Часть I. Основы криптографии

Раздел 1.1. Введение в криптографическую защиту информации

1.1.1. Открытые сообщения и их характеристики

- Для обмена информацией современные люди используют речь и письменность.
- Информация, передаваемая между людьми, представляет собой сообщения.
- В основе речи и письменности лежит алфавит, с помощью которого человек отображает сообщение.
- Различают естественные алфавиты (например, русский, английский)
- и специальные (например, цифровые, буквенно-цифровые).

- Будем понимать под сообщением, с одной стороны, логически законченную порцию информации (или текст), имеющую идею, смысл и пригодную для общения людей, а с другой стороны, совокупность знаков, отображающих определенным образом сообщение.

- Криптография имеет дело с сообщениями, отображаемыми с помощью письменных средств общения какого-либо языка с определенной системой графики и орфографии. Сообщения, с содержанием которых может ознакомиться и понять их смысл любой человек, называются открытыми.
- С точки зрения криптографии под открытыми сообщениями понимают сообщения (или текст) подлежащие зашифрованию.

- Открытые сообщения имеют определенные характеристики. Сообщения состоят из букв алфавита. Например, есть русский алфавит, английский алфавит и т.д. Обозначают алфавит следующим образом. Например, русский алфавит строчных букв будет иметь следующее обозначение А={а, б, в, …, э, ю, я}.

- Количество знаков в алфавите называется мощностью алфавита. Так мощность английского алфавита 26 знаков, русского - 33 знака. Обозначают мощность алфавита следующим образом: для русского алфавита мощность A|=33. В криптографии в состав алфавита могут входить кроме букв другие знаки: цифры, знаки препинания, специальные знаки и т.п.

- В настоящее время наиболее часто используют следующие алфавиты:
- 1) бинарный, представляющий собой множество Z2={0,1};
- 2) шестнадцатеричный, представляющий собой множество
- Z16={0,1,…,A,D,C,D,E,F};
- 3) латинский алфавит, представляющий собой множество
- Z26={A,B,C,D,…,X,Y,Z};
- 4) усеченное множество букв кириллицы – Z32= {А,Б,В,…};
- 5) символы, входящие в стандартные коды ASCII- множество Z256.

- В общем случае, если не оговорено иное, будем полагать, что алфавитом сообщений, подлежащих зашифрованию, является множество $Z_m=\{0,1,\ldots,m-1\}$, а величину m будем называть мощностью или модулем алфавита исходных текстов.
- Открытое сообщение характеризуется длиной. Длина сообщения – есть количество знаков алфавита, входящих в сообщение.

- При анализе открытого текста выделяют его характер. С точки зрения содержания различают обычные литературные тексты, формализованные данные межмашинного обмена и т. д. Выделяют сообщения по определенной структуре тематики. Тематическое сообщение характеризуется вероятностными словами: «Сообщаю Вам», «Здравствуйте», «С уважением» и т.п.

- Открытое сообщение характеризуется частотой встречаемости знаков в тексте и элементов сообщения (слов, сочетаний слов и т.п.). Статистика частот встречаемости знаков в тексте и элементов сообщения показывает их неравномерное распределение. В частности, для достаточно большого объема литературного текста на русском языке наиболее часто встречающимися буквами оказываются {о,и}, среди наиболее часто встречающихся букв английского языка – символы {e,t}. В таблице 1.1 приведены частоты встречаемости букв русского алфавита.

- Помимо отдельных знаков сообщения можно характеризовать частотой встречаемости букво- сочетаний из двух или более знаков. Буквосочетание из двух знаков называется биграммой, из трех знаков – триграммой и т.д. Последовательность k знаков называют k-граммой. Анализируя частоту встречаемости знаков или их сочетаний в криптограммах можно получить для них открытое сообщение. Этот метод, используемый для дешифрования сообщения, называется методом частотного анализа.

- Таблица 1.1 - Частоты встречаемости букв русского алфавита
- Буква Частота Буква Частота Буква Частота Буква Частота
- пробел 0,145 р 0,041 я 0,019 х 0,009
- о 0,095 в 0,039 ы 0,016 ж 0,008
- е 0,074 л 0,036 з 0,015 ю 0,007
- а 0,064 к 0,029 ъ, ь 0,015 ш 0,006
- и 0,064 м 0,026 б 0,015 ц 0,004
- т 0,056 д 0,026 г 0,014 щ 0,003
- н 0,056 п 0,024 ч 0,013 э 0,003
- с 0,047 у 0,021 й 0,010 ф 0,002

- Язык, на котором реализовано сообщение, обладает избыточностью
- [1]. Смысл избыточности языка состоит в том, что не каждое сочетание
- букв образует слово. Одни буквы и буквенные сочетания употребляются
- очень часто, другие гораздо реже; третьи вообще не употребляются. Все
- это накладывает на язык множество запретов и тем самым создается «из-
- быточность» языка, используемая криптоаналитиками для взлома шифров.
- Лингвисты определили величину избыточности в самых разных языках
- мира. И везде она колеблется в пределах 70-80 % [2]. То есть в любом тек-
- сте 2/3 букв определяется не субъективной волей автора, а жесткими

- Каждое сообщение характеризуется источником сообщений. Различают следующие виды источников открытых сообщений [3]:
- 1. Детерминированные источники открытых сообщений;
- 2. Источник передачи данных;
- 3. Вероятностные источники открытых сообщений.

- Детерминированный источник открытых сообщений (детерминиро-
- ванная модель источника открытых сообщений) порождает открытые со-
- общения в виде последовательности символов некоторого алфавита, не со-
- держащей запрещенные сочетания символов, в соответствии с правилами
- грамматики реализуемого языка. В ряде криптографических задач данная
- модель источника сообщений используется для различения открытых тек-
- стов от случайных последовательностей с помощью вычислительной тех-
- ники.

- Источник передачи данных. Как рассматривается в [3] появление систем телеобработки привело к появлению нового вида связи, так называемого «передача данных». Целью передачи данных является передача информации для обработки ее вычислительным машинам или же выдача ее этими машинами. Принципиальная новизна вида связи — передачи данных состоит в том, что эта связь осуществляет обмен информацией между компьютерами, а также между компьютерами и человеком.

- Данные, предназначенные для машин, называют «формализованным языком», языком машин. Эти данные передаются в цифровом виде (часто в виде двоичной последовательности). Осмысливание их человеком может происходить только после их представления в соответствующей форме. В криптографи ческих терминах понятия формализованного языка представляют собой словарные величины, а их условные формы — кодобозначения, последние изображаются в виде буквенных, цифровых и смешанных групп различной длины (разрядности).

- Формализованный документ оформляется в виде так

называемого «формата», т.е. формы, в которой размещение данных осуществляется по некоторым жестким правилам на местах, определяемых для данного формата шаблоном. Для чтения таких документов необходимо знать формальный язык и форматы документов. Для формализованных сообщений исчезает понятие открытого текста в общепринятом его понимании «читаемого» текста.

- Признаками «открытого текста» текста формализованного являются не его читаемость, а различные его детерминированные и статистические признаки, связанные с применяемыми способами сжатия и кодирования в системах дискретного фототелеграфа, телевидения, телекоммуникационных сетей.

- Простейшие вероятностные источники сообщений в [3] рассматриваются как источники случайных последовательностей. Считается, что источник генерирует конечную или бесконечную последовательность случайных символов x0, x1, ..., xn-1 из алфавита I. Вероятность случайного сообщения (0, 1,..., n-1) определяется как вероятность совместного события

- При этом, естественно, требуют выполнения условий:
- 1) для любого случайного сообщения (0, 1,..., n-1)
- ( )
- 2) ∑ P(0, 1,…, n-1)=1;
- (0, 1, …, n-1)
- 3) для любого случайного сообщения (0, 1,..., n-1)
- ( ) ∑ ( )

- Смысл последнего условия состоит в том, что вероятность всякого
- случайного сообщения длины n есть сумма вероятностей всех «продолже-
- ний» этого сообщения до длины s. Текст, порождаемый таким источником,
- является вероятностным аналогом языка. Он обладает одинаковыми с язы-
- ком частотными характеристиками k-грамм. Задавая конкретное вероят-
- ностное распределение на множестве открытых текстов, мы задаем соот-
- ветствующую модель источника сообщений. Рассмотрим часто используе-
- мые вероятностные модели источников открытых сообщений.

- Среди простейших вероятностных источников сообщений выделяют:
- стационарные источники независимых символов алфавита, в которых предполагается, что вероятности сообщений полностью определяются вероятностями отдельных символов алфавита, межзнаковые зависимости в тексте игнорируются. Под открытым текстом понимается реализация последовательности независимых испытаний в полиномиальной вероятностной схеме с числом исходов равным т. Исходу взаимно однозначно соответствует символ алфавита I. Эта модель позволяет разделить буквы алфавита на классы высокой, средней и низкой частот использования;

- стационарный источник независимых биграмм. Эта модель точнее предыдущей модели отражает свойства языка. Под открытым текстом такого источника понимается реализация последовательности независимых испытаний в полиномиальной вероятностной схеме с числом исходов не более m^2. Множество результатов взаимно однозначно соответствует множеству всех разрешенных биграмм алфавита;

- - модель независимых биграмм классифицирует все биграммы источника сообщений по вероятности их появления в тексте. Согласно этой модели всякое сообщение, у которого на четном месте располагается первая буква запретной биграммы, имеет нулевую вероятность. В то же время моделью игнорируются запретные биграммы, у которых первая буква располагается на нечетном месте, а также игнорируются свойственные языкам зависимости между соседними биграммами;

- - стационарный источник марковски зависимых букв. Открытый текст такого источника является реализацией последовательности испытаний, связанных простой однородной цепью Маркова с m состояниями. Эта модель учитывает все запретные биграммы (вероятность сообщения, содержащего запретную биграмму, равна нулю), но запретные s-граммы при $s > 2$ учитывает не все.

- Рассмотренные стационарные модели можно уточнять и тем самым усложнить в направлении увеличения глубины зависимости вероятности очередной буквы текста от значений нескольких предыдущих букв.
- Нестационарные источники открытых сообщений учитывают структуру сообщения, вероятности появления s-грамм в тексте зависят от их места в сообщении. Например, если источником сообщения является премьер-министр, а адресатом – король, то с большой вероятностью сообщение начнется со слов «Ваше Величество! …», а завершится соответствующей подписью. Подобные стандарты играют важную роль в криптографическом анализе. В частности, удачно выбранная криптоаналитиком нестационарная модель источника открытых сообщений может в некоторых случаях упростить задачу дешифрования по шифрованному тексту, сведя ее к задаче дешифрования по открытому и шифрованному тексту.

- Выбор подходящей модели для исследования источника открытых сообщений носит, как правило, компромиссный характер и осуществляется в зависимости от свойств конкретного шифра.

1.1.2. k-граммная модель открытого текста

- Для анализа текста, объединяя входящие в него буквы по определенным правилам, можно получать из двух букв – биграммы, из трех букв триграммы и т.д., т.е. некоторые устойчивые словоформы реального человеческого языка (например, слоги, слова, сочетания слов). В общем виде, когда не указывается конкретное количество объединяемых букв, говорят о k-грамме.

- При исследовании математическими методами свойств шифров используют упрощенную модель открытого текста. В качестве такой модели выступает k-граммная модель открытого текста. Основанием для использования такой модели открытого текста [4] является устойчивость k-грамм в человеческом языке, а также теоретико-информационный подход, развитый в работах К. Шеннона.

- Учет частот k-грамм приводит к следующей модели открытого текста
- [1]. Пусть ( )( ) представляет собой массив, состоящий из приближений
- для вероятностей ( ) появления -грамм в открытом
- тексте, , N–множество натуральных чисел, – алфавит
- открытого текста, , $\bar{}$.

- Тогда источник «открытого текста» генерирует последовательность
- ( ) знаков алфавита , в которой -грамма появ-
- ляется с вероятностью ( ) ( )( ), следующая -грамма
- ( ) появляется с вероятностью ( ) ( )( ), и т. д.
- Назовем построенную модель открытого текста вероятностной моделью -
- го приближения.

- Таким образом, простейшая модель открытого текста – вероятностная модель первого приближения – представляет собой последовательность знаков в которой каждый знак появляется с вероятностью ( ) ( )( ), независимо от других знаков. Будем называть также эту модель позначной моделью открытого текста. В такой модели открытый текст имеет вероятность

- В вероятностной модели второго приближения первый знак имеет
- вероятность ( ) ( )( ), а каждый следующий знак зависит от
- предыдущего и появляется с вероятностью

- где ( ) ( )( ), ( ) ( )( ) Другими словами, мо-
- дель открытого текста второго приближения представляет собой простую
- однородную цепь Маркова. В такой модели открытый текст имеет
- вероятность

- 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.

- Необходимость использования математических моделей открытого текста вызвана, 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.

1.1.3. Критерии распознавания открытого текста

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

- Итак, согласно изложенному выше, открытый текст представляет собой реализацию независимых испытаний случайной величины, значениями которой являются буквы алфавита, появляющиеся в соответствии с
- Требуется определить, является ли случайная последовательность букв алфавита открытым текстом или нет. распределением вероятностей

- Пусть – гипотеза, состоящая в том, что данная последовательность – открытый текст, – альтернативная гипотеза. В простейшем случае последовательность можно рассматривать при гипотезе H1 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 последовательность представляет собой реализацию независимых испытаний некоторой случайной величины, значениями которой являются буквы алфавита , появляющиеся в соответствии с распределением вероятностей

- 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 рода, ее вероятность равна . Аналогично вводится ошибка второго рода и ее вероятность . 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, -граммы подряд идущих букв, будем называть критериями запретных -грамм [4]. Они устроены чрезвычайно просто. Отбирается некоторое число редких - грамм, которые объявляются запретными. Теперь, просматривая последовательно -грамму за - граммой анализируемой последовательности , мы объявляем ее случайной, как только в ней встретится одна из запретных - 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 -грамм являются весьма эффективными.

1.1.4. Основные задачи криптографии

- Криптография возникла как наука о методах шифрования, и долгое время именно шифрование (т.е. защита передаваемых или хранимых данных от несанкционированного чтения) оставалась единственной проблемой, изучаемой криптографией. Однако в последнее время, в связи с бурным развитием информационных технологий, возникло множество новых применений, на прямую не связанных с сокрытием секретной информации.

- Необходимость применения криптографических методов вытекает из условий, в которых происходит хранение и обмен информацией. В современных информационных системах очень часто происходит обмен данными в коллективах, члены которых не доверяют друг другу. В таких ситуациях необходимы средства, гарантирующие, что в процессе обмена или хранения информация не будет подвергнута искажениям, или не будет подменена целиком. Такую гарантию может дать только применение научно обоснованных криптографических методов.

- В связи с этим основными задачами криптографии являются:
- обеспечение конфиденциальности данных (предотвращение не санкционированного доступа к данным). Это одна из основных задач криптографии, для ее решения применяется шифрование данных, т.е. такое их преобразование, при котором прочитать их могут только законные пользователи, обладающие соответствующим ключом;

- обеспечение целостности данных— гарантии того, что при передаче или хранении данные не были модифицированы пользователем, не имеющим на это права. Под модификацией понимается вставка, удалениеили подмена информации, а также повторная пересылка перехваченногоранее текста;

- обеспечение аутентификации. Под аутентификацией понимается проверка подлинности субъектов (сторон при обмене данными, автора документов, и т.д.) или подлинности самой информации. Частным случаем аутентификации является идентификация — процедура доказательства субъектом того, что он действительно является именно тем, за кого себя выдает. Во многих случаях субъект X должен не просто доказать свои права, но сделать это так, чтобы проверяющий субъект (Y) не смог впоследствии сам использовать полученную информацию для того, чтобы выдать себя за X. Подобные доказательства называются «доказательствами с нулевым разглашением»;

• обеспечение невозможности отказа от авторства предотвращение

возможности отказа субъектов от совершенных ими действий (обычно -

невозможности отказа от подписи под документом). Эта задача неотделима от другой — обеспечение невозможности приписывания авторства.

Наиболее яркий пример ситуации, в которой стоит такая задача - подписание договора двумя или большим количеством лиц, не доверяющих друг

другу. В такой ситуации все подписывающие стороны должны быть уверены в том, что в будущем, во-первых, ни один из подписавших не сможет

отказаться от своей подписи и, во-вторых, никто не сможет модифицировать, подменить или создать новый документ (договор) и утверждать, что

именно этот документ был подписан

- Основным способом решения рассмотренных задач криптографии является использование электронной подписи.

Помимо перечисленных основных задач можно назвать также электронное голосование, жеребьевку, разделение секрета (распределение секретной информации между несколькими субъектами таким образом, чтобы воспользоваться ей они могли только все вместе) и многое другое [3].

1.1.5. Симметричное и асимметричное шифрование

- Будем понимать под шифрованием такое преобразование текста (сообщения), в результате которого прочитать преобразованный текст может только тот, кто обладает специальным ключом.
- Процесс шифрования (или зашифрования) включает в себя следующие элементы:
- - исходный или открытый текст (сообщение). Обозначим его буквой M;
- - шифрованный текст (сообщение). Обозначим его буквой C;
- - алгоритм шифрования - это способ преобразования открытого текста в шифрованный текст. В данном случае будет использоваться криптографический алгоритм преобразования, т.е. алгоритм зависящий от некоторого параметра, называемого ключом, и удовлетворяющий определенным требованиям. Обозначим его буквой E (начальная буква английского слова Encryption - шифрование);

- - ключ-это важнейший компонент шифрования, определяющий выбор конкретного шифрующего преобразования. Обычно ключ представляет собой буквенную или цифровую последовательность. Процесс зашифрования можно выразить следующей формулой
- C=Ek1(M).
- Преобразование шифрованного текста в открытый текст на основе законно полученного ключа называется расшифрованием (в отличие от дешифрования, которое означает восстановление открытого текста без знания ключа). Обозначим его буквой k.

- Расшифрование включает в себя компоненты, аналогичные рассмотренным выше: шифрованный текст, открытый текст, ключ. Кроме тогорасшифрование включает в себя алгоритм расшифрования. О буквой D. Тогда процесс расшифрования можно выразить следующей формулой:
- M=Dk2(C)
- Алгоритмы зашифрования и расшифрования должны удовлетворять следующему равенству:
- M=Dk2(Ek1(M)).

- Ключи k1 и k2 могут иметь одинаковое значение, а в общем случае могут быть разными для алгоритмов расшифрования и зашифрования.
- В соответствии со значениями ключей зашифрования и расшифрования в современной криптографии различают симметричное и ассиметричное шифрование.

- Симметричное шифрование, как для зашифрования так и для расшифрования, использует либо одинаковые ключи, либо ключи, у которых знание одного из них позволяет легко найти другой.

- Ассиметричное шифрование осуществляется с помощью двух разных ключей, связанных математически между собой и называемых криптопарой. Один из ключей называется открытым или публичным, другой секретным или закрытым. При этом, информация, зашифрованная на открытом ключе, может быть расшифрована только с помощью закрытого ключа, и наоборот, то, что зашифровано закрытым, можно расшифровать только с помощью открытого ключа.

- Закрытый ключ владелец хранит в надёжном месте, и никто, кроме него этот ключ не знает, а копию открытого ключа раздаётся всем желающим. Таким образом, если кто-то захочет обменяться зашифрованными сообщениями с владельцем закрытого ключа, то он зашифровывает сообщение на открытом ключе, который доступен всем желающим, а расшифровать это сообщение можно будет только с помощью закрытого ключа. Как видно, асимметричность проявляется в назначении и использовании ключей зашифрования и расшифрования. Иногда асимметричное шифрование называют шифрованием с открытым ключом.

1.1.6. Классификация шифров

- Классифицировать шифры можно по различным признакам. Например, по области применения различают шифры ограниченного и общего использования, по стойкости различают совершенные, практически стойкие и нестойкие шифры. Наиболее часто применяют классификацию по особенностям используемых в шифрах преобразований (или алгоритмов шифров). Классификация на основе особенностей алгоритмов шифрования приведена на рисунке 1.1. Выделим особенности алгоритмов, приведенных в данной классификации шифров. Одноключевыми или симметричными шифрами называются шифры, в которых для зашифрования и расшифрования используется одинаковый (один и тот же) ключ.

- Двухключевыми или асимметричными шифрами называются шифры, в которых для зашифрования и расшифрования используются разные ключи. Один из ключей является открытым, а другой – секретным.

- Квантовые шифры основаны на квантовомеханическом принципе неопределенности. Процесс отправки и приёма информации выполняется посредством объектов квантовой механики (например, при помощи электронов в электрическом токе или фотонов в линиях волоконно-оптической связи). Самым ценным свойством этого вида шифрования является то, что при посылке сообщения отправляющая и принимающая сторона с достаточно большой вероятностью могут установить факт перехвата противником зашифрованного сообщения.

- Детерминированные шифры - это шифры, в которых каждому тексту открытого сообщения ставится в соответствие ровно один шифрованный текст, т.е. при шифровании одного и того же сообщения одним и тем же ключом всегда будет получаться один и тот же шифротекст.

Рисунок 1.1 – Схема классификации шифров

- В вероятностных шифрах в процедуре шифрования используется дополнительная случайная величина (число) - в результате при шифровании одного и того же исходного сообщения одним и тем же ключом могут получиться разные шифротексты, которые при расшифровке дадут один и тот же результат (исходное сообщение).

- Композиционные шифры построены путем комбинирования относительно простых криптографических преобразований. Например, перестановки и гаммирования, гаммирования и гаммирования, перестановки и замены и т.п. Идея такого подхода заключается в том, что композиция шифров, не являющихся совершенными, может дать шифр, «близкий» к совершенному шифру.

- Шифры замены (подстановки) представляют собой шифры, в которых позиции букв в криптограмме остаются теми же, что и у открытого текста, но символы открытого текста заменяются символами другого алфавита. В шифрах перестановки все буквы алфавита открытого текста остаются в криптограмме, но меняют свои позиции в соответствии с определенными правилами.

- Из шифров перестановки наибольшее распространение получили

маршрутные перестановки, основанные на использовании геометрических фигур. Открытый текст записывается в такую фигуру по некоторой траектории. Шифрованный текст получается путем считывания текста по другой траектории. При использовании столбцовых (строчных) перестановок открытый текст вписывается в таблицу по одному маршруту, а шифрованный текст получают путем считывания символов по другому. Например, открытый текст вписывается в таблицу по столбцам в их естественном порядке, а шифрованный текст получают путем считывания столбцов в порядке, определяемым ключом.

- При шифровании открытого текста с помощью решетки, представляющей собой трафарет с отверстиями, в них вписывают либо буквы, либо слоги, либо слова открытого текста. Затем решетку убирают, свободное место заполняют боле менее осмысленным текстом.

- В аддитивных шифрах буквы алфавита заменяются числами, к которым затем добавляются числа секретной случайной (псевдослучайной) числовой последовательности (гаммы), после чего берется остаток от деления по модулю (операция mod). Если исходное сообщение и гамма представляются в битовом виде, то при зашифровании и расшифровании применяется логическая операция «Исключающее ИЛИ» (XOR, сложение по модулю 2).

- По размеру обрабатываемого (шифруемого) блока различают блочные и поточные (посимвольные) шифры.
- При однозначной замене символ открытого текста заменяется одним символом алфавита шифрованного текста.
- При многозначной замене символ открытого текста может быть заменен одним из нескольких символов алфавита шифрованного текста.
- Для одноалфовитных шифров в процессе шифрования используетсяодин алфавит шифрованного текста.
- Для многоалфавитных шифров в процессе шифрования используетсянесколько одноалфавитных шифров.

- Кроме приведенной шкалы шифры могут быть классифицированы по различным другим критериям, касающимся в основном способов реализации шифраторов, например:
- по виду обрабатываемого сигнала – дискретные и аналоговые;
- по типу засекречиваемых сообщений – для засекречивания телеграфных, речевых, факсимильных сообщений или передачи данных
- по типу связи межу процессом шифрования и расшифрования –
- линейного и предварительного шифрования;
- по виду синхронизации между процессом шифрования и расшифрования- автономные, с каналом синхронизации и полуавтономные.

1.1.7. Модели шифров

- Первая математическая модель шифра была предложена К. Шенноном.
- В настоящее время различают две модели шифров [1]: алгебраическую и ве-
- роятностную. Рассмотрим вначале алгебраическую модель шифра. Пусть X,
- K, Y конечные множества возможных открытых текстов, ключей и шифро-
- ванных текстов соответственно. Обозначим через E множество правил за-
- шифрования. Ek – правило зашифрования на ключе k□K. Обозначим через D
- множество правил расшифрования. Dk – правило расшифрования на ключе
- k□K. Если k представляется в виде k=(kз,kр), где kз – ключ зашифрования, а

- y = Ekз (x),
- а расшифрование - формулой
- x = Dkp (y)
- где x□X, y□Y, (kз,kp)□K.
- Моделью шифра или шифрсистемой [1] назовем совокупность
- ∑A= (X, K, Y, E, D)
- введенных множеств, для которых выполняются следующие свойства:
- 1. Для любых x□X, k□K выполняется равенство
- x = Dk (Ek (x)).
- 2.
- ∪( )

- Другими словами модель шифра можно определить как совокупность множеств открытых текстов, возможных ключей, возможных шифрованных текстов, правил зашифрования и правил расшифрования. Условие 1 означает требование однозначности расшифрования. При этом необходимо учитывать, что одному x может соответствовать несколько y. Условие 2 означает, что любой элемент y□Y может быть представлен в виде Ek(x) для соответствующих x□X и k□K. Заметим, что в общем случае утверждение «для любых k□K и y□Ek(X), выполняется равенство
- Ek(Dk (y))=y

будет неверным.

- Из условия 1 следует свойство инъективности функции Ek, т.е. если x1,
- x2 X, x1 ≠ x2 , то при любом k K выполняется неравенство Ek(x1)≠Ek(x2).
- Рассмотрим модель шифра простой замены в алфавите A.
- Пусть

- где S(A) – симметрическая группа подстановок множества A и L натуральное
- число. X и Yпредставляют собой объединения декартовых степеней множе-
- ства A. Для любого ключа k K, открытого текста x = (x1, .. xn), шифрован-
- ного текста y = (y1, ..., yn) правила зашифрования и расшифрования шифра

- Ek(x) = (k(x1), … , k(xL)),
- Dk(y) = (k
- -1
- (y1), … , k
- -1
- (yL)),
- где k
- -1
- – подстановка, обратная к k. В общем случае X и Yмогут быть разны-
- ми.

- Для шифра перестановки можно использовать следующую алгебраиче-
- скую модель. Пусть X = Y = A
- L
- , K SL, где SL - симметрическая группа под-
- становок множества{1…L}. Можно считать Lколичеством символов алфави-
- та A в шифруемом блоке. Для любого ключа k, открытого текста x = (x1, .. xL)
- и шифрованного текста y = (y1, …, yL) правила зашифрования и расшифрова-
- ния будут иметь вид:

- Ek(x) = (xk(1), .. , xk(L)),
- Dk(y) = (yk
- -1
- (1), … , yk
- -1
- (L)),
- где k-1 – подстановка, обратная к k.

- Для вероятностной модели шифра определим априорные распределе-
- ния вероятностей P(X) и P(K) на множествах X и K соответственно. Тем са-
- мым для любого x□X определена вероятность pX(x)□P(X) и для любого k□K
- – вероятность pK(k)□P(K), для которых выполняются равенства

- ∑ (
- □
-) ∑
- □
- ( )
- Тогда вероятностная модель шифра выглядит следующим образом
- ∑B= (X, K, Y, E, D, P(X), P(K)).
- Потребность в математических моделях шифров и открытого текста
- определяется в первую очередь исследованиями, проводимыми в различных
- областях криптографии.

Спасибо за внимание