Клод Шеннон. Теория связи в секретных системах.[1]

Материал, изложенный в данной статье, первоначально составлял содержание секретного доклада «Математическая теория криптографии», датированного 1 сентября 1945 г, который в настоящее время[2] рассекречен.

1. Введение и краткое содержание.

Вопросы криптографии и секретных систем открывают возможность для интересных применений теории связи. В настоящей статье развивается теория секретных систем. Изложение ведется в теоретическом плане и имеет своей целью дополнить положения, приводимые в обычных работах по криптографии. В этих работах детально изучаются многие стандартные типы кодов и шифров, а также способы их расшифровки. Мы будем иметь дело с общей математической структурой и свойствами секретных систем.

Наше изложение будет ограничено в нескольких отношениях. Во-первых, имеются три общих типа секретных систем: 1) системы маскировки, которые включают применение таких методов, как невидимые чернила, представление сообщения в форме безобидного текста или маскировки криптограммы, и другие методы, при помощи которых факт наличия сообщения скрывается от противника; 2) тайные системы (например, инвертирование речи), в которых для раскрытия сообщения требуется специальное оборудование; 3) «собственно» секретные системы, где смысл сообщения скрывается при помощи шифра, кода и т.д., но само существование сообщения не скрывается и предполагается, что противник обладает любым специальным оборудованием, необходимым для перехвата и записи переданных сигналов. Здесь будет рассмотрен только третий тип систем, так как системы маскировки представляют в основном психологическую проблему, а тайные системы – техническую проблему.

Во-вторых, наше изложение будет ограничено случаем дискретной информации, где сообщение, которое должно быть зашифровано, состоит из последовательных дискретных символов, каждый из которых выбран из некоторого конечного множества. Эти символы могут быть буквами или словами некоторого языка, амплитудными уровнями «квантованной» речи или видеосигнала и т.д., но главный акцент будет сделан на случае букв.

Статья делится на три части. Резюмируем теперь кратко основные результаты исследования. В первой части излагается основная математическая структура секретных систем. В теории связи считается, что язык может рассматриваться как некоторый вероятностный процесс, который создает дискретную последовательность символов в соответствии с некоторой системой вероятностей. С каждым языком связан некоторый параметр $\boldsymbol{D}$, который можно назвать избыточностью этого языка. Избыточность измеряет в некотором смысле, насколько может быть уменьшена длина некоторого текста в данном языке без потери какой-либо части информации. Простой пример: так как в словах английского языка за буквой q всегда следует только буква u, то u может быть без ущерба опущена. Значительные сокращения в английском языке можно осуществить, используя его статистическую структуру, частую повторяемость определенных букв или слов, и т.д. Избыточность играет центральную роль в изучении секретных систем.

Секретная система определяется абстрактно как некоторое множество отображений одного пространства (множества возможных сообщений) в другое пространство (множество

---

[1] Печатается по изданию: К. Шеннон «Работы по теории информации и кибернетике», М., ИЛ, 1963, с. 333-369 (перевод В.Ф.Писаренко) с корректировкой терминологии переводчика.

[2] 1949 год — *прим. ред.*

возможных криптограмм). Каждое конкретное отображение из этого множества соответствует способу шифрования при помощи конкретного ключа.

Предполагается, что отображения являются взаимно-однозначными, так что если известен ключ) то в результате процесса расшифрования возможен лить единственный ответ.

Предполагается далее, что каждому ключу (и, следовательно, каждому отображению) соответствует некоторая априорная вероятность – вероятность выбрать этот ключ. Аналогично каждому возможному сообщению соответствует априорная вероятность, определяемая задающим сообщение вероятностным процессом. Эти вероятности различных ключей и сообщений являются фактически априорными вероятностями для шифровальщика противника и характеризуют его априорные знания относительно интересующей его проблемы.

Чтобы использовать такую секретную систему, сначала выбирается некоторый ключ и посылается в точку приема. Выбор ключа определяет конкретное отображение из множества отображений, образующих систему. Затем выбирается сообщение и с помощью отображения, соответствующего выбранному ключу, из этого сообщения формируется криптограмма. Эта криптограмма передается в точку приема по некоторому каналу и может быть перехвачена противником. На приемном конце с помощью отображения, обратного выбранному, из криптограммы восстанавливают первоначальное сообщение.

Если противник перехватит криптограмму, он может с ее помощью сосчитать апостериорные вероятности различных возможных сообщений и ключей, которые могли быть использованы для составления такой криптограммы. Это множество апостериорных вероятностей образует его сведения о ключах и сообщениях после перехвата. «Сведения», таким образом, представляют собой некоторое множество предположений, которым приписаны вероятности. Вычисление апостериорных вероятностей является общей задачей дешифрования.

Проиллюстрируем эти понятия простым примером. В шифре простой подстановки со случайным ключом имеется 26! отображений, соответствующих 26! способам, которыми мы можем заменить 26 различных букв. Все эти способы равновозможны, и поэтому каждый имеет априорную вероятность 1/26! Если такой шифр применяется к «нормативному английскому языку» и предполагается, что шифровальщик противника не знает ничего об источнике сообщений, кроме того, что он создает английский текст, то априорными вероятностями различных сообщений из N букв являются просто их относительные частоты в нормативном английском тексте.

Если противник перехватил такую криптограмму из N букв, его апостериорные вероятности изменятся. Если N достаточно велико (скажем, 50 букв), имеется обычно единственное сообщение с апостериорной вероятностью, близкой к единице, в то время как все другие сообщения имеют суммарную вероятность, близкую к нулю. Таким образом, имеется, по существу, единственное «решение» такой криптограммы. Для меньших N (скажем, $N = 15$) обычно найдется много сообщений и ключей, вероятности которых сравнимы, и не найдется ни одного сообщения и ключа с вероятностью, близкой к единице. В этом случае «решение» криптограммы неоднозначно.

В результате рассмотрения секретных систем, которые могут быть представлены как совокупность отображений одного множества элементов в другое, возникают две естественные операции комбинирования, производящие из двух данных систем третью. Первая операция комбинирования называется операцией «умножения» (произведением) и соответствует зашифрованию сообщения с помощью системы R с последующим зашифрованием полученной криптограммы с помощью системы S, причем ключи R и S выбираются независимо. Полный результат этой операции представляет собой секретную систему, отображения которой состоят из всех произведений (в обычном смысле произведений отображений) отображений из S на отображения из R. Вероятности результирующих отображений являются произведениями вероятностей двух исходных отображений.

Вторая операция комбинирования является «взвешенным сложением»:

$$\boldsymbol{T} = p\boldsymbol{R} + q\boldsymbol{S},\ p + q = 1.$$

Она представляет собой следующее. Сначала делается предварительный выбор, какая из систем $\boldsymbol{R}$ или $\boldsymbol{S}$ будет использоваться, причем система $\boldsymbol{R}$ выбирается с вероятностью p, а система $\boldsymbol{S}$ с вероятностью q. После этого выбранная система используется описанным выше способом.

Будет показано, что секретные системы с этими двумя операциями комбинирования образуют, по существу, «линейную ассоциативную алгебру» с единицей, – алгебраический объект) подробно изучавшийся математиками.

Среди многих возможных секретных систем имеется один тип с многочисленными особыми свойствами. Этот тип назовем «чистой» системой. Система является чистой, если все ключи равновероятны и если для любых трех отображений $\boldsymbol{T}_i$, $\boldsymbol{T}_j$, $\boldsymbol{T}_k$ из множества отображений данной системы произведение

$$\boldsymbol{T}_i\boldsymbol{T}_j^{-1}\boldsymbol{T}_k$$

также является отображением из этого множества. То есть зашифрование, расшифрование и снова зашифрование с любыми тремя ключами должно быть эквивалентно одному зашифрованию с некоторым ключом.

Можно показать, что для чистого шифра все ключи по существу эквивалентны – все они приводят к тому же самому множеству апостериорных вероятностей. Больше того, каждой криптограмме соответствует некоторое множество сообщений («остаточный класс»), из которых могла бы получиться эта криптограмма, а апостериорные вероятности сообщений в этом классе пропорциональны априорным вероятностям. Вся информация, которую противник получил бы в результате перехвата криптограммы, заключается в установлении остаточного класса. Многие из обычных шифров являются чистыми системами, в том числе простая подстановка со случайным ключом. В этом случае остаточный класс состоит из всех сообщений с таким же набором буквенных повторений, как в перехваченной криптограмме.

По определению, две системы $\boldsymbol{R}$ и $\boldsymbol{S}$ являются «подобными», если существует фиксированное отображение $\boldsymbol{A}$ (имеющее обратное $\boldsymbol{A}^{-1}$) такое, что $\boldsymbol{R} = \boldsymbol{AS}$.

Если $\boldsymbol{R}$ и $\boldsymbol{S}$ подобны, то между получающимися в результате применения этих систем множествами криптограмм можно установить взаимнооднозначное соответствие, приводящее к тем же самым апостериорным вероятностям. Такие две системы аналитически записываются одинаково.

Во второй части статьи рассматривается проблема «теоретической секретности». Насколько легко некоторая система поддается раскрытию при условии, что для анализа перехваченной криптограммы противник располагает неограниченным количеством времени и специалистов? Эта проблема тесно связана с вопросами связи при наличии шумов, и понятия энтропии и неопределенности, введенные в теории связи, находят прямое применение в этом разделе криптографии.

«Совершенная секретность» определяется следующими требованиями к системе. Требуется, чтобы апостериорные вероятности различных сообщений, полученные после перехвата противником данной криптограммы, были бы в точности равны априорным вероятностям тех же сообщений до перехвата. Покажем, что «совершенная секретность» возможна, но требует в случае конечного числа сообщений того же самого числа возможных ключей. Если считать, что сообщение создается с данной «скоростью» $\boldsymbol{R}$ (понятие скорости будет определено позже), то ключ должен создаваться с той же самой или с большей скоростью.

Если используется секретная система с конечным ключом и перехвачены N букв криптограммы, то для противника будет существовать определенное множество сообщений с

определенными вероятностями, которые могли бы создать эту криптограмму. С увеличением N это множество обычно сужается до тех пор, пока в конце концов не получится единственного «решения» криптограммы: одно сообщение с вероятностью, близкой к единице, а все остальные с вероятностями, практически равными нулю. В работе определяется величина $H(N)$, названная *ненадежностью.* Эта величина измеряет (в статистическом смысле), насколько близка средняя криптограмма из N букв к единственному решению, т. е. насколько неточно известно противнику истинное сообщение после перехвата криптограммы из N букв. Далее выводятся различные свойства ненадежности, например: ненадежность ключа не возрастает с ростом N. Эта ненадежность является теоретическим показателем секретности – теоретическим, поскольку она позволяет противнику дешифрировать криптограмму лишь в том случае) если он обладает неограниченным запасом времени.

В этой же части определяется функция $H(N)$ для некоторых идеализированных типов шифров, называемых *случайными шифрами.* С некоторыми видоизменениями эта функция может быть применена ко многим случаям, представляющим практический интерес. Это дает способ приближенного вычисления количества материала, который требуется перехватить, чтобы получить решение секретной системы.

Из подобного анализа следует, что для обычных языков и обычных типов шифров (но не кодов) это «расстояние единственности» равно приблизительно $H(K)/D$. Здесь $H(K)$ – число, измеряющее «объем» пространства ключей. Если все ключи априори равновероятны, то $H(K)$ равно логарифму числа возможных ключей. Вводимое число D – это избыточность языка. Оно измеряет количество «статистических ограничений», налагаемых языком. Для простой подстановки со случайным ключом наше $H(K)$ равно $\log_{10}26!$ или приблизительно 20, а D (в десятичных единицах на букву) для английского языка равно приблизительно 0.7. Таким образом, единственность решения достигается приблизительно при 30 буквах.

Для некоторых «языков» можно построить такие секретные системы с конечным ключом, в которых неопределенность не стремится к нулю при $N \to \infty$. В этом случае противник не получит единственного решения такого шифра, сколько бы материала он не перехватил, и у него будет оставаться много альтернатив с довольно большими вероятностями. Такие системы назовем *идеальными системами.* В любом языке можно аппроксимировать такую ситуацию, т.е. отсрочить приближение $H(N)$ к нулю до сколь угодно больших N. Однако такие системы имеют много недостатков, таких как сложность и чувствительность к ошибкам при передаче криптограммы.

Третья часть статьи посвящена «практической секретности». Две системы с одинаковым объемом ключа могут быть обе разрешимы единственным образом, когда перехвачено N букв, но они могут значительно отличаться по количеству времени и усилий, затрачиваемых для получения решения. На основе анализа основных недостатков секретных систем предлагаются методы построения систем, для решения которых требуются большие затраты времени и сил. Наконец, рассматривается проблема несовместимости различных желательных качеств секретных систем.

Часть I.

МАТЕМАТИЧЕСКАЯ СТРУКТУРА СЕКРЕТНЫХ СИСТЕМ.

2. Секретные системы.

Чтобы приступить к математическому анализу криптографии, необходимо ввести удовлетворительную идеализацию и определить математически приемлемым способом, что

будет пониматься под термином секретная система. Схематическая структура секретной системы показана на рис.1.

Рис. 1. Схема общей секретной системы.

На передающем конце имеются два источника информации – источник сообщений и источник ключей. Источник ключей отбирает конкретный ключ среди всех возможных ключей данной системы. Этот ключ передается некоторым способом на приемный конец, причем предполагается, что его нельзя перехватить (например, ключ передается посыльным). Источник сообщений формирует некоторое сообщение (незашифрованное), которое затем зашифровывается, и готовая криптограмма передается на приемный конец, причем криптограмма может быть перехвачена (например, пересылается по радио). На приемном конце шифровальщик с помощью ключа по криптограмме восстанавливает исходное сообщение.

Очевидно, шифровальщик на передающем конце выполняет некоторую функциональную операцию. Если $\boldsymbol{M}$ – сообщение, $\boldsymbol{K}$ – ключ и $\boldsymbol{E}$ – зашифрованное сообщение (криптограмма), то имеем

$$\boldsymbol{E} = \boldsymbol{f}(\boldsymbol{M},\boldsymbol{K}),$$

т.е. $\boldsymbol{E}$ является функцией от $\boldsymbol{M}$ и $\boldsymbol{K}$. Удобнее, однако, понимать $\boldsymbol{E}$ не как функцию двух переменных, а как (однопараметрическое) семейство операций или отображений, и записывать его в виде:

$$\boldsymbol{E} = \boldsymbol{T_i M}.$$

Отображение $\boldsymbol{T_i}$ примененное к сообщению $\boldsymbol{M}$, дает криптограмму $\boldsymbol{E}$. Индекс $\boldsymbol{i}$ соответствует конкретному используемому ключу.

Вообще мы будем предполагать, что имеется лишь конечное число возможных ключей, каждому из которых соответствует вероятность $\boldsymbol{p_i}$. Таким образом, источник ключей является статистическим процессом, или устройством, которое выбирает одно из множества отображений $\boldsymbol{T}_1,...,\boldsymbol{T_m}$ с вероятностями $\boldsymbol{p}_1,...,\boldsymbol{p_m}$ соответственно. Будем также предполагать, что число возможных сообщений конечно и эти сообщения $\boldsymbol{M}_1,...,\boldsymbol{M_n}$ имеют априорные вероятности $\boldsymbol{q}_1,...,\boldsymbol{q_n}$. Например, возможными сообщениями могли бы быть всевозможные последовательности английских букв, включающих по $\boldsymbol{N}$ букв каждая, а соответствующими вероятностями тогда были бы относительные частоты появления таких последовательностей в нормативном английском тексте.

Должна иметься возможность восстанавливать M на приемном конце, когда известны E и K. Поэтому отображение T_i, из нашего семейства должно иметь единственное обратное отображение T_i^{-1}, так что $T_iT_i^{-1} = I$, где I – тождественное отображение. Таким образом:

$$M = T_i^{-1}E.$$

Во всяком случае, это обратное отображение T_i^{-1} должно существовать и быть единственным для каждого E, которое может быть получено из M с помощью ключа i. Приходим, таким образом, к следующему определению: секретная система есть семейство однозначно обратимых отображений T_i множества возможных сообщений во множество криптограмм, при этом отображение T_i имеет вероятность p_i. Обратно, любое множество объектов такого типа будет называться «секретной системой». Множество возможных сообщений для удобства будет называться «пространством сообщений», а множество возможных криптограмм – «пространством криптограмм».

Две секретные системы совпадают, если они образованы одним и тем же множеством отображений T_i и одинаковыми пространствами сообщений и криптограмм, причем вероятности ключей в этих системах также совпадают.

Секретную систему можно представлять себе как некоторую машину с одним или более переключающими устройствами. Последовательность букв (сообщение) поступает на вход машины, а на выходе ее получается другая последовательность. Конкретное положение переключающих устройств соответствует конкретному используемому ключу. Для выбора ключа из множества возможных ключей должны быть заданы некоторые статистические методы.

Для того чтобы нашу проблему можно было рассмотреть математически, предположим, что противнику известна используемая система. Иными словами, он знает семейство отображений T_i и вероятности выбора различных ключей. Можно было бы, во-первых, возразить, что такое предположение нереалистично, так как шифровальщик противника часто не знает, какая система использовалась или чему равны рассматриваемые вероятности. На это возражение имеется два ответа.

1. Наложенное ограничение слабее, чем кажется с первого взгляда, из-за широты нашего определения секретной системы. Предположим, что шифровальщик перехватывает сообщение и не знает, использовалась ли здесь подстановка или транспозиция, или шифр типа Виженера. Он может считать, что сообщение зашифровано с помощью системы, в которой часть ключа является указанием того, какой из трех типов имеющихся ключей был использован, а следующая часть – конкретный ключ этого типа. Указанным трем различным возможностям шифровальщик приписывает вероятности, учитывая при этом все имеющиеся у него сведения об априорных вероятностях использования шифровальщиком противника соответствующих типов шифров.

2. Наше ограничение обычно в криптографических исследованиях. Оно является пессимистичным, но безопасно, и в конечном счете реалистично, так как можно ожидать, что противник рано или поздно раскроет любую секретную систему. Поэтому даже в том случае, когда разработана совершенно новая система, так что противник не может приписать ей никаких априорных вероятностей, если только он ее уже не раскрыл, нужно иметь в виду его возможную осведомленность.

Эта ситуация аналогична ситуации, возникающей в теории игр, где предполагается, что партнер «обнаруживает» используемую стратегию игры. В обоих случаях это предположение служит для более четкого описания сведений, которыми располагает противная сторона.

Второе возможное возражение против нашего определения секретной системы состоит в том, что в нем не принимаются в расчет используемые обычно на практике вставки в сообщение посторонних нулевых знаков и использование многократных подстановок. В таких случаях для данного сообщения и ключа имеется не единственная криптограмма и

шифровальщик может выбрать по своему желанию одну из нескольких различных криптограмм. Эту ситуацию можно было бы рассмотреть, но это только внесло бы дополнительные усложнения на данном этапе рассуждений без существенного изменения каких-либо из основных выводов.

Если сообщения создаются марковским процессом, то вероятности разных сообщений определяются структурой этого марковского процесса. Однако подойдем к вопросу с более общей точки зрения и будем трактовать сообщения просто как абстрактное множество объектов, которым приписаны вероятности, причем эти объекты не обязательно состоят из последовательностей букв и не обязательно создаются марковским процессом.

Следует подчеркнуть, что далее во всех случаях секретная система означает не одно, а целое множество отображений. После того как выбран ключ, используется только одно из этих отображений и отсюда можно было бы прийти к определению секретной системы как единственного преобразования языка. Однако противник не знает, какой ключ выбран, и остальные возможные ключи столь же важны для него, как и истинный. Именно существование этих других возможных ключей и придает системе секретность. Так как мы интересуемся в первую очередь секретностью, то вынуждены предпочесть данное нами определение понятия секретной системы. Тип ситуации, когда остальные возможности так же важны, как и осуществившаяся, часто встречается в стратегических играх. Ход шахматной игры в большой степени контролируется угрозами, которые не осуществляются. Нечто подобное представляет из себя «фактическое существование» нереализованных возможностей в теории игр.

Следует отметить, что система, состоящая из единственной операции над языком, представляет собой при нашем определении вырожденный тип секретной системы. Это – система с единственным ключом, который имеет вероятность, равную единице. В такой системе нет секретности – шифровальщик противника находит сообщение, применяя к перехваченной криптограмме обратное отображение, также единственное в такой системе. В этом случае шифровальщик противника и шифровальщик получателя информации располагают одинаковой информацией. В общем же случае единственное различие их сведений состоит в том, что последнему известен конкретно использовавшийся ключ, в то время как первому известны лишь априорные вероятности различных ключей из данного множества. Процесс расшифрования для получателя информации состоит в применении к криптограмме отображения, обратного по отношению к конкретному отображению, использованному для составления криптограммы. Процесс дешифрования для противника представляет собой попытку определить сообщение (или конкретный ключ), имея в распоряжении только криптограмму и априорные вероятности различных ключей и сообщений.

Существует много трудных эпистемологических вопросов, связанных с теорией секретности, или вернее с любой теорией, связанной с реальным применением вопросов теории вероятностей (так обстоит дело, в частности, с априорными вероятностями, теоремой Байеса и т.д.). Трактуемая абстрактно теория вероятности может быть изложена на строгих логических основах с использованием современной теории меры. Однако в применениях к физическим ситуациям, особенно когда дело касается «субъективных» вероятностей и неповторимых экспериментов, возникают многочисленные вопросы, связанные с логическим обоснованием. Например, при нашем подходе к проблеме секретности допускается, что априорные вероятности различных ключей и сообщений известны шифровальщику противника, но как он может определить их эффективным способом даже при использовании всех своих сведений о данной обстановке?

Можно создать искусственные криптографические ситуации типа «урны и игральной кости», в которых априорные вероятности имеют вполне определенный смысл и идеализация, использованная здесь, является наверняка подходящей. Но в других случаях, которые можно себе представить, например, при перехвате сообщений, передаваемых между

собой марсианами, высадившимися на Землю, априорные вероятности были бы настолько неопределенными, что не имели бы никакого значения.

Наиболее часто встречающиеся на практике криптографические задачи лежат где-то между этими крайними пределами. Шифровальщик противника может иметь желание разделить возможные сообщения на категории «приемлемых», «возможных, но малоправдоподобных» и «неприемлемых», но чувствуется, что более подробное подразделение не имело бы смысла.

К счастью, на практике только очень большие ошибки в априорных вероятностях ключей и сообщений могут вызвать заметные ошибки в важных параметрах. Это происходит из-за того, что число сообщений и криптограмм ведет себя как экспоненциальная функция, а измеряется логарифмической мерой.

3. Способы изображения систем.

Секретная система, в том виде как она определена выше, может быть изображена различными способами. Один из них (удобный для целей иллюстрации) использует линейные схемы, изображенные на рис. 2 и рис. 4. Возможные сообщения представляются точками слева, а возможные криптограммы – точками справа. Если некоторый ключ, скажем, ключ 1, отображает сообщение $\boldsymbol{M}_2$ в криптограмму $\boldsymbol{E}_2$, то $\boldsymbol{M}_2$ и $\boldsymbol{E}_2$ соединяются линией, обозначенной значком 1 и т.д. Для каждого ключа из каждого сообщения должна выходить ровно одна линия. Если это же верно и для каждой криптограммы, скажем, что система является *замкнутой*.

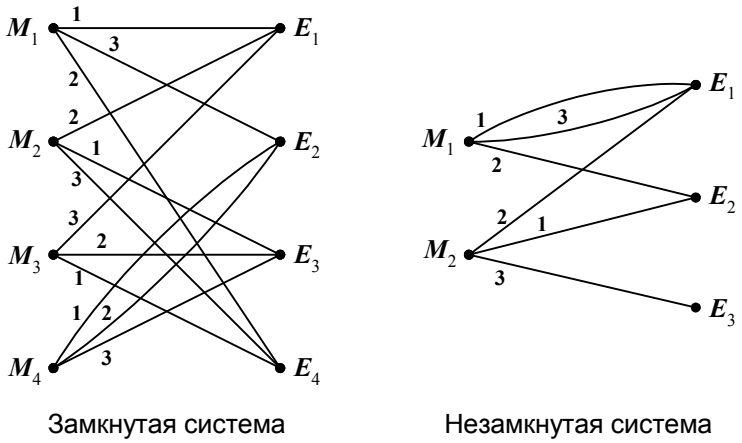


Рис.2. Схемы простых систем.

Более общий способ описания системы состоит в задании операции, с помощью которой, применяя к сообщению произвольный ключ, можно получить криптограмму. Аналогично неявным образом можно определить вероятности различных ключей или с помощью задания способа выбора ключей, или с помощью описания сведений о том, как обычно выбирает ключи противник. Вероятности сообщений определяются просто посредством изложения наших априорных сведений о языке противника, тактической обстановке (которая будет влиять на возможное содержание сообщений) и любой специальной информации, касающейся криптограммы.

4. Примеры секретных систем.

В данном разделе рассматриваются несколько примеров шифров. В дальнейшем в целях иллюстрации будем часто ссылаться на эти примеры.

Шифр простой подстановки.

В таком шифре производится замена каждой буквы сообщения на некоторый определенный символ (обычно также на букву). Таким образом, сообщение

$$\boldsymbol{M} = m_1 m_2 m_3 m_4 \ldots,$$

где $m_1, m_2, \ldots$ – последовательные буквы, переходит в

$$\boldsymbol{E} = e_1 e_2 e_3 e_4 \ldots = \boldsymbol{f}(m_1)\boldsymbol{f}(m_2)\boldsymbol{f}(m_3)\boldsymbol{f}(m_4)\ldots,$$

причем функция $\boldsymbol{f}(m)$ имеет обратную функцию. Ключ является просто перестановкой алфавита (если буквы заменяются на буквы), например,

XGUACDTBFHRSLMQVYZWIEJOKNP.

Первая буква – *X* заменяет букву *A*, *G* заменяет *B* и т.д.

Перестановка с фиксированным периодом $\boldsymbol{d}$.

В этом случае сообщение делится на группы символов длины $\boldsymbol{d}$ и к каждой группе применяется одна и та же перестановка. Эта перестановка является ключом; она может быть задана некоторой перестановкой первых $\boldsymbol{d}$ целых чисел.

Таким образом, для $\boldsymbol{d} = 5$ в качестве перестановки можно взять 23154. Это будет означать, что

$$\boldsymbol{m}_1\boldsymbol{m}_2\boldsymbol{m}_3\boldsymbol{m}_4\boldsymbol{m}_5\boldsymbol{m}_6\boldsymbol{m}_7\boldsymbol{m}_8\boldsymbol{m}_9\boldsymbol{m}_{10}\ldots$$

переходит в

$$\boldsymbol{m}_2\boldsymbol{m}_3\boldsymbol{m}_1\boldsymbol{m}_5\boldsymbol{m}_4\boldsymbol{m}_7\boldsymbol{m}_8\boldsymbol{m}_6\boldsymbol{m}_{10}\boldsymbol{m}_9\ldots$$

Последовательное применение двух или более перестановок будет называться составной перестановкой. Если периоды этих перестановок равны $\boldsymbol{d}_1,\ldots,\boldsymbol{d}_s$, то, очевидно, в результате получится перестановка периода $\boldsymbol{d}$, где $\boldsymbol{d}$ – наименьшее общее кратное $\boldsymbol{d}_1,\ldots,\boldsymbol{d}_s$.

Шифр Виженера и его варианты.

В шифре Виженера ключ задается набором из $\boldsymbol{d}$ букв. Такие наборы подписываются с повторением под сообщением и полученные две последовательности складываются по модулю 26 (каждая буква рассматриваемого алфавита нумеруется от $\boldsymbol{A} = 0$ до $\boldsymbol{Z} = 25$).

Таким образом,

$$\boldsymbol{e_i} = \boldsymbol{m_i} + \boldsymbol{k_i} \pmod{26},$$

где $\boldsymbol{k_i}$ – буква ключа, полученная сокращением числа $\boldsymbol{i}$ по модулю $\boldsymbol{d}$. Например, с помощью ключа *GAH* получаем

Сообщение	*N*	*O*	*W*	*I*	*S*	*T*	*H*	*E*
Повторяемый ключ	*G*	*A*	*H*	*G*	*A*	*H*	*G*	*A*
Криптограмма	*T*	*O*	*D*	*O*	*S*	*A*	*N*	*E*

Шифр Виженера с периодом 1 называется шифром Цезаря. Он представляет собой простую подстановку, в которой каждая буква сообщения $\boldsymbol{M}$ сдвигается вперед на фиксированное число мест по алфавиту. Это число и является ключом; оно может быть любым от 0 до 25. Так называемый шифр Бофора (Beaufort) и видоизмененный шифр Бофора подобны шифру Виженера. В них сообщения зашифровываются с помощью равенств

$$\boldsymbol{e_i} = \boldsymbol{k_i} - \boldsymbol{m_i} \pmod{26} \text{ и}$$
$$\boldsymbol{e_i} = \boldsymbol{m_i} - \boldsymbol{k_i} \pmod{26}$$

соответственно. Шифр Бофора с периодом 1 называется обратным шифром Цезаря.

Повторное применение двух или более шифров Виженера будет называться составным шифром Виженера. Он имеет уравнение

$$e_i = m_i + k_i + l_i + ... + s_i \pmod{26},$$

где $k_i, l_i, ..., s_i$ вообще говоря, имеют различные периоды. Период их суммы $k_i + l_i + ... + s_i$, как и в составной транспозиции, будет наименьшим общим кратным отдельных периодов.

Если используется шифр Виженера с неограниченным неповторяющимся ключом, то мы имеем шифр Вернама, в котором

$$e_i = m_i + k_i \pmod{26},$$

и k_i выбираются случайно и независимо среди чисел 0, 1, ... , 25. Если ключом служит текст, имеющий смысл, то имеем шифр «бегущего ключа».

Диграммная, триграммная и n-граммнол подстановки.

Вместо подстановки одной буквы можно использовать подстановку диграмм, триграмм и т.д. Для диграммной подстановки в общем виде требуется ключ, состоящий из перестановок 26^2 диграмм. Он может быть представлен с помощью таблицы, в которой ряд соответствует первой букве диграммы, а столбец – второй букве, причем клетки таблицы заполнены заменяющими символами (обычно также диграммами).

Шифр Виженера с перемешанным один раз алфавитом.

Такой шифр представляет собой простую подстановку с последующим применением шифра Виженера

$$e_i = f(m_i) + k_i,$$
$$m_i = f^{-1}(e_i - k_i).$$

«Обратным» к такому шифру является шифр Виженера с последующей простой подстановкой

$$e_i = g(m_i + k_i),$$
$$m_i = g^{-1}(e_i) - k_i.$$

Матричная система.

Имеется один метод подстановки n-грамм, который заключается в применении к последовательным n-граммам некоторой матрицы, имеющей обратную. Предполагается, что буквы занумерованы от 0 до 25 и рассматриваются как элементы некоторого алгебраического кольца. Если к n-грамме сообщения применить матрицу a_{ij} то получится n-грамма криптограммы

$$e_i = \sum_{j=1}^{n} a_{ij} m_j \,,\ i = 1,...,n.$$

Матрица a_{ij} является ключом, и расшифровка выполняется с помощью обратной матрицы. Обратная матрица будет существовать тогда и только тогда, когда определитель $|a_{ij}|$ имеет обратный элемент в нашем кольце.

Шифр Плэйфер.

Этот шифр является частным видом диграммной подстановки, которая производится с помощью перемешанного алфавита из 25 букв, записанных в виде квадрата 5×5. (Буква *J* часто опускается при криптографической работе, так как она редко встречается, и в тех случаях, когда она встречается, ее можно заменить буквой *I*). Предположим, что ключевой квадрат записывается следующим образом:

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

В этом случае диграмма *AC*, например, заменяется на пару букв, расположенных в противоположных углах прямоугольника, определяемого буквами *A* и *C*, т.е. на *LO*, причем *L* взята первой, так как она выше *A*. Если буквы диграммы расположены на одной горизонтали, то используются стоящие справа от них буквы. Таким образом, *RI* заменяется на *DF*, *RF* заменяется на *DR*. Если буквы расположены на одной вертикали, то используются буквы, стоящие под ними. Таким образом, *PS* заменяется на *UW*. Если обе буквы диграммы совпадают, то можно использовать для их разделения нуль или же одну из букв опустить и т.п.

Перемешивание алфавита с помощью многократной подстановки.

В этом шифре используются последовательно $\boldsymbol{d}$ простых подстановок. Так, если $\boldsymbol{d} = 4$, то

$$\boldsymbol{m}_1\boldsymbol{m}_2\boldsymbol{m}_3\boldsymbol{m}_4\boldsymbol{m}_5\boldsymbol{m}_6\ldots$$

заменяется на

$$\boldsymbol{f}(\boldsymbol{m}_1)\boldsymbol{f}(\boldsymbol{m}_2)\boldsymbol{f}(\boldsymbol{m}_3)\boldsymbol{f}(\boldsymbol{m}_4)\boldsymbol{f}(\boldsymbol{m}_5)\boldsymbol{f}(\boldsymbol{m}_6)\ldots$$

и т.д.

Шифр с автоключом.

Шифр типа Виженера, в котором или само сообщение или результирующая криптограмма используются в качестве «ключа», называется шифром с автоключом. Шифрование начинается с помощью «первичного ключа» (который является настоящим ключом в нашем смысле) и продолжается с помощью сообщения или криптограммы, смещенной на длину первичного ключа, как в указанном ниже примере, где первичным ключом является набор букв *COMET*. В качестве «ключа» используется сообщение:

Сообщение	*S*	*E*	*N*	*D*	*S*	*U*	*P*	*P*	*L*	*I*	*E*	*S*	...
Ключ	*C*	*O*	*M*	*E*	*T*	*S*	*E*	*N*	*D*	*S*	*U*	*P*	...
Криптограмма	*U*	*S*	*Z*	*H*	*L*	*M*	*T*	*C*	*O*	*A*	*Y*	*H*	...

Если в качестве «ключа» использовать криптограмму, то получится[3]

Сообщение	*S*	*E*	*N*	*D*	*S*	*U*	*P*	*P*	*L*	*I*	*E*	*S*	...
Ключ	*C*	*O*	*M*	*E*	*T*	*U*	*S*	*Z*	*H*	*L*	*O*	*H*	...
Криптограмма	*U*	*S*	*Z*	*H*	*L*	*O*	*H*	*O*	*S*	*T*	*T*	*S*	...

Дробные шифры.

В этих шифрах каждая буква сначала зашифровывается в две (или более) буквы или в два (или более) числа, затем полученные символы каким-либо способом перемешиваются (например, с помощью транспозиции), после чего их можно снова перевести в первоначальный алфавит. Таким образом, используя в качестве ключа перемешанный 25-буквенный алфавит, можно перевести буквы в двузначные пятеричные числа с помощью таблицы:

[3] Эта система является тривиальной с точки зрения секретности, так как за исключением первых $\boldsymbol{d}$ букв, в распоряжении противника имеется весь «ключ».

	0	1	2	3	4
0	L	Z	Q	C	P
1	A	G	N	O	U
2	R	D	M	I	F
3	K	Y	H	V	S
4	X	B	T	E	W

Например, букве B соответствует число 41_5. После того, как полученный ряд чисел подвергнут некоторой перестановке, его можно снова разбить на пары чисел и перейти к буквам.

Коды.

В кодах слова (или иногда слоги) заменяются группами букв. Иногда затем применяется шифр того или иного вида.

5. Оценка секретных систем.

Имеется несколько различных критериев, которые можно было бы использовать для оценки качества предлагаемой секретной системы. Рассмотрим наиболее важные из этих критериев.

Количество секретности.

Некоторые секретные системы являются совершенными в том смысле, что положение противника не облегчается в результате перехвата любого количества сообщений. Другие системы, хотя и дают противнику некоторую информацию при перехвате очередной криптограммы, но не допускают единственного «решения». Системы, допускающие единственное решение, очень разнообразны как по затрате времени и сил, необходимых для получения этого решения, так и по количеству материала, который необходимо перехватить для получения единственного решения.

Объем ключа.

Ключ должен быть передан из передающего пункта в приемный пункт таким способом, чтобы его нельзя было перехватить. Иногда его нужно запомнить. Поэтому желательно иметь ключ настолько малый, насколько это возможно.

Сложность операции зашифрования и расшифрования.

Операции зашифрования и расшифрования должны быть, конечно, по возможности простыми. Если эти операции производятся вручную, то их сложность приводит к потере времени, появлению ошибок и т.д. Если они производятся механически, то сложность приводит к использованию больших и дорогих устройств.

Разрастание числа ошибок.

В некоторых типах шифров ошибка в одной букве, допущенная при шифровании или передаче, приводит к большому числу ошибок в расшифрованном тексте. Такие ошибки разрастаются в результате операции расшифрования, вызывая значительную потерю информации и часто требуя повторной передачи криптограммы. Естественно, желательно минимизировать это возрастание числа ошибок.

Увеличение объема сообщения.

В некоторых типах секретных систем объем сообщения увеличивается в результате операции шифрования. Этот нежелательный эффект можно наблюдать в системах, в которых делается попытка потопить статистику сообщения в массе добавляемых нулевых символов, или где используются многократные замены. Он имеет место также во многих

системах типа «маскировки» (которые не являются обычными секретными системами в смысле нашего определения).

6. Алгебра секретных систем

Если имеются две секретные системы T и R, их часто можно комбинировать различными способами для получения новой секретной системы S. Если T и R имеют одну и ту же область (пространство сообщений), то можно образовать своего рода «взвешенную сумму»

$$S = pT + qR,$$

где $p + q = 1$. Эта операция состоит, во-первых, из предварительного выбора систем T или R с вероятностями p и q. Этот выбор является частью ключа S. После того как этот выбор сделан, системы T или R применяются в соответствии с их определениями. Полный ключ S должен указывать, какая из систем T или R выбрана и с каким ключом используется выбранная система.

Если T состоит из отображений $T_1,...,T_m$ с вероятностями $p_1,...,p_m$, а R – из $R_1,...,R_k$ с вероятностями $q_1,...,q_k$, то система $S = pT + qR$ состоит из отображений $T_1,...,T_m,R_1,...,R_k$ с вероятностями $pp_1,...,pp_m,qq_1,...,qq_k$, соответственно. Обобщая далее, можно образовать сумму нескольких систем

$$S = p_1T + p_2R + ... + p_mU, \ \sum p_i = 1.$$

Заметим, что любая система T может быть записана как сумма фиксированных операций

$$T = p_1T_1 + p_2T_2 + ... + p_mT_m,$$

где T_i – определенная операция шифрования в системе T, соответствующая выбору ключа i, причем вероятность такого выбора равна p_i.

Второй способ комбинирования двух секретных систем заключается в образовании «произведения», как показано схематически на рис. 3. Предположим, что T и R – такие две системы, что область определения (пространство языка) системы R может быть

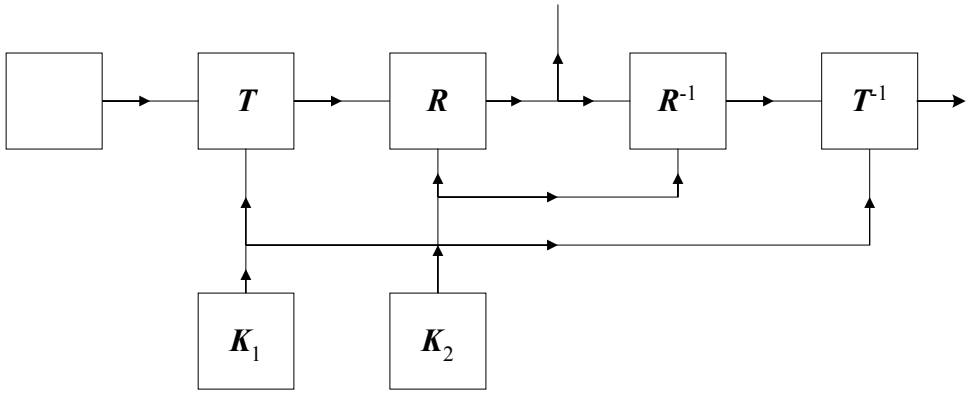


Рис 3. Произведение двух систем $S = RT$.

отождествлена с областью значения (пространством криптограмм) системы T. Тогда можно применить сначала систему T к нашему языку, а затем систему R к результату этой операции, что дает результирующую операцию S, которую запишем в виде произведения

$$S = RT.$$

Ключ системы S состоит как из ключа системы T, так и из ключа системы R, причем предполагается, что эти ключи выбираются соответственно их первоначальным вероятностям и независимо. Таким образом, если m ключей системы T выбирается с вероятностями

$$p_1, p_2, \ldots, p_m,$$

а n ключей системы R имеют вероятности

$$p'_1, p'_2, \ldots, p'_n,$$

то система S имеет самое большее mn ключей с вероятностями $p_i p'_j$. Во многих случаях некоторые из отображений $R_i T_j$ будут одинаковыми и могут быть сгруппированы вместе, а их вероятности при этом сложатся.

Произведение шифров используется часто; например, после подстановки применяют перестановку или после перестановки – код Виженера; или же применяют код к тексту и зашифровывают результат с помощью подстановки, перестановки, дробным шифром и т.д.

Можно заметить, что такое умножение, вообще говоря, некоммутативно (т.е. не всегда $RS = SR$), хотя в частных случаях (таких, как подстановка и перестановка) коммутативность имеет место. Так как наше умножение представляет собой некоторую операцию, оно по определению ассоциативно, т.е. $R(ST) = (RS)T = RST$. Кроме того, верны законы

$$p(p'T + q'R) + qS = pp'T + pq'R + qS$$

(взвешенный ассоциативный закон для сложения);

$$T(pR + qS) = pTR + qTS$$
$$(pR + qS)T = pRT + qST$$

(право- и левосторонние дистрибутивные законы), а также справедливо равенство

$$p_1 T + p_2 T + p_3 R = (p_1 + p_2)T + p_3 R.$$

Следует подчеркнуть, что эти операции комбинирования сложения и умножения применяются к секретным системам в целом. Произведение двух систем TR не следует смешивать с произведением отображений в системах $T_i R_j$, которое также часто используется в настоящей работе. Первое является секретной системой, т.е. множеством отображений с соответствующими вероятностями; второе является фиксированным отображением. Далее, в то время как сумма двух систем $pR + qT$ является системой, сумма двух отображений не определена. Системы T и R могут коммутировать, в то время как конкретные R_j и T_i не коммутируют. Например, если R – система Бофора данного периода, все ключи которой равновероятны, то, вообще говоря,

$$R_i R_j \neq R_j R_i,$$

но, конечно, произведение RR не зависит от порядка сомножителей; действительно

$$RR = V$$

является системой Виженера того же самого периода со случайным ключом. С другой стороны, если отдельные отображения T_i и R_j двух систем T и R коммутируют, то и системы коммутируют.

Системы, у которых пространства M и E можно отождествить (этот случай является очень частым, если последовательности букв преобразуются в последовательности букв), могут быть названы *эндоморфными.* Эндоморфная система T может быть возведена в степень T^n.

Секретная система T, произведение которой на саму себя равно T, т.е. такая, что

$$TT = T,$$

будет называться *идемпотентной.* Например, простая подстановка, транспозиция с периодом p, система Виженера с периодом p (все с равновероятными ключами) являются идемпотентными.

Множество всех эндоморфных секретных систем, определенных в фиксированном пространстве сообщений, образует «алгебраическую систему», т. е. некоторый вид алгебры, использующей операции сложения и умножения. Действительно, рассмотренные свойства сложения и умножения можно резюмировать следующим образом:

Множество эндоморфных шифров с одним и тем же пространством сообщений и двумя операциями комбинирования — операцией взвешенного сложения и операцией умножения — образуют линейную ассоциативную алгебру с единицей, с той лишь особенностью, что коэффициенты во взвешенном сложении должны быть неотрицательными, а их сумма должна равняться единице.

Эти операции комбинирования дают способы конструирования многих новых типов секретных систем из определенных данных систем, как это было показано в приведенных примерах. Их можно также использовать для описания ситуации, с которой сталкивается шифровальщик противника, когда он пытается расшифровать криптограмму неизвестного типа. Фактически он расшифровывает секретную систему типа

$$\boldsymbol{T} = p_1\boldsymbol{A} + p_2\boldsymbol{B} + \ldots + p_r\boldsymbol{S} + p'\boldsymbol{X}, \quad \sum p_i = 1,$$

где $\boldsymbol{A},\boldsymbol{B},\ldots,\boldsymbol{S}$ в данном случае – известные типы шифров с их априорными вероятностями p_i, а $p'\boldsymbol{X}$ соответствует возможности использования совершенно нового неизвестного шифра.

7. Чистые и смешанные шифры

Некоторые типы шифров, такие как простая подстановка, транспозиция с данным периодом, система Виженера с данным периодом, система Виженера со смешанным алфавитом и т.д. (все с равновероятными ключами), обладают некоторой однородностью по отношению к ключу. Каков бы ни был ключ, процессы зашифрования, расшифрирования адресатом и дешифрирования противником являются по существу теми же самыми. Эти системы можно противопоставить системе с шифром

$$p\boldsymbol{S} + q\boldsymbol{T},$$

где $\boldsymbol{S}$ – простая подстановка, а $\boldsymbol{T}$ – транспозиция с данным периодом. В таком случае процессы зашифрования и расшифрирования адресатом или противником полностью меняются в зависимости от того, используется подстановка или транспозиция.

Причина однородности таких систем лежит в групповом свойстве: заметим, что в приведенных выше примерах однородных шифров произведение $\boldsymbol{T}_i\boldsymbol{T}_j$ любых двух отображений из множества равно третьему отображению $\boldsymbol{T}_k$ из этого же множества. С другой стороны, $\boldsymbol{T}_i\boldsymbol{S}_j$ не равно какому-нибудь отображению для шифра

$$p\boldsymbol{S} + q\boldsymbol{T},$$

который содержит только подстановки и транспозиции, но не их произведения.

Было бы можно, таким образом, определить «чистый» шифр как шифр, в котором $\boldsymbol{T}_j$ образуют группу. Однако это было бы слишком сильным ограничением, так как тогда потребовалось бы, чтобы пространство $\boldsymbol{E}$ совпадало с пространством $\boldsymbol{M}$, т.е. чтобы система была эндоморфной. Дробная транспозиция так же однородна, как и обычная транспозиция, но она не эндоморфна. Подходящим является следующее определение: шифр $\boldsymbol{T}$ является чистым, если для каждых $\boldsymbol{T}_i$, $\boldsymbol{T}_j$, $\boldsymbol{T}_k$ имеется такое $\boldsymbol{T}_s$, что

$$\boldsymbol{T}_i\boldsymbol{T}_j^{-1}\boldsymbol{T}_k = \boldsymbol{T}_s,$$

и все ключи равновероятны. В противном случае шифр является смешанным. Шифры на рис. 2 являются смешанными, а на рис. 4 – чистыми, если только все ключи равновероятны.

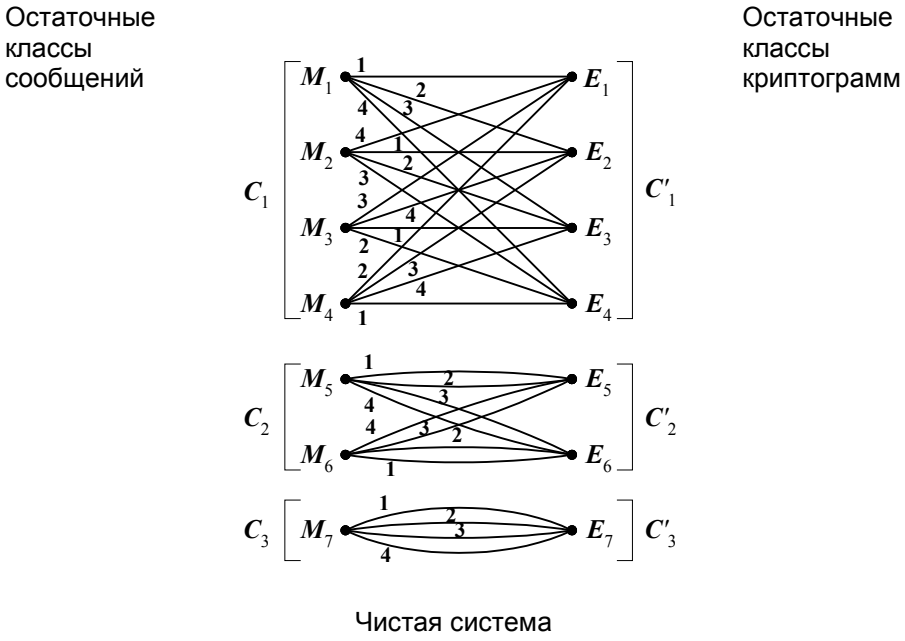


Рис 4.

Теорема 1. *В чистом шифре операции* $T_i^{-1}T_j$*, отображающие пространство сообщений в себя, образуют группу, порядок которой равен* m *– числу различных ключей.*

Так как

$$T_j^{-1}T_kT_k^{-1}T_j = I,$$

то каждый элемент имеет обратный. Ассоциативный закон верен, так как это операции, а групповое свойство следует из того, что

$$T_i^{-1}T_jT_k^{-1}T_l = T_s^{-1}T_kT_k^{-1}T_l = T_s^{-1}T_l,$$

где предполагалось, что $T_i^{-1}T_j = T_s^{-1}T_k$ для некоторого s.

Операция $T_i^{-1}T_j$ означает шифрование сообщения с помощью ключа j с последующим расшифрованием с помощью ключа i, что приводит нас назад к пространству сообщений. Если система T эндоморфна, т.е. T_i отображают пространство Ω_M в само себя (что имеет место для большинства шифров, в которых и пространство сообщений, и пространство криптограмм состоит из последовательностей букв), и если T_i образуют группу и равновероятны, то T – чистый шифр, так как

$$T_iT_j^{-1}T_k = T_iT_r = T_s.$$

Теорема 2. *Произведение двух чистых коммутирующих шифров является чистым шифром.*

Если T и R коммутируют, то $T_iR_j = R_lT_m$ для любых i,j при соответствующих l,m. Тогда

$$T_iR_j(T_kR_l)^{-1}T_mR_n = T_iR_jR_l^{-1}T_k^{-1}T_mR_n = R_uR_v^{-1}R_wT_rT_s^{-1}T_t = R_hT_g.$$

Условие коммутативности не является, однако, необходимым для того, чтобы произведение было чистым шифром.

Система, состоящая из одного ключа, т.е. из единственной определенной операции $\boldsymbol{T}_1$, является чистым шифром, т.е. при единственном возможном выборе индексов имеем

$$\boldsymbol{T}_1\boldsymbol{T}_1^{-1}\boldsymbol{T}_1 = \boldsymbol{T}_1.$$

Таким образом, разложение шифра в сумму таких простых отображений представляет собой разложение в его сумму чистых шифров.

Исследование примера, приведенного на рис. 4, вскрывает некоторые свойства чистого шифра. Сообщения распадаются на определенные подмножества, которые мы будем называть *остаточными классами,* и возможные криптограммы также распадаются на соответствующие им *остаточные классы.* От каждого сообщения в любом классе к каждой криптограмме в соответствующем классе ведет не менее одной линии и нет линий между несоответствующими классами. Число сообщений в классе является делителем полного числа ключей. Число «параллельных» линий от сообщения $\boldsymbol{M}$ к криптограмме в соответствующем классе равно числу ключей, деленному на число сообщений в классе, содержащем это сообщение (или криптограмму).

В приложении[4] показывается, что это верно для чистых шифров и в общем случае. Резюмируя сказанное, мы имеем

Теорема 3. *В чистой системе сообщения можно разделить на множество «остаточных классов» $\boldsymbol{C}_1,\ldots,\boldsymbol{C}_s$, а криптограммы – на соответствующее множество остаточных классов $\boldsymbol{C}_1',\ldots,\boldsymbol{C}_s'$. Эти классы будут иметь следующие свойства:*
1. Остаточные классы сообщений взаимно исключают друг друга и содержат все возможные сообщения. Аналогичное утверждение верно и для остаточных классов криптограмм.
2. Если зашифровать любое сообщение из класса $\boldsymbol{C}_i$ с помощью любого ключа, то получится криптограмма из класса $\boldsymbol{C}_i'$. Расшифрование любой криптограммы из класса $\boldsymbol{C}_i'$ с помощью любого ключа приводит к сообщению из класса $\boldsymbol{C}_i$.
3. Число сообщений в классе $\boldsymbol{C}_i$, скажем $\boldsymbol{\varphi}_i$, равно числу криптограмм в классе $\boldsymbol{C}_i'$ и является делителем $\boldsymbol{k}$ – числа ключей.
4. Каждое сообщение из класса $\boldsymbol{C}_i$, может быть зашифровано в каждую криптограмму из класса $\boldsymbol{C}_i'$ при помощи точно $\boldsymbol{k}/\boldsymbol{\varphi}_i$ различных ключей. То же самое верно и для расшифрирования.

Смысл понятия чистый шифр (и причина для выбора такого термина) лежит в том, что в чистом шифре все ключи являются по существу одинаковыми. Какой бы ключ ни использовался для заданного сообщения, апостериорные вероятности всех сообщений будут теми же самыми. Чтобы показать это, заметим, что два различных ключа, примененных к одному сообщению, дадут в результате две криптограммы из одного остаточного класса, скажем $\boldsymbol{C}_i'$. Поэтому эти две криптограммы могут быть расшифрованы с помощью $\boldsymbol{k}/\boldsymbol{\varphi}_i$ ключей в каждое из сообщений в классе $\boldsymbol{C}_i$, и больше ни в какие возможные сообщения. Так как все ключи равновероятны, то апостериорные вероятности различных сообщений равны

$$\boldsymbol{P}_E(\boldsymbol{M}) = \frac{\boldsymbol{P}(\boldsymbol{M})\cdot\boldsymbol{P}_{\boldsymbol{M}}(\boldsymbol{E})}{\boldsymbol{P}(\boldsymbol{E})} = \frac{\boldsymbol{P}(\boldsymbol{M})\cdot\boldsymbol{P}_{\boldsymbol{M}}(\boldsymbol{E})}{\sum\limits_{\boldsymbol{M}}\boldsymbol{P}(\boldsymbol{M})\cdot\boldsymbol{P}_{\boldsymbol{M}}(\boldsymbol{E})} = \frac{\boldsymbol{P}(\boldsymbol{M})}{\boldsymbol{P}(\boldsymbol{C}_i)},$$

где $\boldsymbol{M}$ – сообщение из класса $\boldsymbol{C}_i$, $\boldsymbol{E}$ – криптограмма из класса $\boldsymbol{C}_i'$ и сумма берется по всем $\boldsymbol{M}$ из класса $\boldsymbol{C}_i$. Если $\boldsymbol{E}$ и $\boldsymbol{M}$ не принадлежат соответствующим остаточным классам, то $\boldsymbol{P}_{\boldsymbol{E}}(\boldsymbol{M}) = 0$.

Аналогично можно показать, что набор апостериорных вероятностей различных ключей всегда одинаков, но эти вероятности ставятся в соответствие ключам лишь после

[4] Имеется в виду приложение к полному тексту работы – *примечание редакции*.

того, как уже использован некоторый ключ. При изменении частного ключа это множество чисел $\boldsymbol{P_E(M)}$ подвергается перестановке. Иными словами, имеем:

Теорема 4. *В чистой системе апостериорные вероятности различных сообщений* $\boldsymbol{P_E(M)}$ *не зависят от выбора ключа. Апостериорные вероятности ключей* $\boldsymbol{P_E(K)}$ *образуют один и тот же набор величин, но подвергаются перестановке в результате различных выборов ключа.*

Грубо говоря, можно считать, что любой выбор ключа в чистом шифре приводит к одинаковым трудностям при дешифрировании. Поскольку все различные ключи приводят к формированию криптограмм из одного и того же остаточного класса, то все криптограммы из одного остаточного класса эквивалентны с точки зрения сложности дешифрирования – они приводят к тем же самым апостериорным вероятностям сообщений и, если учитывать перестановки, к тем же самым вероятностям ключей.

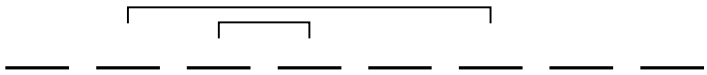
В качестве примера чистого шифра может служить простая подстановка с равновероятными ключами. Остаточный класс, соответствующий данной криптограмме $\boldsymbol{E}$, является множеством всех криптограмм, которые могут быть получены из $\boldsymbol{E}$ с помощью операций $\boldsymbol{T_j T_k^{-1} E}$. В рассматриваемом случае операция $\boldsymbol{T_j T_k^{-1}}$ сама является подстановкой и поэтому любая подстановка переводит криптограмму $\boldsymbol{E}$ в другой член того же самого остаточного класса; таким образом, если криптограмма представляет собой

$$\boldsymbol{E} = XCPPGCFQ,$$

то

$$\boldsymbol{E}_1 = RDHHGDSN,$$
$$\boldsymbol{E}_2 = ABCCDBEF \qquad \text{и т.д.,}$$

принадлежат к тому же остаточному классу. В этом случае очевидно, что криптограммы по существу эквивалентны. Все существенное в простой подстановке со случайным ключом



заключено в характере повторения букв, в то время как сами буквы являются несущественной маскировкой. В действительности можно бы полностью обойтись без них, указав характер повторений букв в $\boldsymbol{E}$ следующим образом:

Это обозначение описывает остаточный класс, но устраняет всю информацию относительно конкретных членов этого класса; таким образом, оно представляет как раз ту информацию, которая имеет значение для дешифровальщика противника. Это связано с одним из методов подхода к раскрытию шифров типа простой подстановки методом характерных слов.

В шифре типа Цезаря имеют значение только первые разности криптограммы по модулю 26. Две криптограммы с теми же самыми разностями ($\Delta \boldsymbol{e_i}$) принадлежат к одному остаточному классу. Этот шифр можно раскрыть путем простого процесса выписывания двадцати шести сообщений из этого остаточного класса и выбора того из них, которое имеет смысл.

Шифр Виженера с периодом $\boldsymbol{d}$ со случайным ключом представляет собой другой пример чистого шифра. Здесь остаточный класс сообщений состоит из всех последовательностей с теми же первыми разностями, что и у криптограммы для букв, отстоящих на расстояние $\boldsymbol{d}$. Для $\boldsymbol{d} = 3$ остаточный класс определяется с помощью равенств

$$\boldsymbol{m}_1 - \boldsymbol{m}_4 = \boldsymbol{e}_1 - \boldsymbol{e}_4$$
$$\boldsymbol{m}_2 - \boldsymbol{m}_5 = \boldsymbol{e}_2 - \boldsymbol{e}_5$$

$$\begin{array}{ccccccc} m_3 & - & m_6 & = & e_3 & - & e_6 \\ m_4 & - & m_7 & = & e_4 & - & e_7 \\ & & \dots & \dots & \dots & & \end{array}$$

где $E = e_1 e_2 \dots$ – криптограмма, а $m_1 m_2 \dots$ является любым сообщением M в соответствующем остаточном классе.

В транспозиции с периодом d со случайным ключом остаточный класс состоит из всех способов расстановок символов криптограммы, в которых никакое e_i не выдвигается из своего блока длины d и любые два e_i с расстоянием d остаются на таком же расстоянии. Это используется для раскрытия шифра следующим образом: криптограмма записывается в виде последовательных блоков длины d один под другим, как показано ниже (для $d = 5$)

$$\begin{array}{ccccc} e_1 & e_2 & e_3 & e_4 & e_5 \\ e_6 & e_7 & e_8 & e_9 & e_{10} \\ e_{11} & e_{12} & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \end{array}$$

Затем столбцы переставляются до тех пор, пока не получится осмысленный текст. После того, как криптограмма разбита на столбцы, оставшейся существенной информацией является только остаточный класс криптограммы.

Теорема 5. *Если шифр T – чистый, то $T_i T_j^{-1} T = T$, где T_i, T_j – любые два отображения из T. Обратно, если это выполняется для любых принадлежащих шифру T_i, T_j, то шифр T является чистым.*

Первая часть этой теоремы следует, очевидно, из определения чистого шифра. Чтобы доказать вторую часть, заметим сначала, что если $T_i T_j^{-1} T = T$ то $T_i T_j^{-1} T_s$ является отображением из T. Остается показать, что все ключи равновероятны. Имеем $T = \sum_s p_s T_s$ и

$$\sum_s p_s T_i T_j^{-1} T_s = \sum_s p_s T_s .$$

Слагаемое в стоящей слева сумме с $s = j$ дает $p_j T_i$. Единственным слагаемым с T_i, в правой части является $p_i T_i$. Так как все коэффициенты неотрицательны, то отсюда следует, что

$$p_j \le p_i .$$

То же самое рассуждение остается справедливым, если i и j поменять местами. Следовательно,

$$p_j = p_i$$

и T – чистый шифр. Таким образом, условие $T_i T_j^{-1} T = T$ можно было бы использовать в качестве другого определения чистого шифра.

8. Подобные системы.

Две секретные системы R и S будем называть подобными, если существует отображение A, имеющее обратное A^{-1}, такое, что

$$R = AS .$$

Это означает, что шифрование с помощью R даст то же, что шифрование с помощью S с последующим применением отображения A. Если использовать запись $R \approx S$ для обозначения того, что R подобно S, то, очевидно, из $R \approx S$ следует $S \approx R$. Кроме того, из $R \approx S$ и $S \approx T$ следует, что $R \approx T$ и, наконец, $R \approx R$. Резюмируя вышеизложенное, можно сказать, что подобие систем является соотношением эквивалентности.

Криптографический смысл подобия состоит в том, что если $\boldsymbol{R} \approx \boldsymbol{S}$, то $\boldsymbol{R}$ и $\boldsymbol{S}$ эквивалентны с точки зрения дешифрирования. Действительно, если шифровальщик противника перехватывает криптограмму из системы $\boldsymbol{S}$, он может перевести ее в криптограмму из системы $\boldsymbol{R}$ простым применением к ней отображения $\boldsymbol{A}$. Обратно, криптограмма из системы $\boldsymbol{R}$ переводится в криптограмму из системы $\boldsymbol{S}$ с помощью $\boldsymbol{A}^{-1}$. Если $\boldsymbol{R}$ и $\boldsymbol{S}$ применяются к одному и тому же пространству сообщений или языку, то имеется взаимно однозначное соответствие между получающимися криптограммами. Соответствующие друг другу криптограммы дают одинаковое апостериорное распределение вероятностей для всех сообщений.

Если имеется некоторый способ раскрытия системы $\boldsymbol{R}$, то любая система $\boldsymbol{S}$, подобная $\boldsymbol{R}$, может быть раскрыта после приведения ее к $\boldsymbol{R}$ с помощью операции $\boldsymbol{A}$. Этот способ часто используется на практике.

В качестве тривиального примера рассмотрим простую подстановку, в которой буквы сообщения заменяются не буквами, а произвольными символами. Она подобна обычной простой подстановке с заменой на буквы. Вторым примером могут служить шифр Цезаря и обратный шифр Цезаря. Последний иногда раскрывают, переводя его сначала в шифр Цезаря. Это можно сделать, обратив алфавит в криптограмме. Шифры Виженера, Бофора и вариант Бофора все подобны, если ключ является случайным. Шифр с «автоключом» (т. е. сообщением, используемым в качестве «ключа») с используемыми вначале ключами $\boldsymbol{K}_1\boldsymbol{K}_2\ldots\boldsymbol{K}_d$ подобен шифру Виженера с ключом, поочередно складываемым и вычитаемым по модулю 26. Отображение $\boldsymbol{A}$ в этом случае представляет собой «дешифровку» автоключа с помощью последовательности из $\boldsymbol{d}$ таких отображений для каждого из начальных ключей.

Часть II.

ТЕОРЕТИЧЕСКАЯ СЕКРЕТНОСТЬ.

9. Введение.

Рассмотрим вопросы, связанные с «теоретической секретностью» систем. Насколько устойчива некоторая система, если шифровальщик противника не ограничен временем и обладает всеми необходимыми средствами для анализа криптограмм? Имеет ли криптограмма единственное решение (даже если для нахождения этого решения может потребоваться такой объем работ, что его практически нельзя будет выполнить), а если нет, то сколько она имеет приемлемых решений? Какой объем текста, зашифрованного в данной системе, нужно перехватить для того, чтобы решение стало единственным? Существуют ли секретные системы, в которых вообще нельзя найти единственного решения независимо от того, каков объем перехваченного зашифрованного текста? Существуют ли секретные системы, в которых противник не получает никакой информации, сколько бы он ни перехватывал зашифрованного текста? В анализе этих вопросов найдут широкое применение понятия энтропии, избыточности, а также и другие понятия, введенные в работе «Математическая теория связи»[5].

[5] К. Шеннон «Работы по теории информации и кибернетике», М., ИЛ, 1963, с. 243-332.

10. Совершенная секретность

Предположим, что имеется конечное число возможных сообщений $M_1,\ldots,M_n$ с априорными вероятностями $P(M_1),\ldots,P(M_n)$ и что эти сообщения преобразуются в возможные криптограммы $E_1,\ldots,E_m$, так что

$$E = T_i M.$$

После того как шифровальщик противника перехватил некоторую криптограмму E, он может вычислить, по крайней мере в принципе, апостериорные вероятности различных сообщений $P_E(M)$. Естественно определить *совершенную секретность* с помощью следующего условия: для всех E апостериорные вероятности равны априорным вероятностям независимо от величины этих последних. В этом случае перехват сообщения не дает шифровальщику противника никакой информации[6]. Теперь он не может корректировать никакие свои действия в зависимости от информации, содержащейся в криптограмме, так как все вероятности, относящиеся к содержанию криптограммы, не изменяются. С другой стороны, если это условие равенства вероятностей не выполнено, то имеются такие случаи, в которых для определенного ключа и определенных выборов сообщений апостериорные вероятности противника отличаются от априорных. А это в свою очередь может повлиять на выбор противником своих действий и, таким образом, совершенной секретности не получится. Следовательно, приведенное определение неизбежным образом следует из нашего интуитивного представления о совершенной секретности.

Необходимое и достаточное условие для того, чтобы система была совершенно секретной, можно записать в следующем виде. По теореме Байеса

$$P_E(M) = \frac{P(M)\cdot P_M(E)}{P(E)},$$

где

$P(M)$ – априорная вероятность сообщения M;

$P_M(E)$ – условная вероятность криптограммы E при условии, что выбрано сообщение M, т.е. сумма вероятностей всех тех ключей, которые переводят сообщение M в криптограмму E;

$P(E)$ – вероятность получения криптограммы E;

$P_E(M)$ – апостериорная вероятность сообщения M при условии, что перехвачена криптограмма E.

Для совершенной секретности системы величины $P_E(M)$ и $P(M)$ должны быть равны для всех E и M. Следовательно, должно быть выполнено одно из равенств: или $P(M) = 0$ [это решение должно быть отброшено, так как требуется, чтобы равенство осуществлялось при любых значениях $P(M)$], или же

$$P_M(E) = P(E)$$

для любых M и E. Наоборот, если $P_M(E) = P(E)$, то

$$P_E(M) = P(M),$$

и система совершенно секретна. Таким образом, можно сформулировать следующее:

Теорема 6. *Необходимое и достаточное условие для совершенной секретности состоит в том, что*

$$P_M(E) = P(E)$$

---

[6] Пурист мог бы возразить, что противник получил некоторую информацию, а именно он знает, что послано какое-то сообщение. На это можно ответить следующим образом. Пусть среди сообщений имеется «чистый бланк», соответствующий «отсутствию сообщения». Если не создается никакого сообщения, то чистый бланк зашифровывается и посылается в качестве криптограммы. Тогда устраняется даже эта крупинка информации.

для всех M *и* E, *т.е.* $P_M(E)$ *не должно зависеть от* M.

Другими словами, полная вероятность всех ключей, переводящих сообщение M_i в данную криптограмму E, равна полной вероятности всех ключей, переводящих сообщение M_j в ту же самую криптограмму E для всех M_i, M_j и E.

Далее, должно существовать по крайней мере столько же криптограмм E, сколько и сообщений M, так как для фиксированного i отображение T_i дает взаимно-однозначное соответствие между всеми M и некоторыми из E. Для совершенно секретных систем для каждого из этих E и любого M $P_M(E) = P(E) \neq 0$. Следовательно, найдется по крайней мере один ключ, отображающий данное M в любое из E. Но все ключи, отображающие фиксированное M в различные E, должны быть различными, и *поэтому число различных ключей не меньше числа сообщений* M. Как показывает следующий пример, можно получить совершенную секретность, когда число сообщений точно равно числу ключей. Пусть M_i занумерованы числами от 1 до n, так же как и E_i, и пусть используются n ключей. Тогда

$$T_i M_j = E_s,$$

где $s = i + j \pmod{n}$. В этом случае оказывается справедливым равенство $P_E(M) = 1/n = P(E)$ и система является совершенно секретной. Один пример такой системы показан на рис. 5, где

$$s = i + j - 1 \pmod 5.$$

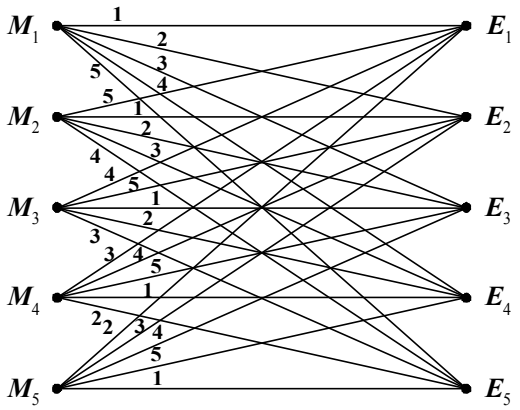


Рис 5. Совершенная система.

Совершенно секретные системы, в которых число криптограмм равно числу сообщений, а также числу ключей, характеризуются следующими двумя свойствами: 1) каждое M связывается с каждым E только одной линией; 2) все ключи равновероятны. Таким образом, матричное представление такой системы является «латинским квадратом».

В «Математической теории связи» показано, что количественно информацию удобно измерять с помощью энтропии. Если имеется некоторая совокупность возможностей с вероятностями $p_1,\ldots,p_n$, то энтропия дается выражением

$$H = -\sum p_i \log p_i .$$

Секретная система включает в себя два статистических выбора: выбор сообщения и выбор ключа. Можно измерять количество информации, создаваемой при выборе сообщения, через $H(M)$

$$H(M) = -\sum P(M) \log P(M),$$

где суммирование выполняется по всем возможным сообщениям. Аналогично, неопределенность, связанная с выбором ключа, дается выражением

$$H(K) = -\sum P(K) \log P(K) .$$

В совершенно секретных системах описанного выше типа количество информации в сообщении равно самое большее $\log n$ (эта величина достигается для равновероятных сообщений). Эта информация может быть скрыта полностью лишь тогда, когда неопределенность ключа не меньше $\log n$. Это является первым примером общего принципа, который будет часто встречаться ниже: существует предел, которого нельзя превзойти при заданной неопределенности ключа – количество неопределенности, которое может быть введено в решение, не может быть больше, чем неопределенность ключа.

Положение несколько усложняется, если число сообщений бесконечно. Предположим, например, что сообщения порождаются соответствующим марковским процессом в виде бесконечной последовательности букв. Ясно, что никакой конечный ключ не даст совершенной секретности. Предположим тогда, что источник ключа порождает ключ аналогичным образом, т.е. как бесконечную последовательность символов.

Предположим далее, что для шифрования и дешифрирования сообщения длины L_M требуется только определенная длина ключа L_K. Пусть логарифм числа букв в алфавите сообщений будет R_M, а такой же логарифм для ключа – R_K. Тогда из рассуждений для конечного случая, очевидно, следует, что для совершенной секретности требуется, чтобы выполнялось неравенство

$$R_M L_M \le R_K L_K.$$

Такой вид совершенной секретности реализован в системе Вернама.

Эти выводы делаются в предположении, что априорные вероятности сообщений неизвестны или произвольны. В этом случае ключ, требуемый для того, чтобы имела место совершенная секретность, зависит от полного числа возможных сообщений.

Можно было бы ожидать, что если в пространстве сообщений имеются фиксированные известные статистические связи, так что имеется определенная скорость создания сообщений R в смысле, принятом в «Математической теории связи», то необходимый объем ключа можно было бы снизить в среднем в R/R_M раз, и это действительно верно. В самом деле, сообщение можно пропустить через преобразователь, который устраняет избыточность и уменьшает среднюю длину сообщения как раз во столько раз. Затем к результату можно применить шифр Вернама. Очевидно, что объем ключа, используемого на букву сообщения, статистически уменьшается на множитель R/R_M, и в этом случае источник ключа и источник сообщений в точности согласован – один бит ключа полностью скрывает один бит информации сообщения. С помощью методов, использованных в «Математической теории связи», легко также показать, что это лучшее, чего можно достигнуть.

Совершенно секретные системы могут применяться и на практике, их можно использовать или в том случае, когда полной секретности придается чрезвычайно большое значение, например, для кодирования документов высших военных инстанций управления, или же в случаях, где число возможных сообщений мало. Так, беря крайний пример, когда имеются в виду только два сообщения – «да» или «нет», – можно, конечно, использовать совершенно секретную систему со следующей таблицей отображений:

M	K	A	B
да		0	1
нет		1	0

Недостатком совершенно секретных систем для случая корреспонденции большого объема является, конечно, то, что требуется посылать эквивалентный объем ключа. В следующих разделах будет рассмотрен вопрос о том, чего можно достигнуть при помощи меньших объемов ключа, в частности, с помощью конечного ключа.

11. Ненадежность.

Предположим теперь, что для английского текста используется шифр простой подстановки и что перехвачено определенное число, скажем N, букв зашифрованного текста. Если N достаточно велико, скажем более 50, то почти всегда существует единственное решение шифра, т.е. единственная последовательность, имеющая смысл на английском языке, в которую переводится перехваченный материал с помощью простой подстановки. Для меньших N шансы на неединственность решения увеличиваются; для $N = 15$, вообще говоря, будет существовать некоторое число подходящих отрывков осмысленного английского текста, в то время как для $N = 8$ окажется подходящей значительная часть (порядка 1/8) всех возможных значащих английских последовательностей такой длины, так как из восьми букв редко повторится больше чем одна. При $N = 1$, очевидно, возможна любая буква и апостериорная вероятность любой буквы будет равна ее априорной вероятности. Для одной буквы система является совершенно секретной.

Это происходит, вообще говоря, со всеми разрешимыми шифрами. Прежде чем перехвачена криптограмма, можно представить себе априорные вероятности, связанные с различными возможными сообщениями, а также с различными ключами. После того как материал перехвачен, шифровальщик противника вычисляет их апостериорные вероятности. При увеличении числа N вероятности некоторых сообщений возрастают, но для большинства сообщений они убывают до тех пор, пока не останется только одно сообщение, имеющее вероятность, близкую к единице, в то время как полная вероятность всех других близка к нулю.

Для самых простых систем эти вычисления можно эффективно выполнить. Таблица 1 дает апостериорные вероятности для шифра Цезаря, примененного к английскому тексту, причем ключ выбирался случайно из 26 возможных ключей. Для того, чтобы можно было использовать обычные таблицы частот букв, диграмм и триграмм, текст был начат в случайном месте (на страницу открытой наугад книги был случайно опущен карандаш). Сообщение, выбранное таким способом, начинается с «creases to» (карандаш опущен на третью букву слова increases). Если известно, что сообщение начинается не с середины, а с начала некоторого предложения, то нужно пользоваться иной таблицей, соответствующей частотам букв, диграмм и триграмм, стоящих в начале предложения.

Таблица 1. *Апостериорные вероятности для криптограммы типа. Цезаря.*

Расшифровки	$N = 1$	$N = 2$	$N = 3$	$N = 4$	$N = 5$
CREAS	0,028	0,0377	0,1111	0,3673	1
DSFBT	0,038	0,0314			
ETGCU	0,131	0,0881			
FUNDV	0,029	0,0189			
GVIEW	0,020				
HWJFX	0,053	0,0063			
IXKGY	0,063	0,0126			
JYLHZ	0,001				
KZMIA	0,004				
LANJB	0,034	0,1321	0,2500		
MBOKC	0,025		0,0222		
NCPLD	0,071	0,1195			
ODQME	0,080	0,0377			
PERNF	0,020	0,0818	0,4389	0,6327	
QFSOG	0,001				
RGTPH	0,068	0,0126			
SHUQI	0,061	0,0881	0,0056		
TIVRJ	0,105	0,2830	0,1667		

Расшифровки	$N = 1$	$N = 2$	$N = 3$	$N = 4$	$N = 5$
UJWSK	0,025				
VKXTL	0,009				
WLYUM	0,015		0,0056		
XMZVN	0,002				
YNAWO	0,020				
ZOBXP	0,001				
APCYQ	0,082	0,0503			
BQDZR	0,014				
H (десятичных единиц)	1,2425	0,9686	0,6034	0,285	0

Шифр Цезаря со случайным ключом является чистым, и выбор частного ключа не влияет на апостериорные вероятности. Чтобы определить эти вероятности, надо просто выписать возможные расшифровки с помощью всех ключей и вычислить их априорные вероятности. Апостериорные вероятности получатся из этих последних в результате деления их на их сумму. Эти возможные расшифровки, образующие остаточный класс этого сообщения, найдены с помощью стандартного процесса последовательного «пробегания алфавита», в таблице 1 они даны слева. Для одной перехваченной буквы апостериорные вероятности равны априорным вероятностям для всех букв[7] (они приведены в таблице под рубрикой $N = 1$).

Для двух перехваченных букв эти вероятности равны априорным вероятностям диграмм, пронормированным на их сумму (они приведены в столбце $N = 2$). Триграммные частоты получены аналогично и приведены в столбце $N = 3$. Для четырех- и пятибуквенных последовательностей вероятности находились из триграммных частот с помощью умножения, так как с некоторым приближением

$$p(ijkl) = p(ijk)p_{jk}(l).$$

Заметим, что для трех букв число возможных сообщений снижается до четырех сообщений достаточно высокой вероятности, причем вероятности всех других сообщений малы по сравнению с вероятностями этих четырех сообщений. Для четырех букв имеются два возможных сообщения и для пяти – только одно, а именно правильная дешифровка.

В принципе это может быть проведено для любой системы, однако в том случае, когда объем ключа не очень мал, число возможных сообщений настолько велико, что вычисления становятся практически невыполнимыми.

Получаемое таким образом множество апостериорных вероятностей описывает, как постепенно, по мере получения зашифрованного материала, становятся более точными сведения шифровальщика противника относительно сообщения и ключа.

Это описание, однако, является слишком исчерпывающим и слишком сложным для наших целей. Хотелось бы иметь упрощенное описание такого приближения к единственности возможного решения.

Аналогичная ситуация возникает в теории связи, когда передаваемый сигнал искажается шумом. Здесь необходимо ввести подходящую меру неопределенности того, что действительно было передано, при условии, что известен только искаженный шумом вариант – принятый сигнал.

В «Математической теории связи» показано, что естественной математической мерой этой неопределенности является условная энтропия передаваемого сигнала при условии, что принятый сигнал известен. Эта условная энтропия для удобства будет называться ненадежностью.

---

[7] Вероятности в приводимой таблице были взяты из таблиц частот, данных в книге Pratt F., Secret and Urgent, Blue Ribbon Books, New York, 1939. Хотя эти таблицы и не являются полными, но для настоящих целей их достаточно.

С криптографической точки зрения секретная система почти тождественна системе связи при наличии шума. На сообщение (передаваемый сигнал) действует некоторый статистический элемент (секретная система с ее статистически выбранным ключом). В результате получается криптограмма (аналог искаженного сигнала), подлежащая дешифрованию. Основное различие заключается в следующем: во-первых, в том, что преобразование при помощи шифра имеет обычно более сложную природу, чем возникающее за счет шума в канале; и, во-вторых, ключ в секретной системе обычно выбирается из конечного множества, в то время как шум в канале чаще является непрерывным, выбранным по существу из бесконечного множества.

Учитывая эти соображения, естественно использовать ненадежность в качестве теоретической меры секретности. Следует отметить, что имеются две основные ненадежности: ненадежность ключа и ненадежность сообщения. Они будут обозначаться через $\boldsymbol{H_E(K)}$ и $\boldsymbol{H_E(M)}$ соответственно. Их величины определяются соотношениями

$$\boldsymbol{H_E(K)} = -\sum_{\boldsymbol{E,K}} \boldsymbol{P(E,K)} \log \boldsymbol{P_E(K)},$$

$$\boldsymbol{H_E(M)} = -\sum_{\boldsymbol{E,M}} \boldsymbol{P(E,M)} \log \boldsymbol{P_E(M)},$$

где $\boldsymbol{E}$, $\boldsymbol{M}$ и $\boldsymbol{K}$ – криптограмма, сообщение и ключ;

$\boldsymbol{P(E,K)}$ – вероятность ключа $\boldsymbol{K}$ и криптограммы $\boldsymbol{E}$;

$\boldsymbol{P_E(K)}$ – апостериорная вероятность ключа $\boldsymbol{K}$, если перехвачена криптограмма $\boldsymbol{E}$;

$\boldsymbol{P(E,M)}$ и $\boldsymbol{P_E(M)}$ – аналогичные вероятности, но не для ключа, а для сообщения.

Суммирование в $\boldsymbol{H_E(K)}$ проводится по всем возможным криптограммам определенной длины (скажем, $\boldsymbol{N}$) и по всем возможным ключам. Для $\boldsymbol{H_E(M)}$ суммирование проводится по всем сообщениям и криптограммам длины $\boldsymbol{N}$. Таким образом, $\boldsymbol{H_E(K)}$ и $\boldsymbol{H_E(M)}$ являются функциями от $\boldsymbol{N}$ – числа перехваченных букв. Это будет иногда указываться в обозначении так: $\boldsymbol{H_E(K,N)}$, $\boldsymbol{H_E(M,N)}$. Заметим, что эти ненадежности являются «полными», т.е. не делятся на $\boldsymbol{N}$ с тем, чтобы получить скорость ненадежности, которая рассматривалась в работе «Математическая теория связи».

Те же самые рассуждения, которые были использованы в «Математической теории связи» для обоснования введения ненадежности в качестве меры неопределенности в теории связи, применимы и здесь. Так, из того, что ненадежность равна нулю, следует, что одно сообщение (или ключ) имеет единичную вероятность, а все другие – нулевую. Этот случай соответствует полной осведомленности шифровальщика. Постепенное убывание ненадежности с ростом $\boldsymbol{N}$ соответствует увеличению сведений об исходном ключе или сообщении. Кривые ненадежности сообщения и ключа, нанесенные на график как функции от $\boldsymbol{N}$, мы будем называть характеристиками ненадежности рассматриваемой секретной системы.

Величины $\boldsymbol{H_E(K,N)}$ и $\boldsymbol{H_E(M,N)}$ для криптограммы шифра Цезаря, рассмотренной выше, сосчитаны и приведены в нижней строке табл. 1. Числа $\boldsymbol{H_E(K,N)}$ и $\boldsymbol{H_E(M,N)}$ в этом случае равны и даны в десятичных единицах (т.е. при вычислениях в качестве основания логарифма бралось 10). Следует отметить, что ненадежность здесь сосчитана для частной криптограммы, так как суммирование ведется только по $\boldsymbol{M}$ (или $\boldsymbol{K}$), но не по $\boldsymbol{E}$. В общем случае суммирование должно было бы проводиться по всем перехваченным криптограммам длины $\boldsymbol{N}$, в результате чего получилась бы средняя неопределенность. Вычислительные трудности не позволяют сделать это практически.

12. Свойства ненадежности.

Можно показать, что ненадежность обладает некоторыми интересными свойствами, большинство из которых соответствует нашему интуитивному представлению о поведении

величины такого рода. Покажем сначала, что ненадежность ключа или фиксированной части сообщения уменьшается при увеличении количества перехваченного зашифрованного текста.

Теорема 7. *Ненадежность ключа* $H_E(K,N)$ *— невозрастающая функция* N[8]. *Ненадежность первых* A *букв сообщения является невозрастающей функцией* N. *Если перехвачено* N *букв, то ненадежность первых* N *букв сообщения меньше или равна ненадежности ключа. Это можно записать следующим образом:*

$$H_E(K,S) \le H_E(K,S), \quad S \ge N,$$
$$H_E(M,S) \le H_E(M,N),$$
$$H_E(M,N) \le H_E(K,N).$$

Введенное во втором утверждении ограничение A буквами означает, что ненадежность вычисляется по отношению к первым буквам сообщения, а не ко всему объему перехваченного сообщения. Если отказаться от этого ограничения, то можно получить возрастание ненадежности сообщения (и обычно это имеет место) с увеличением времени просто из-за того, что большее количество букв допускает и большее разнообразие возможных сообщений. Выводы этой теоремы соответствуют тому, на что можно было бы надеяться при разумной мере секретности, так как едва ли можно оказаться в худшем положении при увеличении объема перехваченного текста. Тот факт, что эти выводы могут быть доказаны, дает лучшее подтверждение полезности принятой нами количественной меры ненадежности.

Справедливость утверждений этой теоремы вытекает из некоторых свойств условной энтропии, доказанных в работе «Математическая теория связи». Так, для доказательства первого или второго утверждения теоремы воспользуемся тем, что для любых случайных событий A и B

$$H(B) \ge H_A(B).$$

Если отождествить B с ключом (при условии, что известны первые S букв криптограммы), а A с остающимися $N-S$ буквами, то мы получим первое утверждение. Аналогично, если отождествить B с сообщением, то получится второе утверждение. Последнее утверждение следует из неравенства

$$H_E(M) \le H_E(K,M) = H_E(K) + H_{E,K}(M)$$

и из того, что $H_{E,K}(M) = 0$, так как K и E полностью определяют M.

Так как сообщение и ключ выбираются независимо, то

$$H(M,K) = H(M) + H(K).$$

Кроме того,

$$H(M,K) = H(E,K) = H(E) + H_E(K),$$

что вытекает из того факта, что знание M и K или E и K эквивалентно знанию всех трех величин M, K и E. Преобразуя эти две формулы, мы получаем формулу для ненадежности ключа:

$$H_E(K) = H(M) + H(K) - H(E),$$

В частности, если $H(M) = H(E)$ то ненадежность ключа $H_E(K)$ равна априорной неопределенности ключа $H(K)$. Это имеет место в совершенно секретных системах, описанных выше.

Формула для ненадежности сообщения может быть получена аналогичным способом. Мы имеем:

---

[8] Здесь предполагается, что ключ фиксирован и не зависит от длины криптограммы N и длины сообщения A. — *Прим. ред.*

$$H(M,E) = H(E) + H_E(M) = H(M) + H_M(E),$$
$$H_E(M) = H(M) + H_M(E) - H(E).$$

Если имеется произведение секретных систем $S = TR$, то следует ожидать, что повторный процесс шифрования не уменьшит ненадежности сообщения. То, что это действительно так, можно показать следующим образом. Пусть M, E_1, E_2 – сообщение и первая и вторая криптограммы соответственно. Тогда

$$P_{E_1E_2}(M) = P_{E_1}(M)$$

Следовательно,

$$H_{E_1,E_2}(M) = H_{E_1}(M)$$

так как для любых случайных величин x, y, z справедливо $H_{xy}(z) \le H_y(z)$ то получаем желаемый результат: $H_{E_2}(M) \ge H_{E_1}(M)$.

Теорема 8. *Ненадежность сообщения для произведения секретных систем* $S = TR$ *не меньше ненадежности для одной системы* R.

Предположим, что имеется система T, которая может быть записана как взвешенная сумма нескольких систем $R, S, \ldots, U$

$$T = p_1R + p_2S + \ldots + p_mU, \quad \sum p_i = 1,$$

и системы $R, S, \ldots, U$ имеют ненадежности $H_1, H_2, \ldots, H_m$.

Теорема 9. *Ненадежность для взвешенной суммы систем ограничена неравенствами*

$$\sum p_iH_i \le H \le \sum p_iH_i - \sum p_i \log p_i$$

Эти границы нельзя улучшить. Здесь H_i *могут означать ненадежность ключа или сообщения.*

Верхняя граница достигается, например, в строго идеальных системах (которые будут описаны ниже), где разложение производится на простые преобразования системы. Нижняя граница достигается, если все системы $R, S, \ldots, U$ приводят к полностью различным пространствам криптограмм. Эта теорема также доказывается с помощью общих неравенств, которым подчиняется ненадежность:

$$H_A(B) \le H(B) \le H(A) + H_A(B),$$

где A может обозначать данную используемую систему, а B – ключ или сообщение.

Имеется аналогичная теорема для взвешенных сумм языков. Для ее доказательства обозначим данный язык буквой A.

Теорема 10. *Предположим, что система может быть применена к языкам* $L_1, L_2, \ldots, L_m$ *и при этом получаются ненадежности* $H_1, H_2, \ldots, H_m$. *Если система применяется к взвешенной сумме* $\sum p_iL_i$ *то ненадежность* H *ограничена неравенствами*

$$\sum p_iH_i \le H \le \sum p_iH_i - \sum p_i \log p_i.$$

Эти границы нельзя улучшить. Рассматриваемая ненадежность может относиться как к ключу, так и к сообщению.

Полная избыточность D_N для N букв сообщения определяется с помощью соотношения

$$\boldsymbol{D_N} = \log \boldsymbol{G} - \boldsymbol{H}(\boldsymbol{M}),$$

где $\boldsymbol{G}$ – полное число сообщений длины $\boldsymbol{N}$, а $\boldsymbol{H}(\boldsymbol{M})$ – неопределенность выбора одного из них. В секретной системе, где полное число возможных криптограмм равно числу возможных сообщений длины $\boldsymbol{N}$, имеет место неравенство $\boldsymbol{H}(\boldsymbol{E}) \le \log \boldsymbol{G}$. Следовательно,

$$\boldsymbol{H_E}(\boldsymbol{K}) = \boldsymbol{H}(\boldsymbol{K}) + \boldsymbol{H}(\boldsymbol{M}) - \boldsymbol{H}(\boldsymbol{E}) \ge \boldsymbol{H}(\boldsymbol{K}) - (\log \boldsymbol{G} - \boldsymbol{H}(\boldsymbol{M})).$$

Поэтому

$$\boldsymbol{H}(\boldsymbol{K}) - \boldsymbol{H_E}(\boldsymbol{K}) \le \boldsymbol{D_N}.$$

Из этого видно, что, например, в замкнутой системе уменьшение ненадежности ключа после перехвата $\boldsymbol{N}$ букв не превзойдет избыточности $\boldsymbol{N}$ языка. В таких системах (к ним относится большинство шифров) только наличие избыточности в исходном сообщении и дает возможность нахождения решения.

Предположим теперь, что имеется чистая секретная система. Обозначим различные остаточные классы сообщений через $\boldsymbol{C}_1, \boldsymbol{C}_2, \ldots, \boldsymbol{C}_r$ и соответствующие остаточные классы криптограмм через $\boldsymbol{C}'_1, \boldsymbol{C}'_2, \ldots, \boldsymbol{C}'_r$. Вероятности всех $\boldsymbol{E}$ из $\boldsymbol{C_i}$ одинаковы

$$\boldsymbol{P}(\boldsymbol{E}) = \frac{\boldsymbol{P}(\boldsymbol{C}_i)}{\boldsymbol{\varphi}_i}, \ \boldsymbol{E} - \text{элемент } \boldsymbol{C_i},$$

где $\boldsymbol{\varphi_i}$ – число различных сообщений в $\boldsymbol{C_i}$. Таким образом, имеем

$$\boldsymbol{H}(\boldsymbol{E}) = -\sum_i \boldsymbol{\varphi}_i \frac{\boldsymbol{P}(\boldsymbol{C}_i)}{\boldsymbol{\varphi}_i} \log \frac{\boldsymbol{P}(\boldsymbol{C}_i)}{\boldsymbol{\varphi}_i} = -\sum_i \boldsymbol{P}(\boldsymbol{C}_i) \log \frac{\boldsymbol{P}(\boldsymbol{C}_i)}{\boldsymbol{\varphi}_i}.$$

Подставив это значение $\boldsymbol{H}(\boldsymbol{E})$ в выражение, полученное выше для $\boldsymbol{H_E}(\boldsymbol{K})$, получим следующую теорему.

Теорема 11. *Для чистого шифра*

$$\boldsymbol{H}_{\boldsymbol{E}}(\boldsymbol{K}) = \boldsymbol{H}(\boldsymbol{K}) + \boldsymbol{H}(\boldsymbol{M}) + \sum_i \boldsymbol{P}(\boldsymbol{C}_i) \log \frac{\boldsymbol{P}(\boldsymbol{C}_i)}{\boldsymbol{\varphi}_i}.$$

Это выражение может быть использовано для вычисления $\boldsymbol{H_E}(\boldsymbol{K})$ в некоторых случаях, представляющих интерес.