 88,72 82 37 82 69 84 34 21 16 4850 82 37 3425 82 37 33 72 46 16,82 37 51 84 16 3413 82 91 17 58,16 17 94 42 37 51 50 48 17 42 5813 37 33 38 48 13 33 17 16 341650 51 69 58 25 16,76 46 48 17 16 42 48 46 78 17 58 8875 48 17 21 16 17,17 48 76 82 84 13 16 75 17 58 4869 13 48 69 84 581676 46 33 17 48 42 58,25 37 33 94 25 16,25 82 42 82 37 58 50 1676 82 46 78 69 51 61 42 94 3417 48 13 48 37 17 58 48,25 82 28 84 3376 16 64 51 4294 13 82 1650 48 37 69 25 16 48

25 33 37 42 16 17 58,37 33 94 42 48 17 16 341650 16 17 48 37 334 65 894 8213 94 48 50 1616 8894 82 25 37 82 13 48 17 17 58 50 1669 33 50 48 38 33 42 48 46 78 17 58 50 1694 13 82 91 94 42 13 33 50 16,94 48 37 48 72 37 34 17 58 8833 17 28 48 46 82 13,38 48 9188 46 48 72-88 13 33 46 331676 37 48 13 82 69 17 48 94 48 17 16 4828 82 94 76 82 84 33,37 33 69 84 33 38 5117 33 28 37 33 841364 25 82 46 33 88,19 16 28 51 37 5876 42 16 981698 33 37 48 91,88 37 33 17 34 21 16 48 94 341394 33 50 82 5094 48 37 84 98 4876 16 37 33 50 16 84,42 48 17 7872 58 25 33,17 3325 82 42 82 37 82 5076 82 25 82 16 42 94 3469 48 50 46 34,1637 58 72 58,17 3325 82 42 82 37 82 9194 42 82 16 42

72 58 25,76 51 94 42 58 17 1613 94 48 50 16 46 82 94 42 16 13 82 28 8272 82 28 33.82 1751 13 16 84 48 4613 48 21 1617 48 82 76 16 94 51 48 50 58 48,42 33 25 16 48,25 33 2551 46 16 98 58,82 94 13 48 21 48 17 17 58 4828 33 69 82 13 58 50 1637 82 75 25 33 50 16,1625 16 42 33,25 82 42 82 37 58 9151 50 16 37 33 48 4276 37 1669 13 51 25 33 8838 48 46 82 13 48 38 48 94 25 82 28 8228 82 46 82 94 33.

Библиографический список

1. Алферов А.П., Зубов А.Ю.,Кузьмин А.С.,Черемушкин А.В. Основы криптонрафии, Москва, Гелиос АРВ,2016,479С.

2. Бабаш А.В., Шанкин Г.П. Криптография. Москва, Солон-Р, 2012,511С.