Министерство образования, науки и молодежной политики Краснодарского края
Государственное бюджетное профессиональное образовательное учреждение
Краснодарского края
«АРМАВИРСКИЙ МАШИНОСТРОИТЕЛЬНЫЙ ТЕХНИКУМ»

Курс лекций по теме:

«*Данные и их кодирование. Теорема Котельникова. Информационные процессы».*

по дисциплине «Основы теории информации»
для студентов 2 курса

специальности *09.02.02 «Компьютерные сети»*

2017

Содержание:

ВВЕДЕНИЕ

Возникновение теории информации связывают обычно с появлением фундаментальной работы американского ученого К. Шеннона «Математическая теория связи» (1948). Однако в теорию информации органически вошли и результаты, полученные другими учеными. Например, Р. Хартли, впервые предложил количественную меру информации (1928), акад. В. А. Котельников, сформулировал важнейшую теорему о возможности представления непрерывной функции совокупностью ее значений в отдельных точках отсчета (1933) и разработал оптимальные методы приема сигналов на фоне помех (1946). Акад. А. Н. Колмогоров, внес огромный вклад в статистическую теорию колебаний, являющуюся математической основой теории информации (1941). В последующие годы теория информации получила дальнейшееразвитие в трудах советских ученых (А. Н. Колмогорова, А. Я. Хинчина, В. И. Сифорова, Р. Л. Добрушина, М. С. Пинскера, А. Н. Железнова, Л. М. Финка и др.), а также ряда зарубежных ученых (В. Макмиллана, А. Файнстейна, Д. Габора, Р. М. Фано, Ф. М. Вудворта, С. Гольдмана, Л. Бриллюэна и др.)

Возникновение индустрии обработки информации привело к возникновению индустрии средств ее защиты и к актуализации самой проблемы защиты информации, проблемы информационной безопасности.

Одна из наиболее важных задач информатизации процессов – кодирование сообщений и шифрования информации

В основе каждой технологии преобразования информации в данные лежат свои принципы. Вопросы, связанные с кодированием информации, относятся к технологическим разделам информатики.

Вопросами защиты и скрытия информации занимается наука криптология. Если рассматривают проблемы разработки конкретных методов и средств кодирования сообщений, то совокупность излагаемых вопросов называют теорией информации и кодирования или прикладной теорией информации.

ДАННЫЕ И ИХ КОДИРОВАНИЕ. ПРИНЦИПЫ КОДИРОВАНИЯ И ДЕКОДИРОВАНИЯ ИНФОРМАЦИИ

Элементы информационных объектов представляются элементами данных по определенному закону. Кодирование — процесс не случайный. Он происходит согласно избранному информационному методу, который исполняет роль *метода кодирования*.

Метод кодирования информации устанавливает соответствие между элементами записываемого информационного объекта и элементами данных, полученных в результате записи.

Выбор метода кодирования информации — важный вопрос технологического раздела информатики. Он должен быть согласован с выбором инструмента и материала записи. Ом также должен удовлетворять критериям, о которых сказано выше.

Для удобства изучения методы кодирования информации принято рассматривать по категориям. Роль этих категорий выполняют так называемые *схемы кодирования*.

Существуют три основные схемы кодирования. Это аналоговое, табличное и цифровое кодирование.

Схемы аналогового кодирования распространены в живой природе. В ходе развития научно-технического прогресса общество постепенно адаптировало их под свои нужды. Именно аналоговое кодирование нашло наиболее раннее применение при записи изображений, звука, видео.

Схемы табличного кодирования не имеют и не могут иметь реализаций в живой природе — это изобретение общества. Люди пользуются табличным кодированием с того момента как научились на пальцах обозначать предметы, животных, людей. На табличном кодировании основаны все виды письменности. Табличное кодирование обеспечивает большинство потребностей неавтоматизированного общественного информационного обмена.

Среди табличных схем кодирования особо выделяют две самостоятельные категории:

схемы таблично-символьного кодирования;

схемы таблично-цифрового кодирования.

Таблично-символьное кодирование широко используют при непосредственном информационном обмене, а схемы табличного и цифрового кодирования применяют, когда информационный обмен между людьми осуществляется с помощью средств вычислительной техники. Например, для обмена письменными сообщениями достаточно схем символьного кодирования. Но если сообщение должно быть отправлено по телеграфу или по электронной почте, то без цифрового кодирования не обойтись.

Цифровое кодирование не имеет реализаций ни в живой природе, ни в непосредственном информационном обмене между людьми. Это достижение современного общества. Применяется оно в системах автоматического информационного обмена и действует при сохранении информации или при её передаче между техническими устройствами.

ПРИНЦИПЫ КОДИРОВАНИЯ ИНФОРМАЦИИ

Вопросы, связанные с кодированием информации, относятся к технологическим разделам информатики. В основе каждой технологии преобразования информации в данные лежат свои принципы. Они связаны с избранной схемой кодирования.

Аналоговое кодирование

Аналоговое кодирование основано на понятии подобия. Цель аналогового кодирования — изменение физической природы последовательности данных. Это бывает полезно для увеличения плотности записи, надёжности хранения, скорости перемещения, удобства воспроизведения и других свойств данных.

Аналоговое кодирование — это способ кодирования, основанный на принципе регистрации непрерывной последовательности сигналов определенной физической природы в виде подобной ей последовательности данных другой физической природы.

Характерными техническими системами, реализующими аналоговое кодирование, являются:

фотографические устройства (кроме цифровых);

магнитофоны и видеокамеры (не цифровые);

устройства приёма и передачи радиосигналов.

Согласно определению, принцип аналогового кодирования имеет две характерные особенности:

как исходная последовательность сигналов, так и результирующая последовательность данных имеют непрерывный характер;

результирующие данные подобны исходным сигналам по избранному критерию подобия.

С принципами непрерывности и подобия связано широкое распространение аналогового кодирования информации в живой природе. Например, при получении визуальной информации человеку важны два фактора: яркость и цвет объекта наблюдения. Яркость определяется амплитудой световой волны, а цвет — её длиной (частотой).

Табличное кодирование

Табличное кодирование — это информационная технология, основанная на *периодическом* сравнении элементов сигнала с имеющимися модельными образцами. Поскольку сравнение не непрерывное, а периодическое, по его результатам формируется не непрерывная, а

дискретная последовательность данных. Эту последовательность называют *выборкой данных*. Выборка данных состоит либо из самих модельных образцов, взятых из справочной таблицы, либо из числовых кодов, указывающих на положение данных образцов в справочной таблице.

В первом случае кодирование называется *таблично-символьным*. Результатом таблично-символьного кодирования является символьная строка — последовательность символов.

Во втором случае кодирование называют таблично-цифровым. Результатом этого кодирования тоже является выборка данных, но состоящая не из символов, а из числовых указателей, обозначающих местоположение образцов в справочной таблице (в таблице кодирования).

Табличное кодирование — это способ кодирования, основанный на принципе формирования дискретной выборки данных по результатам периодического сопоставления регистрируемого сигнала с элементами-образцами предварительно заданного набора.

К таблично-символьным технологиям кодирования относится хорошо знакомая нам письменность. В её основе лежит, как вы знаете, запись звуков речи (непрерывных аналоговых сигналов) с помощью дискретных символов — букв. Сюда же относится и запись музыки с помощью нот. Примером таблично-цифрового кодирования может служить, например, замена букв группами цифр, выражающими положение этих букв в алфавите или в какой-либо иной таблице кодирования.

Как видите, в основе табличного кодирования лежит не принцип непрерывности, характерный для аналогового кодирования, а принцип дискретной выразительности. Два звука «*а*…» разной протяжённости, громкости и тональности выражаются дискретно одной и той же буквой — «А».

В табличном кодировании не соблюдается также и принцип подобия. Так, например, из того факта, что буква «Б» в азбуке имеет номер вдвое больший, чем номер буквы «А», никоим образом не следует, что при воспроизведении она должна звучать вдвое громче или вдвое дольше.

Табличное кодирование очень широко распространено в информационном обмене, обслуживающем общественные отношения. Достаточно сказать, что азбуки всех европейских языков — это таблицы образцов, устанавливающие соответствие между звуками и символами, используемыми для их записи. Вам, конечно, известно, что это соответствие, увы, не всегда бывает однозначным и нередко вызывает появление досадных ошибок в правописании. Поэтому при записи текстов следует руководствоваться не только азбукой, но и правилами орфографии, а также утвержденными словарями. Словари и правила тоже можно рассматривать как разновидности справочных таблиц.

Как таблично-символьное, так и таблично-цифровое кодирование всегда основаны на какой-то общественной договорённости, ведь таблица кодирования должна быть общеизвестной. Если это не так, значит, имеет

место искусственное ограничение информационного обмена, известное как *шифрование*. И основе любого метода шифрования всегда лежит какой-то метод кодирования.

Договорённости об используемой таблице кодирования часто опираются на общепринятые соглашения или на утверждённые стандарты.

Цифровое кодирование

У аналогового кодирования есть одно замечательное достоинство: при его использовании соблюдается принцип подобия между записываемым сигналом и данными, полученными в результате записи. В одних случаях это позволяет сделать запись наглядной, а в других — существенно упрощает её воспроизведение и восприятие. В итоге качественные аналоговые записи субъективно воспринимаются людьми как наиболее «естественные».

Важное достоинство табличного кодирования — лаконичность и однозначность, а важный недостаток — отсутствие подобия между записываемым сигналом и результатом записи. Из-за отсутствия подобия при воспроизведении записи не удается ограничиться сигнальным уровнем информационного обмена. Приходится задействовать второй и даже третий уровни (уровень распознавания образов и уровень интерпретации содержания). Поэтому воспроизведению записей, выполненных табличным кодированием, надо специально учиться. Продолжительность обучения — вся жизнь. Доколе человек остается в обществе, дотоле он находит новые, незнакомые ранее формальные знаки, символы, условные обозначения и другие средства дискретной выразительности.

Совместить принцип подобия, присущий аналоговому кодированию, с принципом дискретной выразительности, присущим табличному кодированию, позволяет так называемое цифровое кодирование.

Цифровое кодирование — это способ кодирования, основанный на принципе формирования выборки данных путём периодического измерения величины регистрируемого сигнала и записи числовых значений, пропорциональных результатам измерений.

Основное достоинство цифрового кодирования — эффективность. Она связана с широким использованием вычислительной техники для операций с выборками данных. Тот факт, что значения, хранящиеся в выборках, пропорциональны реальным физическим сигналам, позволяет использовать операции арифметики для работы с данными. А тот факт, что значения дискретны, позволяет применять к ним операции математической логики. Благодаря развитию вычислительной техники цифровое кодирование с каждым днём находит всё более широкое применение при записи и передаче звукозаписей, изображений и видео.

Аналого-цифровое преобразование

Цифровое кодирование, по сравнению с аналоговым, обеспечивает особую эффективность хранения информации. После преобразования аналоговой записи в цифровую обычно удаётся уменьшить объём хранимых данных примерно в десять раз. На одном компакт-диске цифровой

звукозаписи, как правило, можно разместить десяток музыкальных альбомов, а на одном частотном канале обычного эфирного телевидения легко размещаются десять каналов телевидения цифрового.

Вместе с тем, есть объективные причины, по которым в настоящее время нельзя полностью отказаться от аналоговых схем записи и воспроизведения информации. Вот лишь некоторые из них:

нельзя в одночасье заменить во всём мире обширный парк аналоговых технических устройств;

в мире накоплены огромные архивы кино-, фото-, видео- и звуковых материалов, записанных в аналоговых форматах, — для их воспроизведения аналоговая техника остаётся необходимой;

цифровые схемы кодирования вносят в запись дополнительные погрешности, связанные с самим принципом получения цифровой последовательности данных. При современном уровне развития техники (и технических стандартов) эти погрешности пока остаются достаточно заметными. Из-за них многие потребители пока не готовы отказаться от аналоговых устройств.

Необходимость работать одновременно с информацией, записанной разными технологиями, вызывает потребность в специальном классе приборов, выполняющих преобразование данных. Преобразование аналоговых данных в цифровые называется *аналого-цифровым преобразованием* (*АЦП*) — его применяют перед цифровой записью или передачей данных. Аналого-цифровой преобразователь имеется во всех моделях сотовых телефонов стандарта *GSM*, в цифровых фото- и видеокамерах, в сканирующих устройствах, а также в звуковых адаптерах персональных компьютеров.

Обратное преобразование цифровых данных в аналоговый сигнал называется *цифроаналоговым преобразованием* (*ЦАП*) — его обычно применяют перед воспроизведением данных. Характерный пример — видеоадаптер компьютера.

Если аналоговый сигнал был превращен в выборку данных, а затем по ней был вновь построен аналоговый сигнал, то итоговый сигнал неминуемо отличается от исходного. Искажения, вносимые во время аналого-цифрового преобразования, носят принципиальный характер. Избежать их невозможно, можно только стремиться к их уменьшению. В быту эти искажения часто называют «цифровым шумом».

РАННИЕ СИСТЕМЫ КОДИРОВАНИЯ ТЕКСТОВ

В первые двадцать лет своего развития компьютеры служили только для работы с числами.

Не случайно в те годы их называли *электронными вычислительными машинами*.

Разумеется, даже самые ранние образцы компьютеров умели печатать данные на бумаге. Однако умение печатать буквы и умение работать с текстами — это далеко не одно и то же. Вплоть до 1963 г. вычислительная техника не имела своих стандартов кодирования текстов. Для ввода и вывода текстовых данных использовалось оборудование, заимствованное в телеграфной связи: телетайпы и электрические пишущие машинки. Вместе с оборудованием из телеграфии заимствовались и стандарты кодирования символов.

Двоичное кодирование текста. Система Бэкона

До появления телеграфии существовал лишь один стимул к кодированию текстов — преобразование записи в тайнопись. Сегодня этой цели служит не кодирование, а шифрование, но различать эти понятия стали сравнительно недавно. Так что первые приёмы дискретного кодирования текстов имеют свои корни в криптографии.

В 1605 г. английский ученый, философ и политический деятель Фрэнсис Бэкон (1561—1626)опубликовал труд под названием «О приумножении наук», в котором впервые предложил двузначную схему шифрования текста. В этой схеме каждая буква английского алфавита обозначалась пятисимвольной группой, составленной из двух знаков. Бэкон демонстрировал работу своей системы на знаках и . Разумеется, можно использовать и любые иные приёмы дискретизации знаков — суть системы от этого не зависит.

Всего кодом Бэкона можно представить 32 (25) различимых письменных знака. Поскольку русский алфавит содержит 33 буквы, то, пожертвовав одной буквой (часто жертвуют буквой Ё), код Бэкона можно продемонстрировать и на русскоязычном тексте.

Схема Бэкона не выглядит эффективной, потому что количество знаков исходного сообщения увеличивается в пять раз. Однако цель Бэкона состояла не в том, чтобы сделать текст нечитаемым, а в том, чтобы скрыть сам факт наличия тайнописи.

Схема Бэкона не использует цифры, но её вполне можно считать цифровой. Прежде всего, это дискретная система, а в дискретных системах совершенно всё равно, какими знаками пользоваться. Заменив буквы и цифрами 0 и 1, мы получим таблично-цифровую систему пятиразрядного кодирования.

В соответствии с духом своего времени, Бэкон предполагал использовать изобретение для тайнописи. Однако он не упустил из виду возможности применения своей схемы для передачи сообщений с помощью колокольного звона, боевых труб, мушкетных выстрелов и вспышек света. Отмети также, что Бэкон обосновал использование пары различимых сигналов для передачи сообщений задолго до того, как Г. Лейбниц (1646—1716)впервые применил двоичную систему для представления числовых данных.

Двоичный код переменной длины. Система Морзе

В1844 г., когда американский изобретатель Сэмюэл Морзе (1791—1872)готовил к запуску первую экспериментальную линию телеграфной связи между Вашингтоном и Балтимором, ему потребовалась удобная и эффективная система кодирования символов. Альфред Вейл, помогавший Морзе, предложил кодировать передаваемые символы с помощью двух электрических сигналов: длинного (тире) и короткого (точка).

Вотличие от системы Бэкона, система Морзе несимметрична. В ней разные знаки алфавита кодируются разным количеством элементов (от одного до шести). Чем реже знак встречается в текстах, тем большее количество символов необходимо для его кодирования. Наиболее часто встречающиеся буквы E и T в системе Морзе кодируются одним элементом, а такие буквы, как Q и L — четырьмя.

Система Бодо. Введение управляющих кодов

Третья четверть девятнадцатого века — это эпоха пара и телеграфа. Энергия пара позволила людям быстро перемещаться ни большие расстояния. А телеграф позволил им при этом не разрывать социальные, экономические и культурные связи со своим сообществом. Механизация производственных процессов стала основным содержанием эпохи промышленной революции.

Потребовали механизации и телеграфные сети, охватившие к 1870 г. целые континенты. В то время с азбукой Морзе могли работать только подготовленные люди, способные воспринимать точки и тире «на глаз» или «на слух», а бурно развивающаяся экономика настойчиво требовала более простых телеграфных аппаратов.

Переменная длина кода, эффективная при передаче сообщений вручную, к середине 70-хгодов XIX века стала препятствием для механизации телеграфа. Чтобы приёмный аппарат мог без участия оператора различить, где заканчивается один знак и начинается другой, надо либо ввести дополнительный разделительный элемент, либо кодировать все знаки одинаковым количеством элементов, как предлагал ещё Фрэнсис Бэкон. Технический прогресс избрал второй путь.

В 1874 г. Эмиль Бодо во Франции разработал систему, которую назвали «печатающим телеграфом». Передающее устройство имело клавиатуру с пятью клавишами, похожими на фортепианные. Две левые клавиши (IV и V) приводились в действие левой рукой, а три правые (I, II и III) — правой.

Приёмное устройство распечатывало на бумажной ленте не точки и тире, как в аппаратах Морзе, а обычный текст. Внедрение системы Бодо имело огромный эффект. Отныне политики, банкиры и военачальники могли сами читать приходящие сообщения, не посвящая телеграфиста в конфиденциальное содержание.

Сочетаниями из пяти элементов можно выразить до 32 различных кодов. Бодо разместил их в таблице.

Номер строки определяла одна из четырёх возможных комбинаций клавиш для левой руки (0, IV, V, IV+V), а номер столбца — одна из восьми комбинаций клавиш для право руки (0, I, II, I+II, III, I+III, II+III, I+II+III)

В телеграфии необходимо передавать не только буквы, но также цифры и знаки препинания Поэтому 32-символьнойтаблицы для Бодо было явно не достаточно. В принципе, он мог просто ввести шестую клавишу ( ), но это усложнило бы обучение телеграфистов. Бодо решил действовать иначе — он ввёл вторую таблицу из 32 кодов. В первой таблице он разместил буквы, а во второй — цифры и знаки препинания. Для переключения между основной и дополнительной таблицами Бодо ввёл так называемые управляющие коды. Они не имеют символьного содержания, а сообщают приёмнику о том, что следующие поступающие символы он должен декодировать по другой таблице.

В XX в. роль управляющих кодов значительно усилилась. В современных таблицах кодирования текстов выделены целые области, в которых размещаются коды, не имеющие текстового содержания. Они предназначены исключительно для того, чтобы передатчик мог в какой-то степени управлять приёмником.

Система Мюррея. Введение кодов форматирования

Аппаратура Бодо заметно упростила получение телеграфных сообщений. Для чтения текстов, принятых аппаратом Бодо, специалист не требовался, однако она мало помогла отправителю. Телеграфный ключ Морзе сменили клавиши, похожие на фортепианные, а потребность в квалифицированном операторе по-прежнему осталась. Для решения этой проблемы в 1901 г. новозеландский журналист Дональд Мюррей предложил использовать в передающем устройстве клавиатуру, заимствованную у пишущей машинки.

Вместе с клавиатурой у пишущей машинки были позаимствованы две операции: прокрутка листа бумаги на новую строку и возврат каретки. Была также добавлена новая операция — удаление предыдущего символа как ошибочного. Для исполнения этих операций в таблицу кодирования были введены три новых управляющих кода, которых не было в системе Бодо. Эти коды сохранились до наших дней и выполняют функции форматирования текста:

код *LF* (*Line Feeding*) — код подачи строки;

код *CR* (*Carriage Return*) — код возврата каретки;

код *DEL* (*Delete*) — код отмены символа.

Система Мюррея была создана ради упрощения ввода текстов, но она повлияла и на их вывод. Новые коды форматирования дали возможность печатать принятые сообщения не на длинной ленте, а на листах обычного

формата. В 1908 г. эта возможность была реализована в аппаратах нового поколения, получивших название *телетайпов*.

Система FIELDDATA. Введение кодов-разделителей.

Недостатки системы кодирования Мюррея стали заметны лишь тогда, когда появились первые компьютеры и пришла пора автоматизировать информационный обмен.

Первые компьютерные сети были созданы Министерством обороны США в 50-хгодах XX в. Они соединяли посты наблюдения за воздушной обстановкой, службы управления воздушным движением, метеорологические службы. Обмен данными между компьютерами должен был проходить автоматически, но кодов телеграфной связи для этого оказалось мало. Так появилась группа военных стандартов под общим названием *FIELDDATA*, имевших следующие особенности:

семиразрядное кодирование с возможностью представления до 128 различимых кодов;

наличие кодов не только для прописных, но и для строчных букв английского алфавита;

наличие специальных кодов-разделителей данных.

Введение в действие кодов-разделителей имело огромное значение для автоматизации информационного обмена. Фактически, с введением специальных кодов-разделителей появилась возможность доступа к удалённым базам данных и автоматизации их информационного обмена. Одним из самых ярких проявлений новых возможностей информационного обмена стала электронная почта.

Примеры простейших кодов-разделителей, реализованных в системе *FIELDDATA*:

SBK (*Start of Block*) — начало блока данных. Сегодня этот код назвали бы «началом записи».

EBK (*End of Block*) — конец блока данных («конец записи»).

КОДИРОВАНИЕ И ШИФРОВАНИЕ ИНФОРМАЦИИ

В современном обществе успех любого вида деятельности сильно зависит от обладания определенными сведениями (информацией) и от отсутствия их (ее) у конкурентов. Чем сильней проявляется указанный эффект, тем больше потенциальные убытки от злоупотреблений в информационной сфере и тем больше потребность в защите информации. Одним словом, возникновение индустрии обработки информации привело к возникновению индустрии средств ее защиты и к актуализации самой проблемы защиты информации, проблемы информационной безопасности.

Одна из наиболее важных задач (всего общества) – задача кодирования сообщений и шифрования информации.

Вопросами защиты и скрытия информации занимается наука **криптология** (*криптос*– тайный,*логос*– наука). Криптология имеет два

основных направления – криптографию и криптоанализ. Цели этих направлений противоположны. Криптография занимается построением и исследованием математических методов преобразования информации, а криптоанализ – исследованием возможности расшифровки информации без ключа. Термин "криптография" происходит от двух греческих слов: *криптос* и *графейн*– писать. Таким образом, это тайнопись, система перекодировки сообщения с целью сделать его непонятным для непосвященных лиц и дисциплина, изучающая общие свойства и принципы систем тайнописи.

ОСНОВНЫЕ ПОНЯТИЯ КОДИРОВАНИЯ И ШИФРОВАНИЯ.

Код – правило соответствия набора знаков одного множества X знакам другого множества Y. Если каждому символу X при кодировании соответствует отдельный знак Y, то это кодирование. Если для каждого символа из Y однозначно отыщется по некоторому правилу его прообраз в X, то это правило называется декодированием.

Кодирование – процесс преобразования букв (слов) алфавита X в буквы (слова) алфавита Y.

При представлении сообщений в ЭВМ все символы кодируются байтами.

Пример 1.

Если каждый цвет кодировать двумя битами, то можно закодировать не более $\mathbf{2^2 = 4}$ цветов, тремя –$\mathbf{2^3 = 8}$ цветов, восемью битами (байтом) –$\mathbf{2^8=256}$ цветов. Для кодирования всех символов на клавиатуре компьютера достаточно 8 байтов.

Сообщение, которое мы хотим передать адресату, назовем **открытым сообщением.** Оно, естественно, определено над некоторым алфавитом.

Зашифрованное сообщение может быть построено над другим алфавитом. Назовем его **закрытым сообщением**. Процесс преобразования открытого сообщения в закрытое сообщение и есть **шифрование**.

Если **A**– открытое сообщение, **B**– закрытое сообщение (шифр) ,**f** – правило шифрования, то **f(A) = B**.

Правила шифрования должны быть выбраны так, чтобы зашифрованное сообщение можно было расшифровать. Однотипные правила (например, все шифры типа шифра Цезаря, по которому каждый символ алфавита кодируется отстоящим от него на n позиций символом) объединяются в классы, и внутри класса определяется некоторый параметр (числовой, символьный табличный и т.д.), позволяющий перебирать (варьировать) все правила. Такой параметр называется шифровальным

ключом. Он, как правило, секретный и сообщается лишь тому, кто должен прочесть зашифрованное сообщение (обладателю ключа).

При кодировании нет такого секретного ключа, так как кодирование ставит целью лишь более сжатое, компактное представление сообщения.

Если **k**– ключ, то можно записать **f(k(A)) = B**. Для каждого ключа **k**, преобразование **f(k)** должно быть обратимым, то есть **f(k(B)) = A**. Совокупность преобразования **f(k)** и соответствия множества **k** называется **шифром**.

ВИДЫ ШИФРОВ.

Имеются две большие группы шифров: шифры перестановки и шифры замены.

Шифр перестановки изменяет только порядок следования символов исходного сообщения. Это такие шифры, преобразования которых приводят к изменению только следования символов открытого, исходного сообщения.

Шифр замены заменяет каждый символ кодируемого сообщения на другой(ие) символ(ы), не изменяя порядок их следования. Это такие шифры, преобразования которых приводят к замене каждого символа открытого сообщения на другие символы, причем порядок следования символов закрытого сообщения совпадает с порядком следования соответствующих символов открытого сообщения.

Под **надежностью** понимается способность противостоять взлому шифра. При дешифровке сообщения может быть известно все, кроме ключа, то есть надежность шифра определяется секретностью ключа, а также числом его ключей. Применяется даже открытая криптография, которая использует различные ключи для шифрования, а сам ключ может быть общедоступным, опубликованным. Число ключей при этом может достигать сотни триллионов.

Один из лучших примеров алгоритма шифрования – принятый в 1977 году Национальным бюро стандартов США алгоритм стандарта шифрования данных DES (Data Encrypted Standard). Исследования алгоритма специалистами показали, что пока нет уязвимых мест, на основе которых можно было бы предложить метод криптоанализа, существенно лучший, чем полный перебор ключей. В июле 1991 года введен в действие аналогичный отечественный криптоалгоритм (стандарта ГОСТ 28147-89), который превосходит DES по надежности.

Криптографическая система – семейство X преобразований открытых текстов. Члены этого семейства индексируются, обозначаются символом **k**; параметр **k** является ключом. Множество ключей **K**– это набор возможных значений ключа **k**. Обычно ключ представляет собой последовательный ряд букв алфавита.

Открытый текст обычно имеет произвольную длину. Если текст большой и не может быть обработан шифратором (компьютером) целиком, то он разбивается на блоки фиксированной длины, а каждый блок шифруется отдельно, независимо от его положения во входной последовательности. Такие криптосистемы называются системами блочного шифрования.

Криптосистемы разделяются на **симметричные, с открытым ключом** и **системы электронной подписи**.

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

В системах с открытым ключом используются два ключа– открытый и закрытый, которые математически (алгоритмически) связаны друг с другом. Информация шифруется с помощью открытого ключа, который доступен всем желающим, а расшифровывается лишь с помощью закрытого ключа, который известен только получателю сообщения.

Электронной (цифровой) подписью (ЭЦП) называется присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения. К ЭЦП предъявляются два основных требования: легкость проверки подлинности подписи; высокая сложность подделки подписи.

В настоящее время симметричные шифры - это:

– блочные шифры. Обрабатывают информацию блоками определенной длины (обычно 64, 128 бит), применяя к блоку ключ в установленном порядке, как правило, несколькими циклами перемешивания и подстановки, называемыми раундами. Результатом повторения раундов является лавинный эффект - нарастающая потеря соответствия битов между блоками открытых и зашифрованных данных.

– поточные шифры, в которых шифрование проводится над каждым битом либо байтом исходного (открытого) текста с использованием гаммирования.

Существует множество (не менее двух десятков) алгоритмов симметричных шифров, существенными параметрами которых являются:

- стойкость;
- длина ключа;
- число раундов;
- длина обрабатываемого блока;
- сложность аппаратной/программной реализации.

Распространенные алгоритмы симметричного шифрования:

- DES и TripleDES (3DES)
- AES (Rijndael)
- ГОСТ 28147-89

В частности, AES — симметричный алгоритм блочного шифрования, принятый в качестве американского стандарта шифрования правительством США в 2002году, до него с 1977 года официальным стандартом США был

алгоритм DES. По состоянию на 2006 год AES является одним из самых распространённых алгоритмов симметричного шифрования.

Шифры традиционных симметричных криптосистем можно разделить на следующие основные виды [3,4]:

1. Шифры замены.
2. Шифры перестановки.
3. Шифры гаммирования.

Шифрование методом замены

Шифрование заменой (подстановкой) заключается в том, что символы шифруемого текста заменяются символами того же или другого алфавита в соответствие с заранее оговоренной схемой замены. Данные шифры являются наиболее древними. Принято делить шифры замены на моноалфавитные и многоалфавитные. При моноалфавитной замене каждой букве алфавита открытого текста ставится в соответствие одна и та же буква шифротекста из этого же алфавита одинаково на всем протяжении текста.

Рассмотрим наиболее известные шифры моноалфавитной замены.

Шифрование методом Цезаря

Свое название данный шифр получил по имени римского императора Гая Юлия Цезаря, который использовал этот шифр (сам способ был известен еще до Цезаря) при переписке с Цицероном (около 50 г. до н.э).

При шифровании исходного текста по данному методу каждая буква заменяется на другую букву того же алфавита путем ее смещения в используемом алфавите на число позиций равное K. При достижении конца алфавита выполняется циклический переход к его началу.

Общая формула шифра Цезаря имеет следующий вид:

C=P+K (mod M), где P – номер символа открытого текста, C – соответствующий ему номер символа шифротекста, K – ключ шифрования (коэффициент сдвига), M – размер алфавита (для русского языка M=32)

Для данного шифра замены можно задать фиксированную таблицу подстановок, содержащую соответствующие пары букв открытого текста и шифротекста.

Пример 2.

Таблица подстановок для символов русского текста при ключе K=3 представлена в таблице. Данной таблице соответствует формула C=P+3 (mod 32

Таблица подстановок шифра Цезаря для ключа K=3

а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р
г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у

с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я
ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в

Согласно формуле открытый текст «БАГАЖ» будет преобразован в шифротекст «ДГЖГЙ».

Дешифрование закрытого текста, зашифрованного методом Цезаря осуществляется по формуле P=C-K (mod M)

Другие примеры таблиц замены:

а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р
Q	W	E	R	T	Y	U	I	O	P	[	]	A	S	D	F	G

с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я
H	J	K	L	Z	X	C	V	B	N	M	<	>	@	%

Стойкость метода простой замены низкая. Зашифрованный текст имеет те же самые статистические характеристики, что и исходный, поэтому зная стандартные частоты появления символов в том языке, на котором написано сообщение, и подбирая по частотам появления символы в зашифрованном сообщении, можно восстановить таблицу замены. Для этого требуется лишь достаточно длинный зашифрованный текст, для того, чтобы получить достоверные оценки частот появления символов. Поэтому простую замену используют лишь в том случае, когда шифруемое сообщение достаточно коротко!

Стойкость метода равна 20 - 30, трудоемкость определяется поиском символа в таблице замены. Для снижения трудоемкости при шифровании таблица замены сортируется по шифруемым символам, а для расшифровки формируется таблица дешифрования, которая получается из таблицы замены сортировкой по заменяющим символам.

Многоалфавитная замена повышает стойкость шифра.

<u>Многоалфавитная одноконтурная обыкновенная подстановка</u>

Для замены символов используются несколько алфавитов, причем смена алфавитов проводится последовательно и циклически: первый символ заменяется на соответствующий символ первого алфавита, второй - из второго алфавита, и т.д. пока не будут исчерпаны все алфавиты. После этого использование алфавитов повторяется.

Рассмотрим шифрование с помощью ***таблицы Вижинера*** - квадратной матрицы с n^2 элементами, где n - число символов используемого алфавита. В первой строке матрицы содержится исходный алфавит, каждая следующая строка получается из предыдущей циклическим сдвигом влево на один символ.

Таблица Вижинера для русского алфавита:

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

Для шифрования необходимо задать ключ - слово с неповторяющимися символами. Таблицу замены получают следующим образом: строку "Символы шифруемого текста" формируют из первой строки матрицы Вижинера, а строки из раздела "Заменяющие символы" образуются из строк матрицы Вижинера, первые символы которых совпадают с символами ключевого слова.

При шифровании и дешифровании нет необходимости держать в памяти всю матрицу Вижинера, поскольку используя свойства циклического сдвига, можно легко вычислить любую строку матрицы по ее номеру и первой строке.

При шифровании символы из первой строки заменяются символами остальных строк по правилу a(1,i) -> a(k,i)

где k - номер используемой для шифрования строки.

Используя свойства циклического сдвига влево элементы k-ой строки можно выразить через элементы первой строки

$$a(k,i)=\begin{cases} a(1, i+k-1), \text{если } i \le n-k+1 \\ a(1, i-n+k-1), \text{если } i > n-k+1 \end{cases}$$

При дешифровании производится обратная замена a(k,i) -> a(1,i)

Поэтому необходимо решить следующую задачу: пусть очередной дешифруемый символ в тексте - a(1,j) и для дешифрования используется k-я строка матрицы Вижинера. Необходимо найти в k-ой строке номер элемента, равного a(1,j). Очевидно,

$$a(1,j)=\begin{cases} a(k, j-k+1), \text{если } j \geq k \\ a(k, n-k+j+1), \text{если } j < k \end{cases}$$

Стойкость метода равна стойкости метода подстановки, умноженной на количество используемых при шифровании алфавитов, т.е. на длину ключевого слова и равна 20*L, где L - длина ключевого слова.

С целью повышения стойкости шифрования предлагаются следующие усовершенствования таблицы Вижинера:

1. Во всех (кроме первой) строках таблицы буквы располагаются в произвольном порядке.
2. В качестве ключа используются случайные последовательности чисел, которые задают номера используемых строк матрицы Вижинера для шифрования.

Пример 3

При использовании ключа ***где*** слово ***группа студентов*** шифруется в ***жфштуе фцизйсхтз***

Многоалфавитная одноконтурная монофоническая подстановка

В монофонической подстановке количество и состав алфавитов выбирается таким образом, чтобы частоты появления всех символов в зашифрованном тексте были одинаковыми. При таком положении затрудняется криптоанализ зашифрованного текста с помощью его статистической обработки. Выравнивание частот появления символов достигается за счет того, что для часто встречающихся символов исходного текста предусматривается большее число заменяющих символов, чем для редко встречающихся.

Пример таблицы монофонической замены:

А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	_
Ф	Н	(	Щ	И	Г	Е	R	А	Д	Ы	~	@	S	Л	Я	Ж	^	С	Ш	М	Б	Q	П	Т	Х	Ю	Ъ	Р	}	\	_	#
*	Н	У	Щ	D	+	Е	R	=	Д	Ц	Й	Ч	[	В	Ь	)	О	&	{	М	Б	Q	П	Т	Х	Ю	Ъ	Р	}	\	_	<
Л	Н	(	Щ	И	]	Е	R	%	Д	Ы	~	@	G	/	Я	Э	З	"	Ш	М	Б	Q	П	Т	Х	Ю	Ъ	Р	}	\	_	W
Ф	Н	У	Щ	D	К	Е	R	А	Д	Ц	Й	Ч	S	+	Ь	Ж	^	С	{	М	Б	Q	П	Т	Х	Ю	Ъ	Р	}	\	_	V

Шифрование проводится так же, как и при простой подстановке, с той лишь разницей, что после шифрования каждого символа соответствующий ему столбец алфавитов циклически сдвигается вверх на одну позицию. Таким образом, столбцы алфавитов как бы образуют независимые друг от друга кольца, поворачиваемые вверх на один знак каждый раз после шифрования соответствующего знака исходного текста.

Многоалфавитная многоконтурная подстановка

Многоконтурная подстановка заключается в том, что для шифрования используются несколько наборов (контуров) алфавитов, используемых циклически, причем каждый контур в общем случае имеет свой индивидуальный период применения. Частным случаем многоконтурной полиалфавитной подстановки является замена по таблице Вижинера, если для шифрования используется несколько ключей, каждый из которых имеет свой период применения.

Общая модель шифрования подстановкой может быть представлена в следующем виде:

$t_ш = t_o + w \bmod (k-1)$,

где $t_ш$ - символ зашифрованного текста,

t_o - символ исходного текста,

w - целое число в диапазоне 0 - (k-1),

k - число символов используемого алфавита.

Если w фиксировано, то формула описывает одноалфавитную подстановку, если w выбирается из последовательности $w_1, w_2, ..., w_n$, то получается многоалфавитная подстановка с периодом n.

Если в многоалфавитной подстановке $n > m$ (где m - число знаков шифруемого текста) и любая последовательность w_i, i=1,2,...,n используется только один раз, то такой шифр является теоретически нераскрываемым. Такой шифр получил название шифра Вермэна.

Стойкость простой многоалфавитной подстановки оценивается величиной 20*n, где n - число различных алфавитов, используемых для замены. Усложнение многоалфавитной подстановки существенно повышает ее стойкость. Монофоническая подстановка может быть весьма стойкой (и даже теоретически нераскрываемой), однако строго монофоническую подстановку реализовать на практике трудно, а любые отклонения от монофоничности снижают реальную стойкость шифра.

Шифрование методами перестановки

Шифрование перестановкой заключается в том, что символы открытого текста переставляются по определенному правилу в пределах некоторого блока этого текста. Данные преобразования приводят к изменению только порядка следования символов исходного сообщения.

При достаточной длине блока, в пределах которого осуществляется перестановка, и сложном неповторяющемся порядке перестановки можно достигнуть приемлемой для простых практических приложений стойкости шифра.

Метод простой перестановки

При шифровании методом простой перестановки производят деление открытого текста на блоки одинаковой длины равной длине ключа. Ключ длины *n* представляет собой последовательность неповторяющихся чисел от 1 до *n*. Символы открытого текста внутри каждого из блоков переставляют в соответствие с символами ключа. Элемент ключа Ki в заданной позиции блока говорит о том, что на данное место будет помещен символ открытого текста с номером Ki из соответствующего блока.

Пример 4.

Зашифруем открытый текст «ПРИЕЗЖАЮДНЕМ» методом перестановки с ключом К=3142.

п	р	и	е	з	ж	а	ю	д	н	е	м
и	п	е	р	а	з	ю	ж	е	д	м	н

Для дешифрования шифротекста необходимо символы шифротекста перемещать в позицию, указанную соответствующим им символом ключа Ki.

Например, зашифруем текст

ГРУЗИТЕ_АПЕЛЬСИНЫ_БОЧКАХ блоком размером 8*3 и ключом 5-8-1-3-7-4-6-2.

Таблица простой перестановки будет иметь вид:

Ключ							
5	8	1	3	7	4	6	2
Г	Р	У	З	И	Т	Е	_
А	П	Е	Л	Ь	С	И	Н
Ы	_	Б	О	Ч	К	А	Х

Зашифрованное сообщение:

УЕБ_НХЗЛОЕСЛГАЫЕИАИЬЧРП_

Перестановка, усложненная по таблице

При усложнении перестановки по таблицам для повышения стойкости шифра в таблицу перестановки вводятся неиспользуемые клетки таблицы. Количество и расположение неиспользуемых элементов является дополнительным ключом шифрования.

При шифровании текста в неиспользуемые элементы не заносятся символы текста и в зашифрованный текст из них не записываются никакие символы - они просто пропускаются. При расшифровке символы зашифрованного текста также не заносятся в неиспользуемые элементы.

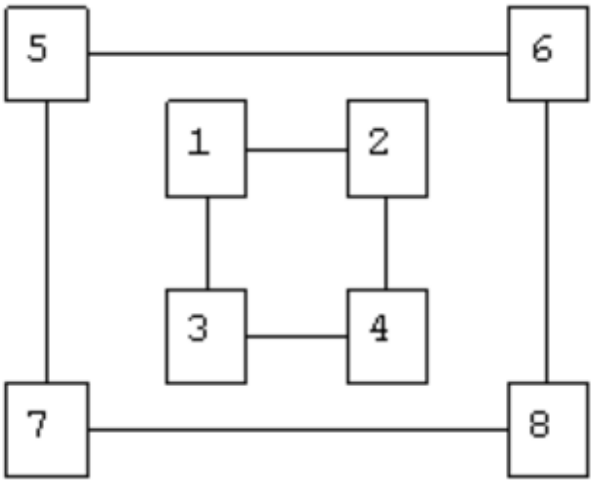
Для дальнейшего увеличения криптостойкости шифра можно в процессе шифрования менять ключи, размеры таблицы перестановки, количество и расположение неиспользуемых элементов по некоторому

алгоритму, причем этот алгоритм становится дополнительным ключом шифра.

Перестановка, усложненная по маршрутам

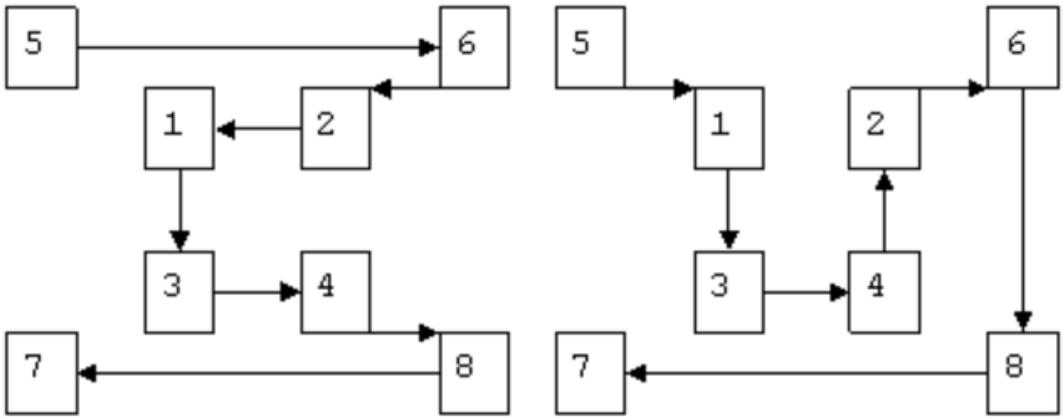
Высокую стойкость шифрования можно обеспечить усложнением перестановок по маршрутам типа гамильтоновских. При этом для записи символов шифруемого текста используются вершины некоторого гиперкуба, а знаки зашифрованного текста считываются по маршрутам Гамильтона, причем используются несколько различных маршрутов. Для примера рассмотрим шифрование по маршрутам Гамильтона при n=3.

Струкрура трехмерного гиперкуба:



Номера вершин куба определяют последовательность его заполнения символами шифруемого текста при формировании блока. В общем случае n-мерный гиперкуб имеет n^2 вершин.

Маршруты Гамильтона имеют вид:



Последовательность перестановок символов в шифруемом блоке для первой схемы 5-6-2-1-3-4-8-7, а для второй 5-1-3-4-2-6-8-7. Аналогично можно получить последовательность перестановок для других маршрутов: 5-7-3-1-2-6-8-4, 5-6-8-7-3-1-2-4, 5-1-2-4-3-7-8-6 и т.д.

Размерность гиперкуба, количество вид выбираемых маршрутов Гамильтона составляют секретный ключ метода.

Стойкость простой перестановки однозначно определяется размерами используемой матрицы перестановки. Например, при использовании матрицы 16*16 число возможных перестановок достигает 1.4E26. Такое число вариантов невозможно перебрать даже с использованием ЭВМ. Стойкость усложненных перестановок еще выше. Однако следует иметь в виду, что при шифровании перестановкой полностью сохраняются вероятностные характеристики исходного текста, что облегчает криптоанализ.

Шифрование методом гаммирования

Под гаммированием понимают наложение на открытые данные по определенному закону гаммы шифра

Гамма шифра – псевдослучайная последовательность, вырабатываемая по определенному алгоритму, используемая для шифровки открытых данных и дешифровки шифротекста.

Суть этого метода состоит в том, что символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности, которая называется гаммой. Иногда такой метод представляют как наложение гаммы на исходный текст, поэтому он получил название "гаммирование".

Процедуру наложения гаммы на исходный текст можно осуществить двумя способами.

При первом способе символы исходного текста и гаммы заменяются цифровыми эквивалентами, которые затем складываются по модулю k-1, где k - число символов в алфавите, т.е.: $R_i=(S_i+G) \bmod(k-1)$, где R_i – символы зашифрованноготекста, S_i – символы исходного текста, G – символы гаммы.

При втором методе символы исходного текста и гаммы представляются в виде двоичного кода, затем соответствующие разряды складываются по модулю 2.

Пример 5

шифрование гаммированием.

шифруемый текст	б	у	д	ь
	010010	100000	110010	100000
знаки гаммы	7	1	8	2
	000111	000001	001000	0000010
зашифрованный текст	010101	1000001	111010	100010

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

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

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

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

В аддитивных шифрах символы исходного сообщения заменяются числами, которые складываются по модулю с числами гаммы. Ключом шифра является гамма, символы которой последовательно повторяются.

Перед шифрованием символы сообщения и гаммы заменяются их номерами в алфавите и само кодирование выполняется по формуле

$$C_i = (T_i + G_i) \bmod N$$

Примечания:

а) ***mod*** - операция целочисленного деления, вычисляющая остаток от деления. Например, $18 \bmod 5 = 3$

или $48 \bmod 44 = 4$. Данная операция доступна в Windows-калькуляторе в режиме "Инженерный".

б) N равен количеству символов применяемого алфавита.

в) C_i, T_i и G_i - номера i-х символов, соответственно, шифрограммы, шифруемого текста и гаммы

г) если C_i будет равно нулю, то его следует приравнять N.

Создание шифрограммы завершается заменой полученных чисел C_i на соответствующие буквы алфавита.

Пример 6.

В рассмотренном ниже примере исходное сообщение - «КАФЕДРА СИСТЕМ ИНФОРМАТИКИ», используемая гамма - «СИМВОЛ».

В данной задаче используется алфавит, состоящий из 44 символов:

Русские буквы, цифры и пробел

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х

24	25	26	27	28	29	30	31	32	33	34	35	36	7	38	39	40	41	42	43	44
Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	пробел	0	1	2	3	4	5	6	7	8	9

Решение:

Схема шифрования гаммированием по модулю ***N***

T	К	А	Ф	Е	Д	Р	А		С	И	С	Т	Е	М		И	Н	Ф	О	Р	М	А	Т	И	К	И
G	С	И	М	В	О	Л	С	И	М	В	О	Л	С	И	М	В	О	Л	С	И	М	В	О	Л	С	И
T	12	1	22	6	5	18	1	34	19	10	19	20	6	14	34	10	15	22	16	18	14	1	20	10	12	10
G	19	10	14	3	16	13	19	10	14	3	16	13	19	10	14	3	16	13	19	10	14	3	16	13	19	10
T+G	31	11	36	9	21	31	20	44	33	13	35	33	25	24	48	13	31	35	35	28	28	4	36	23	31	20
mod N	31	11	36	9	21	31	20	0	33	13	35	33	25	24	4	13	31	35	35	28	28	4	36	23	31	20
0 →N	31	11	36	9	21	31	20	44	33	13	35	33	25	24	4	13	31	35	35	28	28	4	36	23	31	20
C	Э	Й	1	З	У	Э	Т	9	Я	Л	0	Я	Ч	Ц	Г	Л	Э	0	0	Ъ	Ъ	Г	1	Х	Э	Т

Дешифрование выполняется по формуле:
$T_i = (C_i - G_i + N) \bmod N$,
где T_i – это символы исходного сообщения, C_i – символы зашифрованного сообщения, G_i – символы гаммы.

Примечание:
если $T_i = 0$, то его следует взять равным N.
В примере ниже зашифрованное выше сообщение вновь приводится к исходному виду

C	Э	Й	1	З	У	Э	Т	9	Я	Л	0	Я	Ч	Ц	Г	Л	Э	0	0	Ъ	Ъ	Г	1	Х	Э	Т
G	С	И	М	В	О	Л	С	И	М	В	О	Л	С	И	М	В	О	Л	С	И	М	В	О	Л	С	И
C	31	11	36	9	21	31	20	44	33	13	35	33	25	24	4	13	31	35	35	28	28	4	36	23	31	20
G	19	10	14	3	16	13	19	10	14	3	16	13	19	10	14	3	16	13	19	10	14	3	16	13	19	10
C-G	12	1	22	6	5	18	1	34	19	10	19	20	6	14	-10	10	15	22	16	18	14	1	20	10	12	10
C-G+N	56	45	66	50	49	62	45	78	63	54	63	64	50	58	34	54	59	66	60	62	58	45	64	54	56	54
mod N	12	1	22	6	5	18	1	34	19	10	19	20	6	14	34	10	15	22	16	18	14	1	20	10	12	10
0 →N	12	1	22	6	5	18	1	34	19	10	19	20	6	14	34	10	15	22	16	18	14	1	20	10	12	10
T	К	А	Ф	Е	Д	Р	А		С	И	С	Т	Е	М		И	Н	Ф	О	Р	М	А	Т	И	К	И

Схема дешифрирования гаммированием по модулю N

Чем длиннее ключ, тем надежнее шифрование методом гаммирования. На практике длина ключа ограничена возможностями аппаратуры обмена данными и вычислительной техники, а именно выделяемыми объемами памяти под ключ, временем обработки сообщения, а также возможностями аппаратуры подготовки и записи последовательностей ключей. Кроме того, для использования ключа вначале необходимо каким-либо надежным способом доставить его обеим сторонам, обменивающимся сообщениями. Это приводит к возникновению проблемы распределения ключей, сложность решения которой возрастает с увеличением длины ключа и количества абонентов в сети передачи сообщений.

Пример 7:

Используя ключ **весна** закодировать **гаммирование**

Для этого переведем каждую букву слова в шестнадцатеричный код, а затем в двоичный. Кодовое слово также представим в виде двоичного кода. И найдем двоичный результат сложения, который затем переведем в шестнадцатеричный вид:

Исходный текст: *Гаммирование*

Исходный текст в шестнадцатеричном виде:

83 A0 AC AC A8 E0 AE A2 A0 AD A8 A5

Гамма (Ключ): *Весна (82 A5 E1 AD A0)*

Гаммирование

Исх. биты	1000	0011	1010	0000	1010	1100
Гамма	1000	0010	1010	0101	1110	0001
Результат	0000	0001	0000	0101	0100	1101

Исх. биты	1010	1100	1010	1000	1110	0000
Гамма	1010	1101	1010	0000	1000	0010
Результат	0000	0001	0000	1000	0110	0010

Исх. биты	1010	1110	1010	0010	1010	0000
Гамма	1010	0101	1110	0001	1010	1101
Результат	0000	1011	0100	0011	0000	1101

Исх. биты	1010	1101	1010	1000	1010	0101
Гамма	1000	0010	1010	0101	1110	0001
Результат	0010	1111	0000	1101	0100	0101

Закодированный текст в шестнадцатеричном виде:

01 05 4D 01 08 62 0B 43 0D 2F 0D 45

Шифрование с помощью аналитических преобразований

Достаточно надежное закрытие информации может обеспечить использование при шифровании некоторых аналитических преобразований. Например, можно использовать методы алгебры матриц - в частности умножение матрицы на вектор.

В качестве ключа задается квадратная матрица ||a|| размера n*n. Исходный текст разбивается на блоки длиной n символов. Каждый блок рассматривается как n-мерный вектор. А процесс шифрования блока заключается в получении нового n-мерного вектора (зашифрованного блока) как результата умножения матрицы ||a|| на исходный вектор.

Расшифрование текста происходит с помощью такого же преобразования, только с помощью матрицы, обратной ||a||. Очевидно, что ключевая матрица ||a|| должна быть невырожденной.

Комбинированные методы шифрования

Достаточно эффективным средством повышения стойкости шифрования является комбинированное использование нескольких различных способов шифрования, т.е. последовательное шифрование исходного текста с помощью двух или более методов.

Стойкость комбинированного шифрования S не ниже произведения стойкостей используемых способов

$S >= S_1*S_2*...*S_k$

Если какой-либо способ шифрования при независимом применении может обеспечить стойкость не ниже S, то комбинировать его с другими способами целесообразно лишь при выполнении условия

$R > R_1+R_2+ ... +R_k$,

где R_i - трудоемкость i-го способа, используемого при комбинированном шифровании, R - трудоемкость того способа, который обеспечивает стойкость не ниже S.

Криптография изучает, кроме криптосистем (симметричных, с открытым ключом, электронной подписи), еще и системы управления ключами.

Системы управления ключами– это информационные системы, целью которых является составление и распределение ключей между пользователями информационной системы.

Разработка ключевой, парольной информации является типовой задачей администратора безопасности системы. Ключ может быть сгенерирован как массив нужного размера статистически независимых и равновероятно распределенных на двоичном множестве{0, 1}элементов.

Пример 8.

Для таких целей можно использовать программу, которая вырабатывает ключ по принципу "электронной рулетки". Когда число пользователей, то есть объем необходимой ключевой информации, очень большой, используют чаще аппаратные датчики случайных (псевдослучайных) чисел. Пароли также необходимо менять.

Например, известный вирус Морриса пытается войти в систему, последовательно пробуя пароли из своего внутреннего эвристически составленного списка в несколько сотен процедур, имитирующих "сочинение" паролей человеком.

Пароли должен генерировать и раздавать пользователям системный администратор по безопасности, исходя из основного принципа: обеспечения равной вероятности появления каждого из символов алфавита в пароле.

В процессе шифрования, чтобы ключ был использован полностью, необходимо многократно выполнять процедуру кодировки с различными элементами. Базовые циклы заключаются в многократном применении разных элементов ключа и отличаются друг от друга только числом повторения и порядком использования ключевых элементов.

Пример 9.

В банковских системах первоначальный обмен ключами между клиентом и банком осуществляется на магнитных носителях без передачи ключей через открытые компьютерные сети. Секретный ключ клиента хранится на сервере сертификации банка и закрыт для доступа. Для осуществления всех операций с ЭЦП на компьютер клиента устанавливается программное обеспечение, которое предоставляет банк, а все необходимые данные для клиента – открытый, закрытый ключ, логин, пароль и др. — обычно хранятся на отдельной дискете или на специальном устройстве, подключаемом к компьютеру клиента.

Все современные криптосистемы построены по принципу Кирхгоффа: секретность зашифрованных сообщений определяется секретностью ключа.

Это означает, что если даже алгоритм шифрования будет известен криптоаналитику, то он, тем не менее, не в состоянии будет расшифровать закрытое сообщение, если не располагает соответствующим ключом. Все классические шифры соответствуют этому принципу и спроектированы таким образом, чтобы не было пути вскрыть их более эффективным способом, чем полный перебор по всему ключевому пространству, то есть перебор всех возможных значений ключа. Ясно, что стойкость таких шифров определяется размером используемого в них ключа.

Пример 10.

В российских шифрах часто используется 256-битовыйключ, а объем ключевого пространства составляет $\mathbf{2^{256}}$. Ни на одном реально существующем или возможном в недалеком будущем компьютере нельзя

подобрать ключ (полным перебором) за время, меньшее многих сотен лет. Российский криптоалгоритм проектировался с большим запасом надежности, стойкости.

ОРГАНИЗАЦИОННЫЕ ПРОБЛЕМЫ КРИПТОЗАЩИТЫ

Информационная безопасность информационной системы – защищенность информации, обрабатываемой компьютерной системой, от внутренних (внутрисистемных) или внешних угроз, то есть состояние защищенности информационных ресурсов системы, обеспечивающее устойчивое функционирование, целостность и эволюцию системы. К защищаемой информации (информационным ресурсам системы) относятся электронные документы и спецификации, программное обеспечение, структуры и базы данных и др.

Оценка безопасности компьютерных систем базируется на различных классах защиты систем:

класс систем минимальной защищенности (класс D);

класс систем с защитой по усмотрению пользователя (класс C);

класс систем с обязательной защитой (класс B);

класс систем с гарантированной защитой (класс A).

Эти классы имеют и подклассы, но мы их не будем здесь детализировать.

Рассмотренные значения стойкости шифров являются потенциальными величинами. Они могут быть реализованы при строгом соблюдении правил использования криптографических средств защиты.

Основные правила криптозащиты:

1. Сохранение в тайне ключей.
2. Исключение дублирования.
3. Достаточно частая смена ключей.

Под дублированием здесь понимается повторное шифрование одного и того же отрывка текста с использованием тех же ключей (например, если при первом шифровании произошел сбой). Нарушение этого правила резко снижает надежность шифрования, так как исходный текст может быть восстановлен с помощью статистического анализа двух вариантов зашифрованного текста.

Важнейшим правилом криптозащиты является достаточно частая смена ключей. Причем частота может определяться исходя из длительности использования ключа или исходя из объема зашифрованного текста. При этом смена ключей по временному графику является защитной мерой против возможного их хищения, смена после шифрования определенного объема текста - от раскрытия шифра статистическими методами.

Нельзя допускать злоумышленнику возможности направить в систему ряд специально подобранных сообщений и получать их в зашифрованном виде. Такого взлома не может выдержать ни одна криптосистема!

Важными аспектами организации криптозащиты являются выбор способа закрытия, распределение ключей и доставка их в места пользования (механизм распределения ключей).

Выбор способа защиты тесно связан с трудоемкостью метода шифрования, степенью секретности закрываемых данных, стойкостью метода и объемом шифруемой информации.

Один из принципов криптографии является предположение о несекретности метода закрытия информации. Предполагается, что необходимая надежность закрытия обеспечивается только за счет сохранения в тайне ключей. Отсюда вытекает принципиальная важность формирования ключей, распределения их и доставка в пункты назначения. Основными правилами механизма распределения ключей являются:

1. Ключи должны выбираться случайно.
2. Выбранные ключи должны распределяться таким образом, чтобы не было закономерностей в изменении ключей от пользователя к пользователю.
3. Должна быть обеспечена тайна ключей на всех этапах функционирования системы. Ключи должны передаваться по линиям связи, почте или курьерами в зашифрованном виде с помощью другого ключа. На практике часто образуется иерархия ключей шифрования, в которой ключи нижнего уровня при пересылке шифруются с помощью ключей верхнего уровня. Ключ в вершине иерархии не шифруется, а задается и хранится у доверенного лица, рассылается пользователям курьерами. Чем ниже уровень ключа, тем чаще он меняется и рассылается по линиям связи. Подобная схема шифрования ключей часто используется в сетях.

ЗАКЛЮЧЕНИЕ

В пособии описаны принципы кодирования и декодирования информации. Приведены примеры ранних систем кодирования текстов, что позволяет студентам с помощью исторических фактов лучше понять необходимость кодирования и этапы развития криптологии. Подробно описаны виды шифров: шифры перестановки, шифры замены, шифры гаммирования. Приведены примеры, иллюстрирующие теоретические основы шифрования. Также рассмотрены организационные проблемы криптозащиты. В приложении собраны задания для практической работы по соответствующей теме.

ПРИЛОЖЕНИЕ 1.

ЗАДАНИЯ К ПРАКТИЧЕСКОЙ РАБОТЕ №2

Тема: Шифрование текстовой информации
Цель: закрепить навыки шифрования и дешифровки методом перестановки, замены, гаммирования.

Вариант 1

Задание 1.
Открытый текст: **ЭТО_ТЕКСТ_ДЛЯ_ШИФРОВАНИЯ**
Проведите шифрование методом простой перестановки, используя ключ для подстановки **436215**

Задание 2.
Открытый текст: **ЭТО ТЕКСТ ДЛЯ ШИФРОВАНИЯ**
Найдите закрытый текст, используя метод Цезаря

Задание 3.
Открытый текст **ПОСЫЛАЮ _15_ КГ _ ВЗРЫВЧАТКИ**
Используя табличный способ кодирования и таблицу 6х4 (6 столбцов, 4 строки) с траекторией заполнения сверху вниз. Способ получения закрытого сообщения – змейкой, начиная с левого нижнего угла

Задание 4.
С помощью таблицы Вижинера и ключевого слова **МОЦАРТ** закодируйте фразу: **ПОСТРОЮ СЕБЕ ДВУХЭТАЖНЫЙ ДОМ**

Задание 5.
Закрытое сообщение: **209·(000-8)1· +369+:4**
Ключ: 15423
Найдите открытое сообщение. Решите пример

Вариант 2

Задание 1.
Открытый текст: **ЭТО_ТЕКСТ_ДЛЯ_ШИФРОВАНИЯ**
Проведите шифрование методом простой перестановки, используя ключ для подстановки **432651**

Задание 2.
Открытый текст: **ПОСЫЛАЮ СТО КГ ВЗРЫВЧАТКИ**
Найдите закрытый текст, используя метод Цезаря

Задание 3.
Открытый текст **ПОСЫЛАЮ _15_ КГ _ ВЗРЫВЧАТКИ**

Используя табличный способ кодирования и таблицу 6х4 (6 столбцов, 4 строки) с траекторией заполнения снизу вверх. Способ получения закрытого сообщения – змейкой, начиная с левого верхнего угла

Задание 4.
С помощью таблицы Вижинера и ключевого слова **САЛЬЕРИ** закодируйте фразу: **ПОСТРОЮ СЕБЕ ДВУХЭТАЖНЫЙ ДОМ**

Задание 5.
Закрытое сообщение: **9·7-9+7·6·4-4·6614:+** **К**люч: 32541
Найдите открытое сообщение. Решите пример

Вариант 3

Задание 1.
Открытый текст: **ЭТО_ТЕКСТ_ДЛЯ_ШИФРОВАНИЯ**
Проведите шифрование методом простой перестановки, используя ключ для подстановки **523164**

Задание 2.
Открытый текст: **ПОСТРОЮ СЕБЕ ДВУХЭТАЖНЫЙ ДОМ**
Найдите закрытый текст, используя метод Цезаря

Задание 3.
Открытый текст **ПОСЫЛАЮ _15_ КГ _ ВЗРЫВЧАТКИ**
Используя табличный способ кодирования и таблицу 4х6 (4 столбца, 6 строк) с траекторией заполнения снизу вверх. Способ получения закрытого сообщения – змейкой, начиная с правого нижнего угла

Задание 4.
С помощью таблицы Вижинера и ключевого слова **МУЗЫКА** закодируйте фразу: **ПОСТРОЮ СЕБЕ ДВУХЭТАЖНЫЙ ДОМ**

Задание 5.
Закрытое сообщение: **·209(-0008+1)1·3:69+4**
Ключ: 21543
Найдите открытое сообщение. Решите пример

Вариант 4

Задание 1.
Открытый текст: **ХОРОШО_КОГДА_КАНИКУЛЫ**
Проведите шифрование методом простой перестановки, используя ключ для подстановки **5273164**

Задание 2.
Открытый текст: **ХОРОШО КОГДА ЛЕТНИЕ КАНИКУЛЫ**
Найдите закрытый текст, используя метод Цезаря

Задание 3.
Открытый текст **ПОСЫЛАЮ _15_ КГ _ ВЗРЫВЧАТКИ**
Используя табличный способ кодирования и таблицу 4х6 (4 столбца, 6 строк) с траекторией заполнения сверху вниз. Способ получения закрытого сообщения – змейкой, начиная с правого верхнего угла

Задание 4.
С помощью таблицы Вижинера и ключевого слова **МУЗЫКА** закодируйте фразу: **КТО СЛЕДУЮЩИЙ ПРОЙДИТЕ В КАБИНЕТ**

Задание 5.
Закрытое сообщение: **4+0(1)4:6+·2(3+·213)**
Ключ: 24315
Найдите открытое сообщение. Решите пример

Вариант 5

Задание 1.
Открытый текст: **ХОРОШО_КОГДА_КАНИКУЛЫ**
Проведите шифрование методом простой перестановки, используя ключ для подстановки **5432167**

Задание 2.
Открытый текст: **КТО СЛЕДУЮЩИЙ ПРОЙДИТЕ В КАБИНЕТ**
Найдите закрытый текст, используя метод Цезаря

Задание 3.
Открытый текст **ПОСЫЛАЮ _15_ КГ _ ВЗРЫВЧАТКИ**
Используя табличный способ кодирования и таблицу 4х6 (4 столбца, 6 строк) с траекторией заполнения по спирали (по часовой стрелке) от левого верхнего угла. Способ получения закрытого сообщения – снизу вверх

Задание 4.
С помощью таблицы Вижинера и ключевого слова **САЛЬЕРИ** закодируйте фразу: **КТО СЛЕДУЮЩИЙ ПРОЙДИТЕ В КАБИНЕТ**

Задание 5.
Закрытое сообщение: **154(-0)01:+619·38+( )**
Ключ: 24315
Найдите открытое сообщение. Решите пример

Вариант 6

Задание 1.
Открытый текст: **ХОРОШО_КОГДА_КАНИКУЛЫ**
Проведите шифрование методом простой перестановки, используя ключ для подстановки **5471326**

Задание 2.
Открытый текст: **ВВЕДИТЕ ОТВЕТ В ДИАЛОГОВОМ ОКНЕ**
Найдите закрытый текст, используя метод Цезаря

Задание 3.
Открытый текст **СИСТЕМА_ПОТРЕБУЕТ_ОТВЕТА**
Используя табличный способ кодирования и таблицу 4х6 (4 столбца, 6 строк) с траекторией заполнения по спирали (против часовой стрелки) от левого верхнего угла. Способ получения закрытого сообщения – снизу вверх

Задание 4.
С помощью таблицы Вижинера и ключевого слова **МОЦАРТ** закодируйте фразу: **КТО СЛЕДУЮЩИЙ ПРОЙДИТЕ В КАБИНЕТ**

Задание 5.
Закрытое сообщение: **(·9028-0003+·1)4:+96**
Ключ: 32451
Найдите открытое сообщение. Решите пример

Вариант 7

Задание 1.
Открытый текст: **ЛЕТО_ПРОШЛО_НАДО_УЧИТЬСЯ**
Проведите шифрование методом простой перестановки, используя ключ для подстановки **541326**

Задание 2.
Открытый текст: **ЛЕТО БЫСТРО ПРОШЛО НАДО УЧИТЬСЯ**
Найдите закрытый текст, используя метод Цезаря

Задание 3.
Открытый текст **СИСТЕМА_ПОТРЕБУЕТ_ОТВЕТА**
Используя табличный способ кодирования и таблицу 4х6 (4 столбца, 6 строк) с траекторией заполнения снизу вверх. Способ получения закрытого сообщения – змейкой, начиная с левого нижнего угла

Задание 4.
С помощью таблицы Вижинера и ключевого слова **МАСТЕР** закодируйте фразу: **КТО СЛЕДУЮЩИЙ ПРОЙДИТЕ В КАБИНЕТ**

Задание 5.
Закрытое сообщение: **·79-97··6+-46·414+:6**
Ключ: 25143

Найдите открытое сообщение. Решите пример

Вариант 8

Задание 1.

Открытый текст: **ЛЕТО_ПРОШЛО_НАДО_УЧИТЬСЯ**

Проведите шифрование методом простой перестановки, используя ключ для подстановки **623415**

Задание 2.

Открытый текст: **ПРИ ПИСЬМЕ СВЕТ ДОЛЖЕН ПАДАТЬ СЛЕВА**

Найдите закрытый текст, используя метод Цезаря

Задание 3.

Открытый текст **СИСТЕМА_ПОТРЕБУЕТ_ОТВЕТА**

Используя табличный способ кодирования и таблицу 4х6 (4 столбца, 6 строк) с траекторией заполнения сверху вниз. Способ получения закрытого сообщения - по спирали (по часовой стрелке) от левого верхнего угла.

Задание 4.

С помощью таблицы Вижинера и ключевого слова **МАСТЕР** закодируйте фразу: **ПОЧЕМУ ЛЮДИ НЕ ЛЕТАЮТ КАК ПТИЦЫ**

Задание 5.

Закрытое сообщение: **4+1(0)4+6:·2+3(·2)31**

Ключ: 24513

Найдите открытое сообщение. Решите пример

Вариант 9

Задание 1.

Открытый текст: **ЛЕТО_ПРОШЛО_НАДО_УЧИТЬСЯ**

Проведите шифрование методом простой перестановки, используя ключ для подстановки **364215**

Задание 2.

Открытый текст: **СЕГОДНЯ К НАМ ПРИДУТ МОИ ДРУЗЬЯ**

Найдите закрытый текст, используя метод Цезаря

Задание 3.

Открытый текст **СИСТЕМА_ПОТРЕБУЕТ_ОТВЕТА**

Используя табличный способ кодирования и таблицу 6х4 (6 столбцов, 4 строки) с траекторией заполнения сверху вниз. Способ получения закрытого сообщения - по спирали (против часовой стрелки) от левого верхнего угла.

Задание 4.
С помощью таблицы Вижинера и ключевого слова **МУЗЫКА** закодируйте фразу: **ПОЧЕМУ ЛЮДИ НЕ ЛЕТАЮТ КАК ПТИЦЫ**

Задание 5.
Закрытое сообщение: **-1(54:01)0·+961)3(8+**
Ключ: 52143
Найдите открытое сообщение. Решите пример

Вариант 10

Задание 1.
Открытый текст: **СЕГОДНЯ_ПРИДУТ_МОИ_ДРУЗЬЯ**
Проведите шифрование методом простой перестановки, используя ключ для подстановки **34215**

Задание 2.
Открытый текст: **КОЛОКОЛЬНЫЙ ЗВОН ПОЛЕЗЕН ДЛЯ ЗДОРОВЬЯ**
Найдите закрытый текст, используя метод Цезаря

Задание 3.
Открытый текст **СИСТЕМА_ПОТРЕБУЕТ_ОТВЕТА**
Используя табличный способ кодирования и таблицу 6х4 (6 столбцов, 4 строки) с траекторией заполнения снизу вверх. Способ получения закрытого сообщения – змейкой, начиная с правого нижнего угла.

Задание 4.
С помощью таблицы Вижинера и ключевого слова **САЛЬЕРИ** закодируйте фразу: **ПОЧЕМУ ЛЮДИ НЕ ЛЕТАЮТ КАК ПТИЦЫ**

Задание 5.
Закрытое сообщение: **42·3(+5:)57(9-85·9:)**
Ключ: 51243
Найдите открытое сообщение. Решите пример

Вариант 11

Задание 1.
Открытый текст: **СЕГОДНЯ_ПРИДУТ_МОИ_ДРУЗЬЯ**
Проведите шифрование методом простой перестановки, используя ключ для подстановки **25143**

Задание 2.
Открытый текст: **КТО ХОРОШО ЕСТ ТОТ ХОРОШО РАБОТАЕТ**
Найдите закрытый текст, используя метод Цезаря

Задание 3.

Открытый текст **КОЛОКОЛЬНЫЙ_ЗВОН_ПОЛЕЗЕН**
Используя табличный способ кодирования и таблицу 6х4 (6 столбцов, 4 строки) с траекторией заполнения снизу вверх. Способ получения закрытого сообщения – змейкой, начиная с правого верхнего угла

Задание 4.
С помощью таблицы Вижинера и ключевого слова **МОЦАРТ** закодируйте фразу: **ПОЧЕМУ ЛЮДИ НЕ ЛЕТАЮТ КАК ПТИЦЫ**

Задание 5.
Закрытое сообщение: **99·7-·+7·664-4·+614:**
Ключ: 13254
Найдите открытое сообщение. Решите пример

Вариант 12

Задание 1.
Открытый текст: **СЕГОДНЯ_ПРИДУТ_МОИ_ДРУЗЬЯ**
Проведите шифрование методом простой перестановки, используя ключ для подстановки **35142**

Задание 2.
Открытый текст: **БЕЗ ТРУДА НЕ ВЫНУТЬ И РЫБКУ ИЗ ПРУДА**
Найдите закрытый текст, используя метод Цезаря

Задание 3.
Открытый текст **КОЛОКОЛЬНЫЙ_ЗВОН_ПОЛЕЗЕН**
Используя табличный способ кодирования и таблицу 6х4 (6 столбцов, 4 строки) с траекторией заполнения сверху вниз. Способ получения закрытого сообщения – по спирали, против часовой стрелки, начиная от правого верхнего угла

Задание 4.
С помощью таблицы Вижинера и ключевого слова **МАСТЕР** закодируйте фразу: **ХОЧУ ПЯТЕРКУ ПО ПРАКТИЧЕСКОЙ**

Задание 5.
Закрытое сообщение: **(104+6+:)43+(·23)1·2**
Ключ: 15324
Найдите открытое сообщение. Решите пример

Вариант 13

Задание 1.
Открытый текст: **ДЕТЯМ_ПОЛЕЗЕН_МОРСКОЙ_ВОЗДУХ**

Проведите шифрование методом простой перестановки, используя ключ для подстановки **3267145**

Задание 2.
Открытый текст: **САМЫЙ ДЛИННЫЙ ДЕНЬ В ГОДУ ЛЕТОМ**
Найдите закрытый текст, используя метод Цезаря

Задание 3.
Открытый текст **КОЛОКОЛЬНЫЙ_ЗВОН_ПОЛЕЗЕН**
Используя табличный способ кодирования и таблицу 6х4 (6 столбцов, 4 строки) с траекторией заполнения по спирали. Способ получения закрытого сообщения- по спирали, по часовой стрелке, начиная от правого нижнего угла.

Задание 4.
С помощью таблицы Вижинера и ключевого слова **МУЗЫКА** закодируйте фразу: **ХОЧУ ПЯТЕРКУ ПО ПРАКТИЧЕСКОЙ**

Задание 5.
Закрытое сообщение: **4(51-01)0:196+·+(83)**
Ключ: 31425
Найдите открытое сообщение. Решите пример

Вариант 14

Задание 1.
Открытый текст: **ДЕТЯМ_ПОЛЕЗЕН_МОРСКОЙ_ВОЗДУХ**
Проведите шифрование методом простой перестановки, используя ключ для подстановки **3742365**

Задание 2.
Открытый текст: **САМАЯ КОРОТКАЯ НОЧЬ В ГОДУ ЛЕТОМ**
Найдите закрытый текст, используя метод Цезаря

Задание 3.
Открытый текст **КОЛОКОЛЬНЫЙ_ЗВОН_ПОЛЕЗЕН**
Используя табличный способ кодирования и таблицу 4х6 (4 столбца, 6 строк) с траекторией заполнения по спирали. Способ получения закрытого сообщения- снизу вверх, начиная от правого нижнего угла.

Задание 4.
С помощью таблицы Вижинера и ключевого слова **САЛЬЕРИ** закодируйте фразу: **ХОЧУ ПЯТЕРКУ ПО ПРАКТИЧЕСКОЙ**

Задание 5.
Закрытое сообщение: **2(43·15+):(87-9·)5:9**
Ключ: 13542
Найдите открытое сообщение. Решите пример

Вариант 15

Задание 1.

Открытый текст: **ДЕТЯМ_ПОЛЕЗЕН_МОРСКОЙ_ВОЗДУХ**

Проведите шифрование методом простой перестановки, используя ключ для подстановки **5241673**

Задание 2.

Открытый текст: **САМЫЙ КОРОТКИЙ ДЕНЬ В ГОДУ ЗИМОЙ**

Найдите закрытый текст, используя метод Цезаря

Задание 3.

Открытый текст **КОЛОКОЛЬНЫЙ_ЗВОН_ПОЛЕЗЕН**

Используя табличный способ кодирования и таблицу 4х6 (4 столбца, 6 строк) с траекторией заполнения сверху сниз. Способ получения закрытого сообщения - против часовой стрелки, начиная от правого нижнего угла

Задание 4.

С помощью таблицы Вижинера и ключевого слова **МОЦАРТ** закодируйте фразу: **ХОЧУ ПЯТЕРКУ ПО ПРАКТИЧЕСКОЙ**

Задание 5.

Закрытое сообщение: **·4(32:+5)5978-(95):·**

Ключ: 25341

Найдите открытое сообщение. Решите пример

ЛИТЕРАТУРА:

1. Шеннон К. Э. Работы по теории информации и кибернетике, М.: ИЛ, 1963. 832 с.

2. А.В. Аграновский, Р.А. Хади. Практическая криптография (серия «Аспекты защиты»), М.: Солон-Пресс, 2002. 254 с.

3. Т.Л. Партыка, И.И. Попов. Информационная безопасность. М.: Форум-Инфра, 2007. 368 с.

4. С.В. Глушаков А.С. Сурядный. Программирование на Visual Basic 6. Х.: Фалио, 2004. 497с.

5. Брюс Шнайер. Прикладная криптография, 2е изд, изд.Триумф,2002. 816 с.

6. У. Диффи и М.Э. Хеллман. Новые направления в криптографии,1976 . 654 с.

7. http://profbeckman.narod.ru/

8. https://studfiles.net/preview/2774511/page:2/

9. http://www.intuit.ru/studies/courses/691/547/lecture/12373?page=5