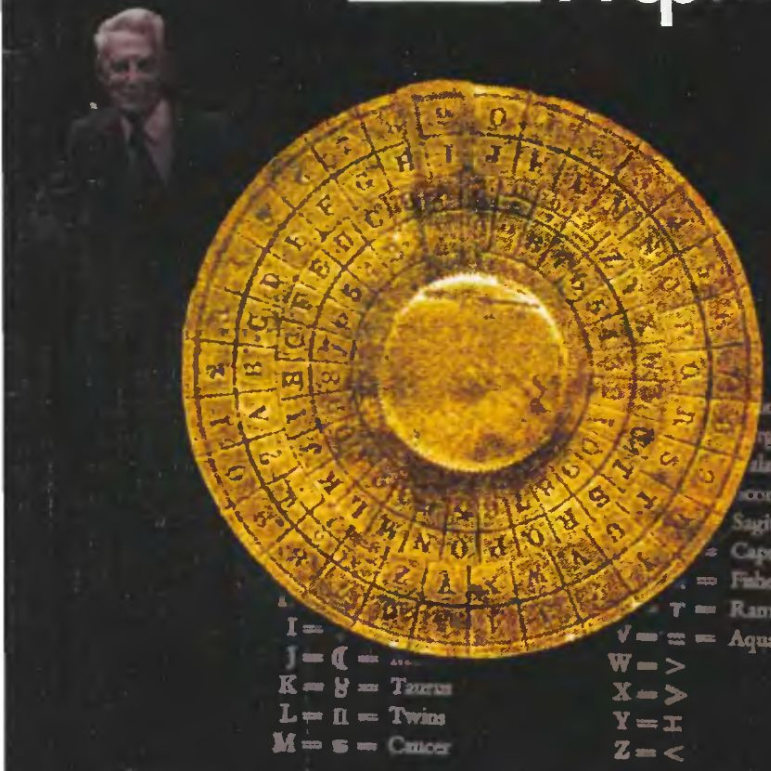
А. Ю. Зубов

Совершенные шифры



гелиос арв

А. Ю. Зубов

Совершенные шифры

Дополнительные главы
курса криптографии

Москва
«Гелиос АРВ»
2003

ББК 32.8166
351

Зубов А.Ю.

351 Совершенные шифры: Вступительное слово чл.-корр. РАН Б. А. Севастьянова. — М.: Гелиос АРВ, 2003. — 160 с., ил.

ISBN 5-85438-076-5

Изложены свойства и конструкции безусловно стойких шифров, названных К. Шенноном совершенными по отношению к различным криптоатакам. Выделяются совершенные шифры с минимально возможным числом ключей, а также стойкие к попыткам обмана со стороны злоумышленника.

Для научных работников, аспирантов, специализирующихся в области математических проблем криптографии, преподавателей и студентов, изучающих дисциплину "Криптографические методы защиты информации" по специальностям "Компьютерная безопасность", "Комплексное обеспечение безопасности автоматизированных систем", "Информационная безопасность телекоммуникационных систем".

ББК
32.8166

Зубов Анатолий Юрьевич

Совершенные шифры

Заведующая редакцией *Т. А. Денисова*
Корректор *Е. Н. Клитина*
ЛР № 066255 от 29.12.98. Издательство "Гелиос АРВ". www.gelios-arv.ru
107140, Москва, Верхняя Красносельская, 16. Тел. (095)264-44-39,
e-mial: info@gelios-arv.ru
Формат 84×108/32. Бумага офсетная. 5 п. л. Тираж 2000 экз. Заказ № 2243.
Отпечатано с готовых диапозитивов в РГУП "Чебоксарская типография № 1".
Адрес типографии: 428019, г. Чебоксары, пр. И. Яковлева, 15.

ISBN 5-85438-076-5

Вступительное слово

В приложениях математики обычно сначала строят математическую модель исследуемого объекта. Затем эта модель изучается математическими методами. Выводы из полученных результатов будут правильными, если математическая модель правильно отражала основные свойства объекта.

В криптографии при применении математических методов необходимо использовать ту или иную модель открытой информации. Например, для чтения перехваченного зашифрованного с помощью простой замены длинного текста достаточно знать частоты букв того языка, на котором был написан открытый текст. Если длина криптограммы была сравнительно небольшой, то для ее чтения может понадобиться уже статистика биграмм, триграмм и т.д. В конце концов всегда используется так называемая "читаемость открытого текста", которая в математической модели никак не определяется. Использование какой-либо модели является слабым звеном любого анализа стойкости шифрсистемы. В работах К.Шеннона в середине 20-го века было показано, что существуют совершенные шифры, которые не поддаются дешифровке никаким способом. Это утверждение математически доказано и справедливо при любой модели языка. В частности, таким является гаммирование с помощью равновероятной гаммы.

В книге А.Ю.Зубова дается подробное изложение теории совершенных шифров. Описываются различные классы совершенных шифров, в частности имитостойкие совершенные шифры и шифры, стойкие к шифратакам, основанным на совокупности нескольких шифртекстов, полученных на одном ключе.

В книге широко используются многие комбинаторные и алгебраические структуры (латинские квадраты и прямоугольники, блок-схемы, ортогональные массивы, группы, квазигруппы, векторные пространства над конечными полями).

Тематика этой книги до сих пор не была достойно отражена в многочисленных изданиях, которые в последнее время выходили на русском языке. Полагаю, что книга будет полезна специалистам в области защиты информации.

Б. А. Севастьянов,
член-корреспондент РАН,
действительный член Академии криптографии РФ

Введение

В 40-х годах прошлого века К. Шеннон, разрабатывая теорию криптографической стойкости, ввел понятие совершенного шифра как шифра, обеспечивающего наилучшую защиту ([Шен63]). Определение совершенного шифра потребовало математической формализации задачи, отвечающей интуитивному представлению о том, что лучший шифр должен создавать для оппонента наиболее неблагоприятные условия для криптоанализа. Имеется в виду, что сведения об открытом тексте, которые криптоаналитик мог бы получить на основе изучения перехваченной криптограммы, не должны отличаться от общеизвестной априорной информации об открытом тексте. К. Шеннон характеризовал шифры, являющиеся совершенными по отношению к криптоатаке на основе одного шифртекста. Таковыми оказались, например, шифры гаммирования со случайной равновероятной гаммой, к числу которых относится шифр Вернама, известный также под названием одноразовый шифр-блокнот (по-английски — *One Time Pad*).

Совершенный шифр особенно хорош тем, что для него невозможен полный перебор ключей с целью определения открытого текста по известной криптограмме. Например, при попытке перебрать все 2^n возможных ключей шифра Вернама (при наличии криптограммы длиной в n бит) криптоаналитик получит вместе с истинным открытым текстом и все другие осмысленные открытые тексты той же длины. Выбрать же из них нужный открытый текст не представляется возможным. Метод шифрования, который предлагает шифр Вернама, можно было бы считать идеальным, если бы не один серьезный недостаток — слишком большой расход ключевой информации. Конечно, современные технические средства позволяют обеспечить хранение большого объема ключей, используя, например, лазерные диски. Однако реализация

данного метода при шифровании больших объемов открытого текста будет слишком дорогой и неудобной. Например, чтобы обеспечить шифрование изображения со спутника-шпиона, необходимо будет отправить в космос целый контейнер с несколькими тысячами дисков. Большие трудности возникают также при попытке объединить в сети связи большое количество абонентов. Ведь в этом случае необходимо иметь возможность быстро получать доступ к любому ключу любого пользователя (которых может быть несколько тысяч)[1]. Таким образом, на практике, как правило, приходится довольствоваться шифрами, которые не являются совершенными. Тем не менее в тех случаях, когда наиболее важна секретность, а объем текста невелик (как, например, в "горячей линии" Москва–Вашингтон[2]), совершенным шифрам следует отдать предпочтение.

В некоторых книгах по криптографии на русском языке, появившихся в 90-е годы, не вполне корректно утверждается, что шифр Вернама является единственным совершенным шифром. Это утверждение становится почти правильным, если ограничиться рассмотрением лишь совершенных шифров с минимально возможным числом ключей. В общем же случае утверждение о единственности совершенного шифра совсем неверно. Более того, существуют совершенные шифры с неравновероятными ключами. Подчеркнем также, что совершенные шифры являются таковыми лишь в совершенно определенных условиях. Тот же самый шифр Вернама является нестойким к криптоатакам на основе нескольких криптограмм, полученных на одном ключе. Этот шифр потому и "одноразовый", что обеспечивает надежную защиту лишь при однократном использовании ключа, коим является случайная равновероятная гамма.

---

[1] Хотя эта задача и сложна, но не безнадежна. Имеются способы "размножения" качественных ключей, с некоторыми из которых можно ознакомиться, например, в [Rub96].

[2] Об этом указывается, например, в [Мэс88], [Бра99].

Как мы уже отмечали, в основе рассмотрения совершенных шифров лежит математическая модель шифра. Имеются различные подходы к построению таких моделей (см., например, [Алф01], [Баб02], [Бра99], [Sti95]). В данной книге предлагается некоторая модификация модели, приведенной в [Алф01]. Она использует понятия опорного шифра, ключевого потока, а также введение двух классов шифров — с ограниченным ключом и с неограниченным ключом. На наш взгляд, такой подход устраняет ряд неясных вопросов, обычно возникающих при изложении данной темы.

После К. Шеннона понятие совершенного шифра было обобщено и для некоторых других криптоатак (см., например, [Sti88], [Soe88], [God90]). К ним относятся криптоатаки на основе совокупностей шифртекстов, полученных на одном ключе (соответствующие им совершенные шифры названы $U(L)$ -, $S(L)$ - или $O(L)$ -стойкими), а также криптоатаки на основе известного открытого текста ($M(L)$ -стойкие шифры).

Следует отметить, что данная тематика развивается в связи с изучением так называемых кодов аутентификации с секретностью, которые представляют собой некие формальные математические модели теории аутентификации. На самом деле в работах на эту тему речь идет о традиционных вопросах имитостойкости шифров, коими, по сути дела, являются коды аутентификации с секретностью. В связи с этим возникает естественный вопрос: существуют ли шифры, являющиеся одновременно совершенными (в том или ином смысле) и обладающие лучшими параметрами имитостойкости, к которым традиционно относят вероятности имитации и подмены? Оказывается, что при определенных условиях такие шифры существуют.

В данной книге делается попытка разобраться во всех упомянутых нюансах и с единых позиций изложить вопросы о строении совершенных шифров. Однако, даже изучив эту книгу, читатель далеко не всегда сможет построить примеры

совершенных шифров с минимально возможным числом ключей для различных типов криптоатак. Дело в том, что многие результаты в этой области формулируются примерно так: если при некоторых значениях параметров существует некая комбинаторная конфигурация, то существует и совершенный шифр с соответствующими параметрами. В свою очередь, вопрос о существовании подобных конфигураций на сегодняшний день является открытой проблемой. Условие минимальности числа ключей существенно с точки зрения возможных практических приложений. Если же от него отказаться, то примеры совершенных шифров (для любых рассматриваемых здесь криптоатак) привести несложно. Отметим также, что в книге рассматриваются в основном криптоатаки, целью которых является получение информации об открытом тексте. Лишь в дополнении речь идет о криптоатаках, целью которых является получение информации об использованном ключе.

Кратко остановимся на содержании книги.

В главе 1 указываются основные пассивные и активные атаки, которые обычно используются в криптоанализе.

В главе 2 вводится математическая модель шифра, лежащая в основе всех содержательных результатов. Дается определение совершенного шифра и показывается, что совершенным может быть лишь шифр с неограниченным ключом. Приводится характеризация К. Шеннона совершенных шифров с минимально возможным числом ключей. Доказывается, что таковыми являются так называемые шифры табличного гаммирования, определяемые латинскими квадратами, и только они. Рассматриваются совершенные шифры, которые обладают минимальными вероятностями имитации и подмены. Эти вероятности характеризуют эффективность активных атак. Указывается связь таких шифров с математической теорией блок-схем.

В главе 3 строятся линейные совершенные шифры. Для них множества шифрвеличин и шифробозначений представляют собой множества ненулевых элементов линейных про-

странств над конечным полем. Предлагаются конструкции на основе линейных рекуррентных последовательностей максимального периода.

В главе 4 теория совершенных шифров К. Шеннона обобщается для других криптоатак. Прежде всего, изучается случай криптоатаки на основе неупорядоченной совокупности шифртекстов, полученной на одном ключе. Устанавливается связь конструкций изучаемых шифров с ортогональными массивами. Изучаются шифры, обеспечивающие наилучшую защиту к рассматриваемой пассивной атаке и активным атакам.

В главе 5 рассматриваются криптоатаки на основе упорядоченных совокупностей шифртекстов, а также на основе упорядоченных совокупностей открытых и шифрованных текстов, полученных на одном ключе. Приводится иерархия различных понятий совершенной стойкости.

В главе 6 изучаются комбинаторные свойства шифров, обеспечивающих наилучшую защиту к атакам на основе неупорядоченных совокупностей шифртекстов, полученных на одном ключе.

Глава 7 посвящена изучению комбинаторных свойств совершенных шифров для криптоатак на основе упорядоченных совокупностей текстов. Указывается связь конструкций таких шифров с кратно транзитивными множествами подстановок (в частности, групп подстановок) и латинскими прямоугольниками.

Почти все утверждения, приведенные в книге, были сформулированы в работах, указанных в списке литературы. Однако автора не удовлетворяло либо отсутствие доказательств, либо их чрезмерная лаконичность, либо недостаточная проработанность понятийной основы. Некоторые "очевидные" утверждения автору удалось доказать лишь при некоторых дополнительных ограничениях. В предлагаемом варианте все основные утверждения доказаны и адаптированы для понимания студентами.

Материал книги можно использовать для углубленного изучения теоретических основ криптографии в рамках спецкурсов (или дисциплин по выбору) будущими специалистами по защите информации. Тематика книги, на наш взгляд, полезна с точки зрения расширения математического кругозора читателя, поскольку в ней естественным образом возникает целый ряд алгебраических и комбинаторных объектов, таких, как группа, квазигруппа, векторное пространство, конечное поле, латинский квадрат или прямоугольник, ортогональный массив или блок-схема. В книге приводятся числовые примеры, позволяющие читателю лучше разобраться в данной тематике и понять общие утверждения. От читателя требуется знание основ алгебры и теории вероятностей.

Автор выражает глубокую признательность Ф.М.Малышеву и Б.А.Севастьянову за конструктивную критику и ряд ценных замечаний, существенно улучшивших данную работу.

Глава 1

Криптоатаки

Надежность или стойкость шифрования определяется объемом работы криптоаналитика, необходимой для вскрытия системы. Шифрсистема может служить объектом нападения противника, располагающего тем или иным интеллектуальным и вычислительным потенциалом. Возможности потенциального противника определяют требования, предъявляемые к надежности шифрования.

Исходная информация и цели криптоаналитика могут быть разными. Несомненно, основная цель противника состоит в получении конфиденциальной информации. Целью нападения может служить также примененный секретный ключ, с помощью которого криптоаналитик может вскрывать другие криптограммы. Шифрсистема может быть невосприимчивой к одним угрозам и быть уязвимой по отношению к другим. Попытки противника по добыванию зашифрованной информации обычно называют *криптоатаками*.

В криптографии с секретным ключом обычно рассматривают следующие криптоатаки (см., например, [Алф01], [Бра99]).

- *Атака на основе шифртекста*: криптоаналитик располагает шифртекстами $y_1, \ldots, y_m$, полученными из неизвестных открытых текстов $x_1, \ldots, x_m$ различных сообщений. Требуется найти хотя бы один из x_i, $i=\overline{1,m}$, (или соответствующий ключ k_i), исходя из достаточного числа m криптограмм, или убедиться в своей неспособности сделать это. В качестве частных случаев возможно совпадение ключей: $k_1=\ldots=k_m$ или совпадение открытых текстов: $x_1=\ldots=x_m$.

- *Атака на основе известного открытого текста*: *криптоаналитик* располагает парами $(x_1, y_1), \ldots, (x_m, y_m)$ открытых и отвечающим им шифрованных текстов. Требуется определить ключ k_i для хотя бы одной из пар. В частном случае, когда $k_1 = \ldots = k_m = k$, требуется определить ключ k или, убедившись в своей неспособности сделать это, определить открытый текст x_{m+1} еще одной криптограммы y_{m+1}, зашифрованной на том же ключе.
- *Атака на основе выбранного открытого текста* отличается от предыдущей лишь тем, что криптоаналитик имеет *возможность выбора* открытых текстов $x_1, \ldots, x_m$. Цель атаки — та же, что и предыдущей. Подобная атака возможна, например, в случае, когда криптоаналитик имеет доступ к шифратору передающей стороны, или в системах опознавания "свой-чужой".
- *Атака на основе выбранного шифртекста* отличается от второй атаки лишь тем, что криптоаналитик имеет *возможность выбора* шифртекстов $y_1, \ldots, y_m$. Цель атаки — та же, что и во втором случае. Подобная атака возможна, например, в случае, когда криптоаналитик имеет доступ к шифратору принимающей стороны.

Атаки на основе выбранных текстов считаются наиболее опасными. Иногда к указанным атакам добавляют и другие. Шифр, выдерживающий все возможные атаки, можно признать стойким или надежным.

Различие в действенности криптоатак можно прокомментировать на примере криптоанализа поточного шифра простой замены. Хотя этот шифр легко вскрываем даже при использовании атаки на основе шифртекста, это все-таки требует некоторых усилий. При проведении атаки на основе известного открытого текста задача становится вовсе тривиальной, как только в доступных открытых текстах встретятся

все буквы алфавита. Наконец, при атаке на основе выбранного открытого текста ничего не нужно ждать, так как ключ автоматически получается при зашифровании всех букв алфавита.

При оценке эффективности любой криптоатаки обычно пользуются общепринятым в криптографии *правилом Керкгоффса* (голландского криптографа XIX в.). Это правило изложено в книге "Военная криптография", изданной в 1883 г. В ней сформулировано шесть следующих требований к системам шифрования.

- Система должна быть нераскрываемой, если не теоретически, то практически.
- Компрометация системы не должна причинять неудобств ее пользователям.
- Секретный ключ должен быть легко запоминаемым без каких-либо записей.
- Криптограмма должна быть представлена в такой форме, чтобы ее можно было передать по телеграфу.
- Аппаратура шифрования должна быть портативной и такой, чтобы ее мог обслуживать один человек.
- Система должна быть простой. Она не должна требовать ни запоминания длинного перечня правил, ни большого умственного напряжения.

Второе из этих правил и стало называться правилом Керкгоффса. Суть его состоит в том, что при проведении криптоанализа можно считать известной систему шифрования. *Стойкость* (или надежность) *шифрования должна определяться лишь секретностью ключа шифрования.* Признание всеми этого принципа в криптографии связано с тем, что "шила в мешке не утаишь". Рано или поздно те или иные сведения об используемой шифрсистеме становятся известными. В военных условиях могут быть захвачены узлы связи с шифртехникой. Может потерпеть аварию и попасть в руки

противника самолет или судно, оборудованные шифрсредствами. Нельзя исключать предательства шифровальщика и т.п. Тем не менее шифры, используемые специальными службами, всемерно охраняются. Это обусловлено необходимостью в дополнительном запасе прочности, поскольку до сих пор создание шифров с *доказуемой стойкостью* является очень сложной проблемой.

В [Бра99] используется термин *криптосистема ограниченного использования* для систем, стойкость которых основывается на сохранении в секрете самого алгоритма шифрования. Простейшим историческим примером такой системы является шифр Цезаря. Там же вводится термин *криптосистема общего использования* для систем, стойкость которых основывается не на секретности алгоритма шифрования, а на секретности используемого ключа.

Обоснование надежности шифрсистем осуществляется, как правило, теоретически и экспериментально при моделировании криптоатак с привлечением группы высококвалифицированных специалистов, которым предоставляются благоприятные условия для работы и необходимая техника. На государственном уровне гарантию надежности криптографической защиты дают уполномоченные для этой цели организации. В России такой организацией является ФАПСИ. Любые средства шифрования, используемые государственными организациями, должны иметь сертификат ФАПСИ.

Рассмотрение вопросов надежности шифрования невозможно без введения качественной и количественной мер. В криптографии рассматривают два подхода к стойкости — *теоретическую* (или безусловную) *стойкость* и *практическую* (или вычислимую) *стойкость*. При рассмотрении вопроса о теоретической стойкости шифров отвлекаются от реальных временных и сложностных затрат по вскрытию шифра (что определяет подход к практической стойкости). Во главу угла ставится принципиальная возможность получения некоторой информации об открытом тексте или использован-

ном ключе. Теоретически стойкие (или совершенные) шифры характеризуются тем, что сама задача дешифрования для них становится бессмысленной. Это значит, что никакой метод криптоанализа, включая полный перебор ключей, не позволяет не только определить ключ или открытый текст, но даже получить *некоторую* информацию о них. Далее будет дано формальное определение совершенного шифра.

Указанные криптоатаки относятся к разряду пассивных атак. Так классифицируются действия потенциального противника, который "пассивно изучает" передаваемые по каналу связи шифрованные сообщения, может их перехватить и подвергнуть криптоанализу с целью получения информации об открытом тексте или использованном ключе. Однако современные технические средства позволяют потенциальному противнику "активно" вмешиваться в процесс передачи сообщения. Обычно различают два типа активных атак, которые носят названия *имитации* и *подмены* сообщения. Атака имитации состоит в том, что противник "вставляет" в канал связи сфабрикованное им "шифрованное" сообщение, которое на самом деле не передавалось от законного отправителя к получателю. При этом противник рассчитывает на то, что получатель воспримет это сфабрикованное сообщение как подлинное (аутентичное). Атака подмены состоит в том, что противник, наблюдая передаваемое по каналу связи подлинное сообщение от отправителя, "изымает" его и заменяет поддельным[3]. На активные атаки также распространяется правило Керкгоффса.

Различные шифры могут быть более или менее уязвимыми к активным атакам. Способность самого шифра (без использования дополнительных средств) противостоять активным атакам обычно называют *имитостойкостью* шифра. Количественной мерой имитостойкости шифра служат вероятности имитации и подмены соответственно. Эти вероятно-

[3] Противник может принять свое решение на основе наблюдения ряда сообщений.

сти определяют шансы противника на успех при навязывании получателю ложного сообщения. Имеются достижимые нижние оценки этих вероятностей. Естественно считать наиболее имитостойкими шифры, для которых эти нижние оценки достигаются.

Нас, в первую очередь, будут интересовать совершенные шифры с достижимыми нижними оценками вероятностей имитации и подмены.

Глава 2

Теоретическая стойкость шифров

В данной главе излагаются основные положения теории совершенных шифров.

Систематически вопрос о теоретической стойкости шифров впервые исследовал К. Шеннон в своей фундаментальной работе [Шен63], опубликованной в 1949 г.[4] В этой книге он рассматривал вероятностную модель шифра (или *секретной системы*) и криптоатаку на основе шифртекста. Проследим за его рассуждениями.

Как мы указывали, конечной целью работы криптоаналитика является текст сообщения или ключ шифрования. Однако весьма полезной может быть даже некоторая *вероятностная* информация об открытом тексте. Например, уже предположение о том, что открытый текст написан по-русски, предоставляет криптоаналитику априорную информацию об этом сообщении даже до того, как он увидит шифртекст. Так, например, он заранее знает, что слово *дорогой* является более вероятным началом сообщения, чем, скажем, набор, состоящий из букв *абвгдеж*. Поэтому первой целью криптоанализа является увеличение количества априорной информации о каждом возможном открытом тексте таким образом, чтобы истинный открытый текст сделать более вероятным после получения шифртекста, хотя, конечно, и не обязательно точным.

Пусть, например, криптоаналитик перехватил текст *мтутпти* и знает (или предполагает), что он был зашифрован при помощи шифра простой замены. Этот шифр-

---

[4] Известно, что основные результаты по теории секретных систем (оформленные в виде секретного отчета) были получены К. Шенноном до 1945 г. Примерно в те же годы концепция совершенного шифра разрабатывалась в одной закрытой работе, выполненной под руководством В. А. Котельникова (см. [Анд98]).

текст свидетельствует о том, что открытый текст состоит из семи букв, причем вторая, четвертая и шестая буквы совпадают друг с другом, а остальные отличны от этой буквы и попарно различны. Хотя нельзя быть уверенным, что этим словом является *дорогой* (это может быть еще *молоток, потолок* или что-то подобное), тем не менее *апостериорные вероятности* таких открытых текстов возрастают относительно их априорных вероятностей. Криптоаналитик, кроме того, полностью уверен (в предположении, что использовалась именно простая замена) в том, что этот открытый текст не может быть ни словом *призрак*, ни словом *сатирик*, и, таким образом, апостериорная вероятность обоих этих открытых текстов сокращается до нуля, даже вне зависимости от их априорных вероятностей. Шеннон назвал шифр *совершенным*, если ни один шифртекст не раскрывает никаких сведений о соответствующем ему открытом тексте. Это означает, что для совершенных шифров апостериорные вероятности открытых текстов (вычисленные после получения криптограммы) совпадают с их априорными вероятностями.

Для формализации нам понадобится математическая модель шифра.

§ 2.1. Математическая модель шифра

Используя терминологию, принятую в [Алф01], под *шифром* мы понимаем любой симметричный шифр однозначной замены, алфавитом которого служит множество *шифр-величин*. Это множество адаптировано к способу шифрования. Им может быть, например, множество отдельных знаков исходного алфавита, m-грамм, или другое конечное множество слов.

Шифрвеличины, составляющие открытый текст, поочередно шифруются одной из "простых замен", составляющих данный шифр замены. Выбор той или иной "простой замены"

осуществляется с помощью *ключевого потока* (или, в терминологии [Алф01], *распределителя*), представляющего собой последовательность номеров "простых замен". Ключевой поток может получаться случайным образом, например, с помощью рандомизатора типа игровой рулетки. Такой шифр мы будем называть *шифром с неограниченным ключом*. Ключами шифра служат всевозможные ключевые потоки. Шифр с неограниченным ключом полностью определяется своим действием на множестве шифрвеличин и рандомизатором. Ключевой поток может также функционально зависеть от ключа шифра и вычисляться детерминированно (по некоторому алгоритму или программе). Число возможных ключевых потоков фиксированной длины не превосходит в этом случае числа ключей шифра. Такой шифр мы будем называть *шифром с ограниченным ключом*. Подавляющее большинство шифров, используемых на практике, являются именно шифрами с ограниченным ключом. Ключевым потоком для них служит, как правило, выходная последовательность некоторого *автономного автомата*[5)], множество внутренних состояний которого совпадает с множеством ключей шифра.

После неформального пояснения нашего подхода перейдем к детальному описанию модели шифра.

Пусть X и Y — конечные множества шифрвеличин и шифробозначений, с которыми оперирует некоторый шифр замены,

$$|X| > 1,\ |Y| > 1,\ |Y| \geq |X|.$$

Это означает, что открытые и шифрованные тексты представляются словами в алфавитах X и Y соответственно. Процесс зашифрования открытого текста $x = x_1 \ldots x_l$ заключается в

[5)] Определение автомата можно найти в любом учебнике по дискретной математике, например в [Сач77] или [Гор86].

замене каждой шифрвеличины x_i на некоторое шифробозначение y_i, $i = \overline{1,l}$, в соответствии с одним из n $(n > 1)$ инъективных отображений $e_j : X \to Y$, индексированных числами $j \in K = \{0,1,...,n-1\}$. Будем называть эти отображения e_j *простыми заменами*[6]. Ясно, что максимальное число n простых замен, составляющих шифр замены, не превосходит числа размещений

$$A_{|Y|}^{|X|}.$$

Пусть

$$e_j(X) = \{e_j(x),\ x \in X\},\ j = \overline{0,n-1}.$$

Через d_j обозначим отображение $e_j(X) \to X$, такое что $d_j(e_j(x)) = x$ для любого $x \in X$. По определению

$$Y = \bigcup_{j \in K} e_j(X).$$

Определение 2.1.1. *Опорным шифром шифра замены назовем совокупность*

$$\Sigma = (X, K, Y, E, D) \qquad (2.1.1)$$

объектов, в которой X и Y — множества шифрвеличин и шифробозначений, $K = \{0,1,...,n-1\}$ — множество ключей,

[6] В соответствии с общепринятым названием шифра простой замены.

и[7] $E = \{e_j, j \in K\}$ — *множество правил зашифрования,* $D = \{d_j, j \in K\}$ — *множество правил расшифрования.*

Определение 2.1.2. *l-й степенью опорного шифра* $\sum$ *назовем совокупность объектов*

$$\sum{}^{l} = (X^l, K^l, Y^l, E^{(l)}, D^{(l)}), \qquad (2.1.2)$$

$l \in \mathbf{N}$, *в которой* X^l, K^l, Y^l — *декартовы степени множеств* X, K, Y *соответственно; множество* $E^{(l)}$ *состоит из отображений*

$$e_{\bar{k}} : X^l \to Y^l, \ \bar{k} \in K^l,$$

таких что для $\bar{x} = x_1 \ldots x_l \in X^l$ *и* $\bar{k} = k_1 \ldots k_l \in K^l$

$$e_{\bar{k}}(\bar{x}) = e_{k_1}(x_1) \ldots e_{k_l}(x_l) \in Y^l, \ e_{k_i} \in E, \ i = \overline{1,l};$$

множество $D^{(l)}$ *состоит из отображений*

$$d_{\bar{k}} : e_{\bar{k}}(X^l) \to X^l, \ \bar{k} \in K^l,$$

таких что для $\bar{y} = y_1 \ldots y_l \in e_{\bar{k}}(X^l)$ *и* $\bar{k} = k_1 \ldots k_l \in K^l$

$$d_{\bar{k}}(\bar{y}) = d_{k_1}(y_1) \ldots d_{k_l}(y_l) \in X^l, \ d_{k_i} \in D, \ i = \overline{1,l}.$$

При $l = 1$ шифр $\sum^{l}$ совпадает с шифром $\sum$.

[7] В соответствии с терминологией [Алф01].

Введя понятие степени опорного шифра, мы определили действие шифра замены на последовательности шифрвеличин — элементарных единиц открытого текста. Теперь мы должны объяснить, как строится ключевой поток, т. е. последовательность $k_1,...,k_l$, $k_j \in K$, $j = \overline{1,l}$, номеров простых замен (e_{k_j}), используемых для зашифрования произвольного открытого текста $x = x_1...x_l$, $x_i \in X$, $i = \overline{1,l}$.

Как мы уже отмечали, имеется два, принципиально разных, способа построения такой последовательности. Рассмотрим первый способ.

Если нужно случайно выбрать один из двух вариантов, то достаточно подбросить монету. Исход бросания ("орел" или "решка") укажет случайный выбор. Аналогично можно поступить для случайного выбора одного из 2^m вариантов — достаточно подбросить монету m раз подряд. Заметим, что при этом исходы бросаний образуют последовательность испытаний случайной величины ξ, принимающей значения 0 и 1 с вероятностями p и q соответственно ($p + q = 1$). Нулем мы обозначили "орел", единицей — "решку". Обычно $p = q = 1/2$, хотя это и не обязательно. Вместо монеты можно было использовать другой рандомизатор.

Используя приведенную аналогию, будем в первом случае строить ключевой поток с помощью некоторого рандомизатора, который выбирает тот или иной ключевой поток данной длины l в соответствии с некоторым априорным распределением вероятностей, заданным на множестве K^l, $l \in \mathbf{N}$.

Заметим, что аналогичная ситуация имеет место и при выборе шифрвеличин из множества X^l, $l \in \mathbf{N}$. Этот выбор производится в соответствии с частотными характеристиками открытых текстов. Хорошо известно (см. [Алф01]), что такие

характеристики для обычных ("читаемых") открытых текстов далеко не равномерны. Пусть

$$P(K^l) = \{p_{K^l}(\bar{k}),\ \bar{k} \in K^l\} \qquad (2.1.3)$$

и

$$P(X^l) = \{p_{X^l}(\bar{x}),\ \bar{x} \in X^l\} \qquad (2.1.4)$$

— выбранные априорные распределения вероятностей. Обозначим через $\widetilde{K}^l$, $\widetilde{X}^l$ случайные величины, принимающие значения из K^l и X^l в соответствии с распределениями (2.1.3) и (2.1.4). По определению случайные величины $\widetilde{K}^l$, $\widetilde{X}^l$ мы полагаем независимыми.

Далее нам понадобится понятие *l-го опорного шифра*, под которым мы будем понимать совокупность

$$(\widetilde{X}^l, \widetilde{K}^l, \widetilde{Y}^l, E^{(l)}, D^{(l)}),$$

где $\widetilde{X}^l$, $\widetilde{K}^l$ — введенные выше случайные величины, $\widetilde{Y}^l$ — случайная величина с множеством исходов Y^l и распределением вероятностей

$$P(Y^l) = \{p_{Y^l}(\bar{y}),\ \bar{y} \in Y^l\},$$

$E^{(l)}$, $D^{(l)}$ — множества правил зашифрования и правил расшифрования, введенных определением 2.1.2. Распределение $P(Y^l)$ индуцируется $P(X^l)$ и $P(K^l)$ и вычисляется по формуле

$$p_{Y^l}(\bar{y}) = \sum_{\substack{(\bar{x},\bar{k})\in X^l\times K^l:\\ e_{\bar{k}}(\bar{x})=\bar{y}}} p_{X^l}(\bar{x})\cdot p_{K^l}(\bar{k}). \qquad (2.1.5)$$

В связи с введением понятия l-го опорного шифра сделаем одно замечание.

В ряде случаев не всякое слово длины l в алфавите X может появиться в открытом тексте. Например, в тексте на русском языке не может встретиться биграмма ъъ. С точки зрения шифрования совершенно безразлично, встретится такая биграмма в тексте или нет. Для нас важно то, что при задании распределения вероятностей $P(X^l)$ в соответствии с частотными характеристиками языка мы должны положить вероятность l-граммы, содержащей ъъ, равной нулю. Поэтому мы будем исключать из X^l l-граммы, которые не встречаются в множестве открытых текстов, рассматривая вместо X^l множество $X^{(l)}$, состоящее лишь из тех l-грамм, для которых

$$p_{X^l}(\bar{x}) > 0.$$

Это условие будет использоваться по существу при изучении совершенных шифров в следующем параграфе.

Мы будем также полагать, что "запрещенных" l-грамм "не слишком много", точнее, что для любого $l \in \mathbb{N}$ выполняется неравенство

$$\left|X^{(l+1)}\right| > \left|X^{(l)}\right|. \qquad (2.1.6)$$

Для этого достаточно, например, естественного условия, состоящего в том, что любой открытый текст можно "удлинить", т. е. дополнить некоторой шифрвеличиной до открытого текста большей длины.

В той же связи вместо Y^l мы рассматриваем $Y^{(l)}$. При этом (как и для опорного шифра) полагаем

$$Y^{(l)} = \bigcup_{\bar{k} \in K^l} e_{\bar{k}}(X^{(l)}). \tag{2.1.7}$$

Теперь мы можем ввести понятие шифра с неограниченным ключом.

Определение 2.1.3. *Пусть*

$$\Sigma_{\text{H}}^{(l)} = (\widetilde{X}^{(l)}, \widetilde{K}^l, \widetilde{Y}^{(l)}, E^{(l)}, D^{(l)}) \tag{2.1.8}$$

— совокупность случайных величин $\widetilde{X}^{(l)}, \widetilde{K}^l, \widetilde{Y}^{(l)}$, *множеств правил зашифрования и расшифрования* $E^{(l)}, D^{(l)}$, *для которой выполняются условия*

$$P\{\widetilde{X}^{(l)} = \bar{x}\} > 0, \quad P\{\widetilde{K}^l = \bar{k}\} > 0 \tag{2.1.9}$$

при любых $\bar{x} \in X^{(l)}$, $\bar{k} \in K^l$.

Тогда шифром замены с неограниченным ключом назовем семейство

$$\Sigma_{\text{H}} = (\Sigma_{\text{H}}^{(l)}, \ l \in \mathbb{N}). \tag{2.1.10}$$

При этом совокупность (2.1.8) *будем называть* l*-м опорным шифром шифра* Σ_{H}.

Шифр с неограниченным ключом представляет собой семейство шифров[8] $\Sigma_{\text{H}}^{(l)}$, действующих на множествах $X^{(l)}$

[8] В смысле определения шифра, введенного в [Алф01].

открытых текстов, $l \in \mathbb{N}$, и объединенных общим способом преобразования множества шифрвеличин. Для зашифрования открытого текста длины l (так же как и для расшифрования криптограммы длины l) шифр с неограниченным ключом использует l-й опорный шифр. При этом из множества K^l с помощью некоторого рандомизатора случайно выбирается ключ $\bar{k}$ в соответствии с априорным распределением $P(K^l)$.

Сделаем ряд пояснений в связи с определением 2.1.3.

Может возникнуть вопрос: почему вместо семейства моделей $\sum_{\mathrm{H}}^{(l)}$ в этом определении не рассматривать одну модель с множеством открытых текстов

$$\overline{X} = \bigcup_{l=1}^{\infty} X^{(l)},$$

множеством ключей

$$\overline{K} = \bigcup_{l=1}^{\infty} K^l$$

и множеством шифрованных текстов

$$\overline{Y} = \bigcup_{l=1}^{\infty} Y^{(l)}.$$

Такой подход обладает, на наш взгляд, одним существенным недостатком. Дело в том, что при этом не всякий открытый текст можно зашифровать на любом ключе. В самом деле, ключ $\bar{k} \in K^l$ можно применять лишь к открытому тексту $\bar{x} \in X^{(l)}$. Поэтому мы не можем рассматривать правила зашифрования как отображения $e_{\bar{k}} : \overline{X} \to \overline{Y}$ для любого

$\bar{k} \in \bar{K}$. Отметим, что указанная возможность предусматривается в модели шифра, предлагаемой в [Бра99]. Там в качестве правил зашифрования рассматриваются отображения

$$e_{\bar{k}} : \bar{X}_{\bar{k}} \to \bar{Y}, \qquad (2.1.11)$$

где $\bar{X}_{\bar{k}}$ — множество открытых текстов, которые *можно зашифровать* на ключе $\bar{k}$. Конечно, и этот подход имеет право на существование, однако в наших дальнейших рассмотрениях он создал бы почти непреодолимые технические сложности. Поэтому мы будем исходить из того, что в любой модели шифра типа

$$(\bar{X}, \bar{K}, \bar{Y}, \bar{E}, \bar{D})$$

правила зашифрования являются отображениями типа (2.1.11) для любого $\bar{k} \in \bar{K}$.

Еще одно соображение в пользу предложенной модели шифра с неограниченным ключом состоит в том, что мы избегаем введения распределений вероятностей на бесконечных множествах открытых текстов и ключей, что само по себе является проблемным вопросом.

Построим теперь модель шифра с ограниченным ключом.

Исходными предпосылками в этом построении служат опорный шифр Σ, введенный определением 2.1.1, конечное множество $\mathbf{K}$ ключей шифра и множество правил зашифрования

$$\{e_k : X^l \to Y^l,\ k \in \mathbf{K},\ l \in \mathbf{N}\}.$$

В определении действия e_k на открытом тексте длины l, так же как и для шифра с неограниченным ключом, используется ключевой поток

$$k_1, k_2, ..., k_l,\ k_i \in K,\ i = \overline{1,l},$$

где, по-прежнему, $K = \{0,1,...,n-1\}$ — множество номеров простых замен, входящих в опорный шифр. Отличие от шифра с неограниченным ключом состоит в том, что для шифра с ограниченным ключом ключевой поток детерминированно вычисляется по выбранному ключу $\kappa \in \mathbf{K}$.

Обозначим через K^* множество слов конечной длины в алфавите K.

Определение 2.1.4. *Пусть*

$$\psi : \mathbf{K} \times \mathbf{N} \to K^* \qquad (2.1.12)$$

— произвольное отображение, такое, что для любых $\kappa \in \mathbf{K}$, $l \in \mathbf{N}$, *и некоторых* $k_i \in K$, $i = \overline{1,l}$,

$$\psi(\kappa, l) = k_1 ... k_l,$$

причем

$$\{\psi(\kappa, 1),\ \kappa \in \mathbf{K}\} = K.$$

Назовем последовательность $k_1, ..., k_l$ *ключевым потоком, отвечающим ключу* κ *и числу* l, *а само отображение* ψ *— генератором ключевого потока (или просто генератором).*

Подчеркнем, что в определении 2.1.4 ключевой поток однозначно определяется выбором ключа $\kappa \in \mathbf{K}$ и числом l.

Далее мы введем последовательность моделей $\sum_{o}^{(l)}$, $l \in \mathbf{N}$. При этом будем исходить из некоторых априорных распределений $P(\mathbf{K})$ и $P(X^{(l)})$, $l \in \mathbf{N}$, не содержащих нулевых вероятностей. Существенное отличие от аналогич-

ной модели для шифра с неограниченным ключом состоит в том, что в качестве множества возможных ключевых потоков длины l мы рассматриваем не множество K^l, а множество

$$K^{(l)} = \{\psi(\kappa, l),\ \kappa \in \mathbf{K}\}.$$

Пусть для $\bar{k} = k_1 \ldots k_l \in K^l$

$$\mathbf{K}_l(\bar{k}) = \{\kappa \in \mathbf{K} : \psi(\kappa, l) = \bar{k}\}.$$

Введем распределение вероятностей $P(K^{(l)})$ так, что

$$p_{K^{(l)}}(\bar{k}) = \sum_{\kappa \in \mathbf{K}_l(\bar{k})} p_{\mathbf{K}}(\kappa). \qquad (2.1.13)$$

Определение 2.1.5. *Пусть*

$$\Sigma_{\mathrm{O}}^{(l)} = (\widetilde{X}^{(l)}, \widetilde{K}^{(l)}, \widetilde{Y}^{(l)}, E^{(l)}, D^{(l)}) \qquad (2.1.14)$$

— совокупность случайных величин $\widetilde{X}^{(l)}, \widetilde{K}^{(l)}, \widetilde{Y}^{(l)}$, правил зашифрования и расшифрования $E^{(l)}, D^{(l)}$, для которой распределение $P(K^{(l)})$ определяется формулой (2.1.13) *и выполняется условие*

$$P\{\widetilde{X}^{(l)} = \bar{x}\} > 0 \qquad (2.1.15)$$

при любых $\bar{x} \in X^{(l)}$.

Тогда шифром замены с ограниченным ключом назовем семейство

$$\Sigma_{\mathrm{O}} = (\Sigma_{\mathrm{O}}^{(l)},\ l \in \mathbf{N}). \qquad (2.1.16)$$

При этом совокупность (2.1.14) *будем называть* l*-м опорным шифром шифра* $\sum_{\text{О}}$.

Заметим, что для каждого $l \in \mathbf{N}$ множества $\mathbf{K}_l(\bar{k})$, $\bar{k} \in K^{(l)}$, образуют разбиение множества $\mathbf{K}$ на классы эквивалентных ключей, порождающих одинаковые ключевые потоки длины l. Поэтому представляется более резонным выбирать для зашифрования открытого текста длины l не столько ключ $\kappa \in \mathbf{K}$, сколько порождаемый этим ключом ключевой поток, т.е. использовать модель $\sum_{\text{О}}^{(l)}$ из совокупности (2.1.16).

Криптографические свойства шифра с ограниченным ключом определяются, в первую очередь, свойствами его генератора ключевого потока. Например, если

$$\psi(\kappa, l) = k' \ldots k'$$

для любого $\kappa \in \mathbf{K}$ и подходящего $k' \in K$, то получаем "слабый" шифр простой замены. Если

$$\psi(\kappa, l) = k_1 \ldots k_p k_1 \ldots k_p \ldots$$

представляет собой периодическую последовательность (в которой

$$\left|\{k_1, \ldots, k_p\}\right| \geq 2),$$

то получаем более стойкий периодический шифр замены. Таковым является, например, шифр Виженера.

После того как введены формальные определения шифров с ограниченным и неограниченным ключом, приведем ряд примеров.

Пример 2.1.6. *Шифр Цезаря (сдвиговый шифр).*

Данный шифр использует в качестве алфавита открытых текстов и одновременно множеств шифрвеличин и шифробозначений $\mathbf{Z}_n = \{0,1,...,n-1\}$. Число n — это число букв алфавита, например, русского или английского языка, в котором, для удобства, каждая буква заменена своим порядковым номером. Шифр использует n простых замен (правил зашифрования)

$$e_j : X \to Y, \quad j = \overline{0,n-1},$$

таких что

$$e_j(x) = (x + j) \bmod n, \tag{2.1.17}$$

и соответственно n правил расшифрования

$$d_j : Y \to X, \quad j = \overline{0,n-1},$$

таких что

$$d_j(y) = (y - j) \bmod n. \tag{2.1.18}$$

Таким образом, опорный шифр шифра Цезаря имеет вид

$$\Sigma = (\mathbf{Z}_n, \mathbf{Z}_n, \mathbf{Z}_n, E, D), \tag{2.1.19}$$

где

$$X = K = Y = \mathbf{Z}_n, \quad E = \{e_j, \ j \in \mathbf{Z}_n\}, \ D = \{d_j, \ j \in \mathbf{Z}_n\},$$

e_j определяется формулой (2.1.17), а d_j — формулой (2.1.18).

Шифр Цезаря — это шифр замены с ограниченным ключом, для которого $\mathbf{K} = \mathbf{Z}_n$. Генератором ключевого потока для него служит отображение

$$\psi : \mathbf{Z}_n \times \mathbf{N} \to \mathbf{Z}_n^*,$$

такое что

$$\psi(k, l) = \underbrace{k \ldots k}_{l \text{ раз}}.$$

Пусть распределение $P(X^{(l)})$ определяется частотными характеристиками языка, а распределение $P(\mathbf{K})$ положим, например, равномерным: $p_{\mathbf{K}}(\kappa) = 1/n$ для любого $\kappa \in \mathbf{Z}_n$.

Заметим, что для любого $l \in \mathbf{N}$

$$K^{(l)} = \{\underbrace{k \ldots k}_{l \text{ раз}},\ k \in \mathbf{Z}_n\},$$

и что для любого $\bar{k} \in K^{(l)}$

$$p_{K^{(l)}}(\bar{k}) = \frac{1}{n}.$$

Мы определили все компоненты модели Σ_{O} для шифра Цезаря. Обратим внимание на то, что потенциально шифр Цезаря (как и любой другой шифр простой замены) ничуть не хуже любого многоалфавитного шифра замены. Однако "плохой" генератор ключевого потока делает его сравнительно слабым шифром[9]. Это наглядно подтверждается следующим примером.

Пример 2.1.7. *Шифр модульного гаммирования с л.р.с. в качестве генератора.*

[9] Отметим, что блочный шифр простой замены, например, DES не так уж и слаб.

Опорный шифр данного шифра — тот же, что и для шифра Цезаря. В качестве множества $\mathbf{K}$ ключей шифра рассмотрим множество V_m, m-мерных ненулевых векторов с координатами из $\mathbf{Z}_n$, $m \in \mathbf{N}$. Таким образом, $|\mathbf{K}| = n^m - 1$. В качестве генератора используем линейный регистр сдвига (л.р.с.) длины m над кольцом $(\mathbf{Z}_n, +, \cdot)$ (рис. 1):

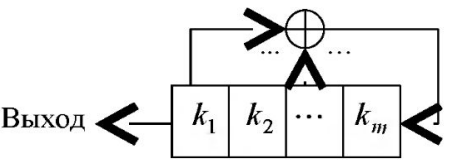


Рис. 1. Линейный регистр сдвига

Ключевой поток (который обычно называют *гаммой* применительно к рассматриваемому шифру) — это выходная последовательность регистра, т. е. *линейная рекуррентная последовательность*[10] с начальным вектором $K = (k_1, \ldots, k_m)$ и характеристическим многочленом, определяемым выбором обратных связей регистра.

Не вдаваясь в детали, заметим, что при правильном выборе параметров регистра сдвига рассматриваемый шифр будет использовать при зашифровании открытого текста не одну (как шифр простой замены), а все n простых замен (2.1.17). Поэтому такой шифр значительно более стоек, чем любой (поточный) шифр простой замены.

Пример 2.1.8. *Шифр модульного гаммирования со случайной гаммой.*

[10] См., например, [Алф01].

Опорный шифр рассматриваемого шифра — тот же, что и в предыдущих примерах. Генератор ключевого потока (гаммы шифра) позаимствуем из [Неч99], это — *"вертушка со стрелкой"* (рис. 2).

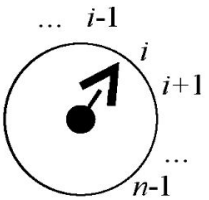


Рис. 2. Вертушка со стрелкой

Обод вертушки разделен на n равных частей (дуг). Каждая из них помечена числами от 0 до $n-1$. Запуская вертушку, получим какое-нибудь число из $\mathbf{Z}_n$. Для того чтобы получить ключевой поток длины l, нужно l раз воспользоваться вертушкой. Если она — "правильная", то

$$P(K^{(l)}) = \{p_{K^{(l)}}(\bar{k}) = 1/n^l,\ \bar{k} \in \mathbf{Z}_n^l\}$$

для любого $l \in \mathbf{N}$.

Мы построили пример случайного шифра.

В приведенных примерах множества шифрвеличин и шифробозначений совпадали с алфавитом открытых текстов. Однако так бывает далеко не всегда. Для блочных шифров, например для DES, множеством шифрвеличин служит множество всех возможных блоков некоторой длины. Надеемся, что примеры моделей подобных шифров читатель сможет построить самостоятельно.

§ 2.2. Шифры, совершенные по К. Шеннону

В данном параграфе под шифром мы будем понимать введенную в §2.1 модель шифра замены с ограниченным или с неограниченным ключом.

Введем понятие совершенного шифра. Для этого нам потребуются условные вероятности

$$p_{X^{(l)}/Y^{(l)}}(\bar{x}/\bar{y}) \quad \text{и} \quad p_{Y^{(l)}/X^{(l)}}(\bar{y}/\bar{x}),$$

для $\bar{x} \in X^{(l)}$, $\bar{y} \in Y^{(l)}$, $l \in \mathrm{N}$ [11].

Как мы знаем из § 2.1, имеет смысл рассматривать такие вероятности лишь для $\bar{x}, \bar{y}$, имеющих одинаковые длины[12], так как ни при каких обстоятельствах открытый текст не будет зашифрован в шифрованный текст другой длины.

Пусть

$$\bar{x} = x_1 \ldots x_l \in X^{(l)}, \quad \bar{y} = y_1 \ldots y_l \in Y^{(l)}.$$

Для шифра с ограниченным ключом вероятность $p_{Y^{(l)}/X^{(l)}}(\bar{y}/\bar{x})$ вычисляется по формуле

$$p_{Y^{(l)}/X^{(l)}}(\bar{y}/\bar{x}) = \sum_{\bar{k} \in K^{(l)}(\bar{x},\bar{y})} p_{K^{(l)}}(\bar{k}), \qquad (2.2.1)$$

если $K^{(l)}(\bar{x},\bar{y}) \neq \varnothing$, и полагается равной нулю, если $K^{(l)}(\bar{x},\bar{y}) = \varnothing$, где

---

[11] Множества $X^{(l)}$ и $Y^{(l)}$ определены в § 2.1.

[12] В алфавитах X и Y соответственно.

$$K^{(l)}(\bar{x},\bar{y}) = \{\bar{k} \in K^{(l)} : e_{k_i}(x_i) = y_i,\ i = \overline{1,l}\},$$

а $p_{K^{(l)}}(\bar{k})$ определяется формулой (2.1.13). При этом распределение вероятностей $P(K^{(l)})$ определяется через априорное распределение $P(\mathrm{K})$ на множестве ключей шифра по формуле (2.1.14).

Для шифра с неограниченным ключом соответствующая вероятность вычисляется по формуле

$$p_{Y^{(l)}/X^{(l)}}(\bar{y}/\bar{x}) = \sum_{\bar{k} \in K^l(\bar{x},\bar{y})} p_{K^l}(\bar{k}), \qquad (2.2.1')$$

если $K^l(\bar{x},\bar{y}) \neq \varnothing$, и полагается равной нулю, если $K^l(\bar{x},\bar{y}) = \varnothing$, где

$$K^l(\bar{x},\bar{y}) = \{\bar{k} \in K^l : e_{k_i}(x_i) = y_i,\ i = \overline{1,l}\},$$

а $P(K^l)$ — априорное распределение вероятностей на K^l.

Вероятность $p_{X^{(l)}/Y^{(l)}}(\bar{x}/\bar{y})$ вычисляется стандартным образом:

$$p_{X^{(l)}/Y^{(l)}}(\bar{x}/\bar{y}) = \frac{p_{X^{(l)}}(\bar{x}) \cdot p_{Y^{(l)}/X^{(l)}}(\bar{y}/\bar{x})}{p_{Y^{(l)}}(\bar{y})}. \qquad (2.2.2)$$

Определение 2.2.1. *Шифр называется совершенным*[13], *если для любых* $\bar{x} \in X^{(l)}$, $\bar{y} \in Y^{(l)}$ *и любого натурального числа* l *выполняется равенство*

[13] Точнее было бы назвать шифр совершенным по К. Шеннону.

$$p_{X^{(l)}/Y^{(l)}}(\bar{x}/\bar{y}) = p_{X^{(l)}}(\bar{x})\ ^{14)}. \qquad (2.2.3)$$

Часто бывает удобнее пользоваться эквивалентным определением совершенного шифра, которое состоит в условии

$$p_{Y^{(l)}/X^{(l)}}(\bar{y}/\bar{x}) = p_{Y^{(l)}}(\bar{y}). \qquad (2.2.4)$$

Покажем, что совершенным может быть лишь шифр с неограниченным ключом, и критерием совершенности для такого шифра является свойство совершенности составляющих его опорных шифров.

В следующем утверждении мы используем обозначение $K_l(\bar{x},\bar{y})$ для множества $K^{(l)}(\bar{x},\bar{y})$, если рассматривается шифр с ограниченным ключом, и для множества $K^{l}(\bar{x},\bar{y})$, если рассматривается шифр с неограниченным ключом.

Утверждение 2.2.2. *Если шифр является совершенным, то для любых* $\bar{x}\in X^{(l)}$, $\bar{y}\in Y^{(l)}$ *и любого натурального числа* l *выполняется неравенство*

$$\left|K_l(\bar{x},\bar{y})\right| \geq 1. \qquad (2.2.5)$$

Доказательство. Предположим противное: пусть $\left|K_l(\bar{x},\bar{y})\right| = 0$ при некоторых $\bar{x}\in X^{(l)}$, $\bar{y}\in Y^{(l)}$. Тогда, согласно (2.2.1) (или (2.2.1′)), мы бы имели равенство

$$p_{Y^{(l)}/X^{(l)}}(\bar{y}/\bar{x}) = 0,$$

[14)] Условие (2.2.3) эквивалентно тому, что $\widetilde{X}^{(l)}$ и $\widetilde{Y}^{(l)}$ являются независимыми случайными величинами.

а согласно (2.2.2), и равенство

$$p_{X^{(l)}/Y^{(l)}}(\bar{x}/\bar{y}) = 0.$$

Из (2.2.3) следует, что вероятность $p_{X^{(l)}}(\bar{x})$ также оказывается равной нулю, вопреки условию (2.1.9).

Утверждение 2.2.3. *Шифр с ограниченным ключом не является совершенным.*

Доказательство. Если зафиксировать $\bar{x} \in X^{(l)}$ и заставить $\bar{y}$ пробегать все множество $Y^{(l)}$, то (согласно утверждению 2.2.2) должен существовать ключ $\bar{k} \in K^{(l)}$ такой, что $e_{\bar{k}}(\bar{x}) = \bar{y}$. Поэтому для совершенного шифра

$$\left|K^{(l)}\right| \geq \left|Y^{(l)}\right|,$$

что невозможно для любого $l \in \mathrm{N}$, поскольку

$$\left|K^{(l)}\right| \leq |\mathrm{K}|,$$

где $|\mathrm{K}|$ — константа, а

$$\left|Y^{(l)}\right| \geq \left|X^{(l)}\right|.$$

Последнее неравенство, а также условие (2.1.6), означает, что с ростом l величина $\left|Y^{(l)}\right|$ неограниченно растет.

Итак, совершенными могут быть лишь шифры с неограниченным ключом. Более того, непосредственно из определений 2.1.3 и 2.2.1 следует

Утверждение 2.2.4. *Шифр* $\Sigma_{\text{Н}}$ *с неограниченным ключом является совершенным шифром тогда и только тогда, когда его* l*-й опорный шифр* $\Sigma_{\text{Н}}^{(l)}$ *является совершенным шифром при любом* $l \in \text{N}$.

Это утверждение позволяет нам при изучении свойств совершенных шифров рассматривать лишь их опорные шифры. В связи с этим далее мы будем понимать под *шифром* совокупность

$$\Sigma_{\text{В}} = (\widetilde{X}, \widetilde{K}, \widetilde{Y}, E, D)\ ^{15)}, \qquad (2.2.6)$$

состоящую из случайных величин $\widetilde{X}, \widetilde{K}, \widetilde{Y}$, заданных на конечных множествах X — открытых текстов, K — ключей и Y — шифрованных текстов соответственно введением априорных распределений вероятностей

$$P(X) = \{p_X(x) > 0,\ \ x \in X\},$$

$$P(K) = \{p_K(k) > 0,\ \ k \in K\};$$

при этом $|X| > 1,\ |Y| > 1,\ |K| > 1$; а также множеств E — правил зашифрования $e_k : X \to Y$, и D — правил расшифрования $d_k : e_k(X) \to X$, для каждого $k \in K$, для которых выполняются соотношения

[15)] Индекс "В" в обозначении модели указывает на ее вероятностный характер.

$$d_k(e_k(x)) = x,$$

при любых $x \in X$, $k \in K$, и

$$Y = \mathop{\mathbf{Y}}_{k \in K} e_k(X).$$

Случайные величины $\widetilde{X}$ и $\widetilde{K}$ полагаем независимыми.

Перейдем к изучению модели шифра Σ_{B}.

Прежде всего, нам придется повторить некоторые соотношения, которые уже приводились выше в другой форме.

Аналогично (2.1.5) для модели Σ_{B} вероятность $p_Y(y)$ вычисляется по формуле

$$p_Y(y) = \sum_{\substack{(x,k) \in X \times K: \\ e_k(x) = y}} p_X(x) \cdot p_K(k). \qquad (2.2.7)$$

Заметим, что из общих соображений следует равенство

$$\sum_{y \in Y} p_Y(y) = 1,$$

которое полезно проверить и непосредственно. Для этого рассмотрим отображение $f : X \times K \to Y$, определенное условием $f(x,k) = e_k(x)$ или, иначе, $f\big|_{X \times \{k\}} = e_k$ для любого $k \in K$. Тогда, поскольку $f^{-1}(Y) = X \times K$,

$$\sum_{y \in Y} p_Y(y) = \sum_{y \in Y} \sum_{(x,k) \in f^{-1}(y)} p_X(x) \cdot p_K(k) =$$

$$= \sum_{(x,k)\in X\times K} p_X(x)\cdot p_K(k) = \sum_{x\in X}\sum_{k\in K} p_X(x)\cdot p_K(k) =$$

$$= \sum_{x\in X} p_X(x)\cdot \sum_{k\in K} p_K(k) = 1.$$

Условная вероятность $p_{Y/X}(y/x)$ вычисляется по формуле

$$p_{Y/X}(y/x) = \begin{cases} \sum\limits_{k\in K(x,y)} p_K(k), & K(x,y)\neq\varnothing, \\ 0, & K(x,y)=\varnothing, \end{cases} \qquad (2.2.8)$$

где

$$K(x,y) = \{k\in K : e_k(x) = y\}.$$

Далее, с целью упрощения записи, нижние индексы в обозначениях

$$p_X(x),\ p_K(k),\ p_Y(y),\ p_{Y/X}(y/x),\ p_{X/Y}(x/y),$$

будем опускать, и записывать их в виде

$$p(x),\ p(k),\ p(y), p(y/x),\ p(x/y),$$

соответственно, если понятно, о каком распределении идет речь.

Отметим одно очевидное свойство совершенного шифра (которым мы уже неявно пользовались).

Утверждение 2.2.5. *Если шифр* Σ_{B} *— совершенный, то справедливы неравенства*

$$|X| \le |Y| \le |K|. \qquad (2.2.9)$$

Доказательство. Первое неравенство, очевидно, имеет место для любого шифра (2.2.6). Если шифр — совершенный, то, согласно доказательству утверждения 2.2.2, $|K(x, y)| \geq 1$ [16]. Поэтому для любого $x \in X$ выполняется равенство

$$\{e_k(x),\ k \in K\} = Y, \tag{2.2.10}$$

и поэтому $|Y| \leq |K|$.

В большинстве случаев применяемые на практике шифры обладают свойством $X = Y$. Следуя К. Шеннону, назовем такие шифры *эндоморфными*. К. Шеннону удалось полностью описать эндоморфные совершенные шифры с минимально возможным числом ключей. Согласно (2.2.9), это минимально возможное число ключей $|K|$ не меньше $|Y|$. В несколько более общей форме теорема формулируется следующим образом.

Теорема 2.2.6 (К. Шеннона). *Пусть* Σ_{B} — *шифр, для которого* $|X| = |Y| = |K|$. *Тогда* Σ_{B} — *совершенный шифр тогда и только тогда, когда выполняются два условия:*

(i) $|K(x, y)| = 1$ *для любых* $x \in X$, $y \in Y$;

(ii) *Распределение* $P(K)$ — *равномерно, то есть* $p(k) = 1/|K|$ *для любого ключа* $k \in K$.

Доказательство. Пусть шифр Σ_{B} — совершенный. Тогда, согласно (2.2.10),

$$|\{e_k(x),\ k \in K\}| = |Y| = |K|.$$

[16] Шифр, удовлетворяющий этому условию, будем называть *транзитивным шифром*.

Поэтому из неравенства $k_1 \neq k_2$ следует неравенство $e_{k_1}(x) \neq e_{k_2}(x)$ для любого $x \in X$. Это доказывает необходимость условия (i).

Пусть $X = \{x_1, ..., x_N\}$. Зафиксируем произвольный элемент $y \in Y$ и занумеруем ключи так, чтобы $e_{k_j}(x_j) = y$, $j = \overline{1, N}$. Тогда

$$p(x_j / y) = \frac{p(y / x_j) \cdot p(x_j)}{p(y)} = \frac{p(k_j) \cdot p(x_j)}{p(y)}. \quad (2.2.11)$$

Так как Σ_B — совершенный шифр, то $p(x_j / y) = p(x_j)$. Отсюда и из (2.2.11) получаем равенство $p(k_j) = p(y)$ для любого $j = \overline{1, N}$, которое доказывает необходимость условия (ii).

Пусть условия (i) и (ii) выполнены. Тогда, пользуясь для фиксированного элемента $y \in Y$ введенной выше нумерацией ключей, имеем, на основании (2.2.7), цепочку равенств:

$$p(y) = \sum_{\substack{(x_j, k_j): \\ e_{k_j}(x_j) = y}} p(x_j) \cdot p(k_j) \underset{\text{усл. (ii)}}{=} \frac{1}{N} \cdot \sum_{j=1}^{N} p(x_j) = \frac{1}{N},$$

откуда

$$p(x_j / y) = \frac{p(x_j) \cdot p(y / x_j)}{p(y)} \underset{\text{усл. (i),(ii)}}{=} p(x_j).$$

Достаточность условий теоремы также доказана.

Сделаем ряд замечаний. Во-первых, обратим внимание на то, что *матрица зашифрования* шифра, удовлетворяющего условиям теоремы Шеннона, согласно условию (i) этой теоремы, является *латинским квадратом*[17].

Матрица зашифрования

$K \backslash X$	x_1	.....	x_N
k_1	$e_{k_1}(x_1)$	.....	$e_{k_1}(x_N)$
.....	.....	.....	.....
k_N	$e_{k_N}(x_1)$	.....	$e_{k_N}(x_N)$

Поэтому в случае, когда $X = Y = K$, совершенными являются шифры табличного гаммирования (см. 2.2.7) со случайной равновероятной гаммой, и только они.

Отметим, что число $L(n,n)$ латинских квадратов произвольного порядка n до сих пор неизвестно. Приведем некоторые сведения об этом числе ([Рио63]). Если l_n — число латинских квадратов, в которых элементы первой строки и первого столбца записаны в естественном порядке, то

$$L(n,n) = n! \cdot (n-1)! \cdot l_n.$$

Ряд известных значений l_n сведем в таблицу:

[17] Так называется квадратная таблица, строки и столбцы которой являются перестановками элементов данного множества. Отметим, что понятие латинского квадрата было введено Л. Эйлером, который впервые их исследовал, беря за основу латинский алфавит (или несколько его первых букв).

n	2	3	4	5	6	7
l_n	1	1	4	56	9408	16942080

Укажем, например, все латинские квадраты размера 4×4 (с упорядоченной первой строкой):

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

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

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

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

Определение 2.2.7. *Пусть L — латинский квадрат на произвольном упорядоченном множестве A, $|A| \geq 2$. Пусть строки и столбцы квадрата L занумерованы элементами из A. Шифром табличного гаммирования называется шифр, с ограниченным или с неограниченным ключом, для которого матрица зашифрования опорного шифра совпадает с L.*

Понятие шифра табличного гаммирования обобщает общепринятое понятие шифра гаммирования, который исторически определялся латинским квадратом, представляющим

собой таблицу Виженера. С алгебраической точки зрения латинский квадрат на A является *таблицей Кэли* квазигруппы $(A,*)$ [18]. Поэтому правило зашифрования опорного шифра можно записать также в виде

$$e_k(x) = x * k. \tag{2.2.12}$$

В случае когда $(A,*) = (\mathbf{Z}_n,+)$, шифр совпадает с шифром *модульного гаммирования*, для которого

$$e_k(x) = (x + k) \bmod n. \tag{2.2.13}$$

Отметим, что определение совершенного шифра было рассмотрено К. Шенноном применительно к *фиксированному* распределению $P(X)$, отвечающему частотным характеристикам реального языка. Как нетрудно видеть, утверждение теоремы 2.2.6 остается справедливым для любого распределения $P(X)$. В связи с этим в некоторых работах по криптографии (например, [Mas87]) вводят следующее определение.

Определение 2.2.8. *Шифр* Σ_{B} *называется сильно совершенным, если он остается совершенным для любого распределения* $P(X)$.

Нам понадобится еще одно определение.

---

[18] Квазигруппа – это группоид $(A,*)$ (т. е. множество с операцией), в котором для любых $a, b \in A$ однозначно разрешимы уравнения $a * x = b$ и $y * a = b$.

Определение 2.2.9. *Транзитивный шифр* Σ_{B}, *удовлетворяющий условию* $|X| = |Y| = |K|$, *называется минимальным шифром.*

Предыдущее замечание свидетельствует о том, что в теореме 2.2.6 слова "совершенный шифр" можно заменить словами "сильно совершенный шифр". Таким образом, теорема 2.2.6 дает описание минимальных сильно совершенных шифров. Однако, как мы убедимся далее (теорема 4.2.11), определение 2.2.8 излишне, так как совершенный шифр является также и сильно совершенным.

Еще одно замечание связано с тем, что в матрице зашифрования переменные x и k можно заменить друг на друга. После такой замены будет рассматриваться шифр с транспонированной матрицей зашифрования (которая остается латинским квадратом). Кроме того, из условий теоремы 2.2.6 следует, что и переменные x и y также взаимозаменяемы. Это свойство наглядно проявляется на примере шифра Вернама, определяемого правилом зашифрования (2.2.13) при $n = 2$. Таким образом, в теореме Шеннона все переменные взаимозаменяемы, то есть каждое из множеств X, K, Y может служить как множеством открытых текстов, так и множеством ключей или множеством шифрованных текстов сильно совершенного шифра.

Подчеркнем также, что не только указанные шифры являются совершенными по Шеннону. В качестве примера можно указать следующий неэндоморфный шифр с неравновероятными ключами, являющийся сильно совершенным.

Пример 2.2.10

$$X = \{x_1, x_2\},\ Y = \{1,2,3\},\ K = \{k_1, \ldots, k_6\}.$$

Матрица зашифрования имеет следующий вид:

$K \diagdown X$	x_1	x_2
k_1	1	2
k_2	1	3
k_3	2	1
k_4	2	3
k_5	3	1
k_6	3	2

Вероятности ключей:

$$p(k_1) = 19/80, \quad p(k_2) = 3/20, \quad p(k_3) = 21/80,$$
$$p(k_4) = 1/10, \quad p(k_5) = p(k_6) = 1/8.$$

§ 2.3. Имитостойкие совершенные шифры

Приведем ряд результатов о совершенных шифрах с наилучшими параметрами *имитостойкости*. К таким параметрам обычно относят *вероятности имитации* — p_0 и *вероятность подмены* — p_1. Эти вероятности определяются следующим образом.

При попытке имитации противником шифрованного сообщения $y \in Y$ в случае, когда по каналу связи ничего не передается, это сообщение будет воспринято получателем как аутентичное с вероятностью

$$\sum_{k \in K(y)} p(k),$$

где

$$K(y) = \{k \in K : \exists x \in X\ (e_k(x) = y)\}.$$

Обозначим эту вероятность через $\tilde{p}(y)$.

Шансы на успех в попытке имитации для противника, использующего оптимальную стратегию, определяются величиной

$$\max_{y \in Y} \tilde{p}(y).$$

Эта величина обозначается p_0 и называется вероятностью имитации.

Успех противника при попытке подмены передаваемого шифрованного сообщения $y \in Y$ на отличное от него сообщение $y' \in Y$ характеризуется вероятностью $\tilde{p}(y, y')$ события, состоящего в том, что при расшифровании криптограммы y' на действующем ключе будет получено осмысленное сообщение. Эта вероятность $\tilde{p}(y, y')$ определяется формулой

$$\tilde{p}(y, y') = \frac{\sum\limits_{k \in K(y, y')} p(k) \cdot p_X(d_k(y))}{\sum\limits_{k \in K(y)} p(k) \cdot p_X(d_k(y))},$$

где

$$K(y, y') = K(y) \cap K(y').$$

Наибольшие шансы на успех для противника определяются вероятностью

$$\hat{p}(y) = \max\{\tilde{p}(y, y') : y' \in Y,\ y' \neq y\}.$$

Усредняя эту вероятность по всевозможным сообщениям $y \in Y$, полагаем по определению

$$p_1 = \sum_{y \in Y} p_Y(y) \cdot \tilde{p}(y).$$

Введем обозначения $|X| = \lambda$, $|Y| = \mu$, $|K| = \pi$ для основных параметров шифра Σ_{B}.

Теорема 2.3.1. *Для любого шифра* Σ_{B} *справедливо неравенство*

$$p_0 \geq \frac{\lambda}{\mu}. \tag{2.3.1}$$

Равенство в (2.3.1) *имеет место тогда и только тогда, когда для любого* $y \in Y$ *выполняется соотношение*

$$\sum_{k \in K(y)} p(k) = \lambda / \mu.$$

Доказательство. Справедливы следующие равенства:

$$\sum_{y \in Y} \tilde{p}(y) = \sum_{y \in Y} \sum_{k \in K(y)} p(k) = \sum_{k \in K} p(k) \cdot \lambda = \lambda.$$

В самом деле, любой открытый текст может быть зашифрован на любом ключе. Поэтому в двойной сумме каждый ключ учитывается ровно λ раз. Сумма

$$\sum_{y \in Y} \tilde{p}(y)$$

(равная λ) содержит μ слагаемых, поэтому максимальное слагаемое не может быть меньше λ/μ, откуда следует неравенство (2.3.1). Ясно также, что равенство $p_0 = \lambda/\mu$ выполняется лишь в случае, если $\tilde{p}(y) = \lambda/\mu$ для любого $y \in Y$.

Теорема 2.3.2. *Для любого шифра* Σ_{B} *справедливо неравенство*

$$p_1 \geq \frac{\lambda - 1}{\mu - 1}. \tag{2.3.2}$$

Равенство в (2.3.2) *имеет место тогда и только тогда, когда для любых* $y, y' \in Y$, $y' \neq y$, *выполняется соотношение*

$$\frac{\sum\limits_{k \in K(y,y')} p(k) \cdot p(d_k(y))}{p(y)} = \frac{\lambda - 1}{\mu - 1}. \tag{2.3.3}$$

Доказательство. Из цепочки равенств

$$\sum_{y' \neq y} \tilde{p}(y, y') = \frac{1}{p(y)} \sum_{y' \neq y} \sum_{k \in K(y,y')} p(k) \cdot p(d_k(y)) =$$

$$= \frac{1}{p(y)} \sum_{k \in K(y)} p(k) \cdot p(d_k(y)) \cdot (\lambda - 1) = \frac{p(y)}{p(y)} (\lambda - 1) = \lambda - 1$$

следует, что для любого $y \in Y$ имеет место равенство

$$\sum_{y' \neq y} \tilde{p}(y, y') = \lambda - 1. \qquad (2.3.4)$$

При этом мы воспользовались тем, что в двойной сумме каждый ключ из $K(y)$ учитывается ровно $\lambda - 1$ раз (столько имеется шифрованных текстов $y' \neq y$).

Сумма (2.3.4) (равная $\lambda - 1$) состоит из $\mu - 1$ слагаемых. Поэтому максимальное слагаемое не может быть меньше $(\lambda - 1)/(\mu - 1)$. Следовательно,

$$\hat{p}(y) \geq (\lambda - 1)/(\mu - 1), \qquad (2.3.5)$$

и

$$p_1 = \sum_{y \in Y} p(y) \cdot \hat{p}(y) \geq (\lambda - 1/\mu - 1) \cdot \sum_{y \in Y} p(y) = (\lambda - 1)/(\mu - 1),$$

откуда мы получаем (2.3.2).

Пусть $p_1 = (\lambda - 1)/(\mu - 1)$. Если для некоторого $y_0 \in Y$

$$\hat{p}(y_0) > (\lambda - 1)/(\mu - 1),$$

то, в силу (2.3.5), выполнялись бы соотношения

$$p_1 = \sum_{y \in Y} p(y) \cdot \hat{p}(y) > (\lambda - 1/\mu - 1) \cdot \sum_{y \in Y} p(y) = (\lambda - 1)/(\mu - 1),$$

вопреки условию. Тем самым,

$$\hat{p}(y) = (\lambda - 1)/(\mu - 1)$$

для любого $y \in Y$, и поэтому

$$\tilde{p}(y, y') \leq (\lambda - 1)/(\mu - 1) \qquad (2.3.6)$$

для любых $y, y' \in Y$.

Если для некоторых $y, y' \in Y$ выполнялось бы строгое неравенство

$$\tilde{p}(y, y') < (\lambda - 1)/(\mu - 1),$$

то, в силу (2.3.6), это привело бы к неравенству

$$\sum_{y' \neq y} \tilde{p}(y, y') < \lambda - 1,$$

вопреки (2.3.4). Таким образом,

$$\tilde{p}(y, y') = (\lambda - 1)/(\mu - 1)$$

при любых y, $y' \in Y$, что и требуется.

Представляют интерес совершенные шифры с минимальным числом ключей, для которых вероятности p_0, p_1 минимальны. Имеет место следующий результат ([Sti88]), для формулировки которого нам понадобится определить еще одно понятие.

Определение 2.3.3. *$t-(\mu, \lambda, \sigma)$-схемой называется совокупность B подмножеств (называемых блоками) множества Y, состоящего из μ элементов, такая, что каждое подмножество из B содержит λ элементов, а всякое подмножество множества Y из t элементов содержится ровно в σ подмножествах из B. При $\sigma = 1$ схема называется штейнеровой системой.*

Теорема 2.3.4. *Если для шифра* $\sum_{\text{B}}$ *выполняется равенство* $p_1 = (\lambda - 1)/(\mu - 1)$, *то*

$$\pi \geq \frac{\mu^2 - \mu}{\lambda^2 - \lambda}. \tag{2.3.7}$$

Равенство в (2.3.7) *имеет место тогда и только тогда, когда строки матрицы зашифрования, рассматриваемые как подмножества элементов из* Y, *образуют* $2-(\mu, \lambda, 1)$-*схему. Если при этом* $p_0 = \lambda/\mu$, *то распределения* $P(X)$ *и* $P(K)$ — *равномерные.*

Доказательство. Из условия и теоремы 2.3.2 следует, что выполняется равенство (2.3.3), откуда $|K(y, y')| > 1$ для любых шифртекстов y, y', $y' \neq y$.

Очевидно, что для любых различных упорядоченных пар открытых текстов $(x_1, x_1'), (x_2, x_2')$ верно соотношение

$$K(x_1, x_1'; y, y') \cap K(x_2, x_2'; y, y') = \varnothing,$$

где

$$K(x, x'; y, y') = \{k \in K : e_k(x) = y, e_k(x') = y'\}.$$

Тогда, с одной стороны,

$$\sum_{y, y' \neq y} \sum_{x, x' \neq x} |K(x, x'; y, y')| = \sum_{y, y' \neq y} \left| \bigcup_{x, x' \neq x} K(x, x'; y, y') \right| =$$

$$= \sum_{y, y' \neq y} |K(y, y')| \geq \mu(\mu - 1).$$

С другой стороны, поскольку

$$K(x,x';y_1,y_1')\,\mathrm{I}\;K(x,x';y_2,y_2')=\varnothing$$

для любых различных пар $(y_1,y_1'),(y_2,y_2')$,

$$\sum_{y,y'\neq y}\;\sum_{x,x'\neq x}\left|K(x,x';y,y')\right|=\sum_{x,x'\neq x}\;\sum_{y,y'\neq y}\left|K(x,x';y,y')\right|=$$

$$=\sum_{x,x'\neq x}\left|\;\mathrm{Y}_{y,y'\neq y}\;K(x,x';y,y')\right|=\sum_{x,x'\neq x}|K|=(\lambda^2-\lambda)\pi.$$

Таким образом, $(\lambda^2-\lambda)\pi\geq\mu^2-\mu$, откуда следует (2.3.7).

Рассмотрим семейство B множеств шифртекстов, содержащихся в строках матрицы зашифрования. Каждое множество этого семейства имеет мощность λ. Число множеств семейства B, содержащих выбранные шифртексты y и y', равно $\left|K(y,y')\right|$. Поэтому равенство

$$(\lambda^2-\lambda)\pi=\sum_{y,y'\neq y}\left|K(y,y'\right|=\mu^2-\mu$$

возможно в том и только том случае, когда для любых y и $y'\neq y$, $\left|K(y,y')\right|=1$. Это равносильно тому, что пара (Y,B) является $2-(\mu,\lambda,1)$-схемой.

Установим теперь равномерность распределений $P(X)$ и $P(K)$. Так как $p_1=(\lambda-1)/(\mu-1)$, то, согласно (2.3.3), для любых y, y', y'', $y'\neq y$, $y''\neq y$,

$$\sum_{k\in K(y,y')} p(k)\cdot p(d_k(y)) = \sum_{k\in K(y,y'')} p(k)\cdot p(d_k(y)). \quad (2.3.8)$$

Как отмечено выше,

$$|K(y,y')| = |K(y,y'')| = 1.$$

Поэтому если $e_k(x) = e_{k'}(x') = y$, то из (2.3.8) следует, что

$$p(k)\cdot p(x) = p(k')\cdot p(x').$$

Это означает, что в сумме

$$p(y) = \sum_{k\in K(y)} p(k)\cdot p(d_k(y))$$

все слагаемые одинаковы. Выделяя одно из них, получаем равенство

$$p(y) = p(k)\cdot p(x)\cdot |K(y)|,$$

из которого

$$p(k)\cdot p(x) = \frac{p(y)}{|K(y)|}. \quad (2.3.9)$$

Величина $|K(y)|$ есть число блоков построенной $2-(\mu,\lambda,1)$-схемы, содержащих y. Известно ([Хол70]), что это число не зависит от y и равно

$$|K(y)| = \frac{\mu-1}{\lambda-1}.$$

Отсюда и из (2.3.9) получаем в случае, когда $e_k(x) = y$, формулу

$$p(k) = \left(\sum_{x \in X} p(x) \right) p(k) = \sum_{x \in X} p(x) \cdot p(k) = \\ = \sum_{y \in e_k(X)} \frac{p(y)(\lambda - 1)}{\mu - 1}. \tag{2.3.10}$$

Зафиксируем $y_0 \in Y$ и воспользуемся условием $p_0 = \lambda / \mu$. Согласно теореме 2.3.1 и равенству (2.3.10),

$$\frac{\lambda}{\mu} = \sum_{k \in K(y_0)} p(k) = \\ = \sum_{k \in K(y_0)} \sum_{y \in e_k(X)} \frac{p(y)(\lambda - 1)}{\mu - 1} = \\ = \frac{\lambda - 1}{\mu - 1} \sum_{y \in Y} \sum_{k \in K(y, y_0)} p(y) = \\ = \frac{\lambda - 1}{\mu - 1} \cdot \left[\sum_{y \neq y_0} p(y) + \left| K(y_0) \right| \cdot p(y_0) \right] = \\ = \frac{\lambda - 1}{\mu - 1} \cdot \left[1 - p(y_0) + \frac{\lambda - 1}{\mu - 1} \cdot p(y_0) \right] = \tag{2.3.11}$$

$$= \frac{\lambda - 1}{\mu - 1} - p(y_0) \cdot \frac{\lambda - 1}{\mu - 1} + p(y_0) =$$

$$= \frac{\lambda - 1}{\mu - 1} + p(y_0)\left(1 - \frac{\lambda - 1}{\mu - 1}\right).$$

В этой цепочке равенств мы воспользовались тем, что

$$\left|K(y, y_0)\right| = 1 \text{ и } \sum_{y \in Y} p(y) = 1.$$

Переход от одной двойной суммы к другой объясняется тем, что в строках матрицы зашифрования, отвечающих ключам из $K(y_0)$, должен встретиться любой элемент $y \in Y$. Последнее обстоятельство опять-таки следует из того, что $\left|K(y, y_0)\right| = 1$.

Из соотношения (2.3.11) находим $p(y_0) = 1/\mu$. Учитывая, что y_0 выбиралось произвольно, и, подставляя значение $p(y_0)$ в (2.3.11), получаем для любого $k \in K$

$$p(k) = \frac{\lambda - 1}{\mu - 1} = \frac{1}{\pi}.$$

Наконец, с учетом (2.3.9), для любого $x \in X$

$$p(x) = \sum_{k \in K} p(k) \cdot p(x) = \sum_{k \in K} \frac{p(y)}{|K(y)|} = \sum_{k \in K} \frac{\lambda - 1}{\mu(\mu - 1)} =$$

$$= \frac{\pi(\lambda - 1)}{\mu^2 - \mu} = \frac{(\mu^2 - \mu)(\lambda - 1)}{(\lambda^2 - \lambda)(\mu^2 - \mu)} = \frac{1}{\lambda}.$$

Теорема 2.3.5. *Если существует* $2-(\mu,\lambda,1)$*-схема, то существует и шифр* $\sum_{\mathrm{B}}$*, для которого*

$$p_0 = \lambda/\mu, \quad p_1 = (\lambda - 1)/(\mu - 1), \quad \pi = (\mu^2 - \mu)/(\lambda^2 - \lambda),$$

и распределения $P(X), P(K)$ *— равномерные.*

Доказательство. Пусть пара (Y,B) является $2-(\mu,\lambda,1)$-схемой. Пусть X — произвольное множество из λ элементов. Каждому множеству Z семейства B поставим в соответствие отображение

$$e_Z : X \to Y$$

так, что $e_Z(X) = Z$.

Пусть $K = \{e_Z : Z \in B\}$. Зададим на X, K равномерные распределения вероятностей и рассмотрим произвольный шифр $\sum_{\mathrm{B}}$, определенный таким образом.

Число блоков в (Y,B) равно $\pi = (\mu^2 - \mu))/(\lambda^2 - \lambda)$, каждый элемент $y \in Y$ содержится ровно в $(\mu - 1)/(\lambda - 1)$ блоках. Отсюда следует, что для любого $y \in Y$

$$\sum_{k\in K(y)} p(k) = \frac{\mu-1}{\lambda-1}\cdot\frac{1}{\pi} = \frac{\lambda}{\mu}.$$

По теореме 2.3.1 получаем равенство $p_0 = \lambda/\mu$.

В $2-(\mu,\lambda,1)$-схеме любая пара (y,y') содержится лишь в одном блоке, поэтому $|K(y,y')| = 1$. Отсюда получаем:

$$\frac{\sum\limits_{k\in K(y,y')} p(k)\cdot p(d_k(y))}{\sum\limits_{k\in K(y)} p(k)\cdot p(d_k(y))} = \frac{1/\pi\cdot 1/\lambda}{1/\pi\cdot 1/\lambda\cdot|K(y)|} = \frac{\lambda-1}{\mu-1}.$$

По теореме 2.3.2 $p_1 = (\lambda-1)/(\mu-1)$.

Теорема 2.3.6. *Совершенный шифр* Σ_B, *обладающий параметрами*

$$p_0 = \lambda/\mu,\ \ p_1 = (\lambda-1)/(\mu-1),\ \ \pi = (\mu^2-\mu)/(\lambda^2-\lambda),$$

существует тогда и только тогда, когда выполняется соотношение

$$\mu - 1 \equiv 0(\mathrm{mod}(\lambda^2-\lambda)), \qquad (2.3.12)$$

и существует $2-(\mu,\lambda,1)$*-схема. При этом* $P(X), P(K)$ — *равномерные распределения.*

Доказательство. Рассмотрим сначала необходимость условий. Согласно теореме 2.3.4, множества элементов строк матрицы зашифрования образуют $2-(\mu,\lambda,1)$-схему, при этом $P(X), P(K)$ — равномерные распределения. Воспользуемся критерием совершенности шифра, согласно которому

$$\sum_{k\in K(x,y)} p(k) = \sum_{k\in K(y)} p(k)\cdot p(d_k(y)). \qquad (2.3.13)$$

Отсюда следует, что

$$\frac{1}{\pi}\left|K(x,y)\right| = \frac{1}{\pi}\sum_{k\in K(y)} p(d_k(y)) = \frac{1}{\pi\lambda}\left|K(y)\right|,$$

и поэтому

$$\lambda\cdot\left|K(x,y)\right| = \left|K(y)\right|.$$

Величина $\left|K(y)\right|$, как мы знаем, равна числу блоков схемы, содержащих элемент y, причем

$$\left|K(y)\right| = (\mu-1)/(\lambda-1).$$

Таким образом,

$$\lambda(\lambda-1)\cdot\left|K(x,y)\right| = \mu-1,$$

откуда следует (2.3.12).

Достаточность. Пусть имеется $2-(\mu,\lambda,1)$-схема и выполняется соотношение (2.3.12). Тогда (по теореме 2.3.6) существует шифр Σ_{B} с равномерными распределениями $P(X)$, $P(K)$, имеющий следующие параметры

$$p_0 = \lambda/\mu,\ p_1 = (\lambda-1)/(\mu-1),\ \pi = (\mu^2-\mu)/(\lambda^2-\lambda).$$

Для этого шифра блоки схемы образуют множества элементов строк матрицы зашифрования. Из условия (2.3.12), для

некоторого натурального числа $u \in \mathrm{N}$, выполняются равенства $\mu = u \cdot (\lambda^2 - \lambda) + 1$ и

$$\pi = (\mu^2 - \mu) / (\lambda^2 - \lambda) = \mu \cdot u.$$

Покажем, что элементы в блоках можно упорядочить таким образом, чтобы в каждом столбце получившейся матрицы зашифрования любой элемент $y \in Y$ встречался бы ровно u раз. Для этого заметим, что $|K(y)| = u\lambda$. Это значит, что y должен встретиться в $u\lambda$ строках матрицы. Упорядочим некоторым образом элементы из Y и разместим их в строках матрицы зашифрования с помощью следующей индуктивной процедуры.

Возьмем любой элемент $y_1 \in Y$, входящий в первый блок, и поместим его в начало первой строки матрицы. Затем находим следующий блок, содержащий y_1, и также помещаем этот элемент в начало соответствующей строки матрицы. Так мы поступим u раз. Затем следующие u вхождений y_1 располагаем на вторые позиции соответствующих строк матрицы и т. д. В результате этой процедуры в каждом столбце матрицы y_1 будет встречаться ровно u раз. После расстановки y_1 остается $u(\mu - 1)$ незанятых мест в каждом столбце.

Далее берем элемент $y_2 \neq y_1$. Располагаем u из имеющихся вхождений y_2 в начала строк и т. д. Это возможно, так как имеется $\lambda u - 1$ вхождений y_2 в блоки, не содержащие y_1 (есть лишь один блок, содержащий y_1 и y_2 одновременно).

В результате мы построим матрицу зашифрования шифра $\sum_{\mathrm{B}}$ с нужными значениями параметров и равномерными распределениями $P(X), P(K)$. Кроме того, для любых $x \in X$ и $y \in Y$ справедливы равенства

$$\sum_{k\in K(x,y)} p(k) = \frac{1}{\pi}\left|K(x,y)\right| = u/\pi = \frac{\mu-1}{(\lambda^2-\lambda)\pi} =$$

$$= \frac{1}{\lambda\pi}\left|K(y)\right| = \sum_{k\in K(y)} p(k)p(d_k(y)).$$

Согласно критерию (2.3.13), шифр, соответствующий построенному коду, совершенен.

Помимо оценки (2.3.7) для числа ключей шифра Σ_{B} с минимальным значением вероятности p_1 имеет место также следующая оценка.

Теорема 2.3.7. *Если для шифра* Σ_{B} *выполняется равенство* $p_1 = (\lambda-1)/(\mu-1)$ *и* $\pi > \lambda \geq 2$, *то* $\pi \geq \mu$.

Доказательство. Введем в рассмотрение матрицы B_1, B_2 размеров $\mu\times\pi$ с неотрицательными элементами, строки которых занумерованы элементами $y\in Y$, а столбцы элементами $k\in K$. Пусть

$$B_i = \left(b^{(i)}_{y,k}\right),$$

где

$$b^{(1)}_{y,k} = \begin{cases} p(k)\cdot p(d_k(y)), & \mathrm{y}\in Y(k), \\ 0, & \mathrm{y}\notin Y(k), \end{cases}$$

$$b^{(2)}_{y,k} = \begin{cases} 1, & \mathrm{y}\in Y(k), \\ 0, & \mathrm{y}\notin Y(k). \end{cases}$$

Пусть $C = B_1\cdot B_2^T$. Поскольку

$$\pi \geq rangB_2 \geq rangC,$$

то достаточно показать, что $rangC = \mu$.

Имеем:

$$c_{y,y'} = \sum_{k \in K} b^{(1)}_{y,k} \cdot b^{(2)}_{y',k} = \sum_{k \in K(y,y')} p(k) \cdot p(d_k(y)).$$

Согласно теореме 2.3.2,

$$c_{y,y'} = \begin{cases} \dfrac{\lambda - 1}{\mu - 1} \cdot \sum\limits_{k \in K(y)} p(k) \cdot p(d_k(y)), & y \neq y', \\ \sum\limits_{k \in K(y)} p(k) \cdot p(d_k(y)), & y = y'. \end{cases}$$

По той же теореме для любого $y \in Y$

$$\sum_{k \in K(y)} p(k) \cdot p(d_k(y)) \neq 0. \qquad (2.3.14)$$

Умножив строку матрицы C с номером y на величину, обратную к (1), получим матрицу D, эквивалентную C:

$$D = \begin{pmatrix} \dfrac{\lambda - 1}{\mu - 1} & 1 & \dots & 1 \\ 1 & \dfrac{\lambda - 1}{\mu - 1} & \dots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \dots & \dfrac{\lambda - 1}{\mu - 1} \end{pmatrix}.$$

Поскольку определитель $|D|$ отличен от нуля, то $rangC = rangD = \mu$. Теорема доказана.

Шифр $\sum_{\text{B}}$, удовлетворяющий условиям

$$p_0 = \lambda/\mu, \quad p_1 = (\lambda - 1)/(\mu - 1), \quad \pi = \mu,$$

называется *экстремальным*. В [Re96] получен результат о совершенных экстремальных шифрах. Приведем его без доказательства.

Теорема 2.3.8. *Пусть* $\sum_{\text{B}}$ *— экстремальный шифр с неравновероятным распределением* $P(X)$. *Тогда элементы строк матрицы зашифрования данного шифра можно переупорядочить таким образом, что получится матрица зашифрования совершенного экстремального шифра.*

В качестве следствия этого утверждения в [Re96] приводится также следующая

Теорема 2.3.9. *Для любого числа* $q \geq 3$, *являющегося степенью простого числа, существует совершенный экстремальный шифр* $\sum_{\text{B}}$ *с параметрами* $\lambda = 2q - 1$, $\pi = q^2 - 1$.

Глава 3

Линейные блочные шифры

В этой главе множества X и Y рассматриваются как подмножества векторных пространств над конечным полем.

Пусть F — конечное поле и F^r — пространство векторов-строк длины $r \in \mathrm{N}$ над полем F:

$$F^r = \{\overline{v} = (v_1, ..., v_r) : v_i \in F,\ i = \overline{1,r}\}.$$

Следуя [Mas87], введем

Определение 3.1. *Шифр* $\sum_{\mathrm{B}}$ *назовем линейным над* F, *если*

$$X = F^m,\ Y = F^n\ (m, n \in \mathrm{N}),$$

и равенство

$$e_k(c_1 \cdot \overline{x}_1 + c_2 \cdot \overline{x}_2) = c_1 \cdot e_k(\overline{x}_1) + c_2 \cdot e_k(\overline{x}_2) \qquad (3.1)$$

выполняется для любых элементов $c_1, c_2 \in F$ *и любых* $\overline{x}_1, \overline{x}_2 \in F^m,\ k \in K$.

Условие (3.1) означает, что e_k является линейным отображением F^m на F^n. Нас будет интересовать возможность построения совершенных линейных шифров.

Утверждение 3.2. *Линейных над* F *совершенных шифров не существует.*

Доказательство. Пусть Σ_{B} линейный над F совершенный шифр. Как мы убедились ранее, свойство совершенности шифра эквивалентно независимости случайных величин $\widetilde{X}$ и $\widetilde{Y}$. В силу этого выполняется равенство

$$p_{X,Y}(\overline{0},\overline{0}) = p_X(\overline{0}) \cdot p_Y(\overline{0}). \qquad (3.2)$$

Так как для линейного шифра $e_k(\overline{0}) = \overline{0}$ при любом $k \in K$, то

$$p_{Y/X}(\overline{0}/\overline{0}) = \sum_{k \in K} p(k) = 1,$$

и

$$p_{X,Y}(\overline{0},\overline{0}) = p_{Y/X}(\overline{0}/\overline{0}) \cdot p_X(\overline{0}) = p_X(\overline{0}). \qquad (3.3)$$

Из (3.2) и (3.3) получаем равенство

$$p_X(\overline{0}) = p_X(\overline{0}) \cdot p_Y(\overline{0}).$$

Так как отображение e_k инъективно и $e_k(\overline{0}) = \overline{0}$, то при $\overline{x} \neq \overline{0}$ выполняется неравенство $e_k(\overline{x}) \neq \overline{0}$. Следовательно,

$$p_Y(\overline{0}) = \sum_{\substack{(x,k):\\ e_k(\overline{x})=\overline{0}}} p_X(\overline{x}) \cdot p_K(k) = \sum_{k \in K} p_X(\overline{0}) \cdot p_K(k) =$$

$$= p_X(\overline{0}) \cdot \sum_{k \in K} p_K(k) = p_X(\overline{0}).$$

Мы получили равенство

$$p_X(\overline{0}) = p_X(\overline{0})^2.$$

Согласно определению вероятностной модели шифра, $p_X(\bar{0}) > 0$. Тогда полученное равенство возможно лишь в случае, когда $p_X(\bar{0}) = 1$. Но в таком случае $p_X(\bar{x}) = 0$ для любого ненулевого $\bar{x} \in X$, чего, опять-таки, быть не должно.

Полученное противоречие доказывает наше утверждение.

Попытаемся построить линейный над F совершенный шифр, изменив в определении 3.1 условия $X = F^m$, $Y = F^n$ на условия

$$X = F^m \setminus \{\bar{0}\},\ Y = F^n \setminus \{\bar{0}\},$$

и считая e_k ограничениями на X линейных отображений из F^m в F^n.

Далее под линейным над F шифром будем понимать шифр, удовлетворяющий указанным условиям.

Для линейного над F шифра правило зашифрования e_k можно задать матрицей M_k размеров $n \times m$ и ранга m. В самом деле, пусть $\vec{v} = (\bar{v}_1, ..., \bar{v}_m)$ — базис пространства F^m, $\vec{u} = (\bar{u}_1, ..., \bar{u}_n)$ — базис пространства F^n, и $\vec{x}_{\vec{v}} = (c_1, ..., c_m)$ для $\bar{x} \in X$. Пусть $\bar{y} = e_k(\bar{x}) \in Y$ и

$$\bar{y}_1 = e_k(\bar{v}_1),\ ..., \bar{y}_m = e_k(\bar{v}_m).$$

Так как векторы $\bar{y}_1, ..., \bar{y}_m$ линейно независимы в пространстве Y, матрица

$$M_k = \left((y_1^{\downarrow})_{\vec{u}} ... (y_m^{\downarrow})_{\vec{u}} \right)_{n \times m}$$

имеет ранг m, и выполняется равенство $y_{\overline{u}}^{\downarrow} = M_k \cdot x_{\overline{v}}^{\downarrow}$. Транспонируя его, получаем равенство

$$y_{\overline{u}}^{\rightarrow} = x_{\overline{v}}^{\rightarrow} \cdot M_k^T. \qquad (3.4)$$

Если $F = GF(q)$, то для минимального совершенного линейного над F шифра выполняются равенства

$$|X| = |Y| = |K| = q^m - 1.$$

Отсюда и из теоремы Шеннона получаем следующее утверждение.

Теорема 3.3. *Минимальный линейный над F шифр $\sum_{\mathrm{B}}$ является сильно совершенным тогда и только тогда, когда выполняются условия:*

(i) *для любых $\overline{x}, \overline{y} \in F^m \setminus \{\overline{0}\}$ существует (и единственный) ключ $k \in K$, удовлетворяющий условию* (3.4);

(ii) *распределение $P(K)$ равномерно.*

Пример 3.4. Рассмотрим минимальный, линейный над $F = GF(2)$, шифр $\sum_{\mathrm{B}}$ при $m = 2$. Пусть $K = \{1,2,3\}$ и

$$M_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad M_2 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \quad M_3 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

Векторы из $F^2 \setminus \{\overline{0}\}$ связаны следующими соотношениями:

$$\overline{x} = (1,0), \quad \overline{x} \cdot M_1 = (1,0), \quad \overline{x} \cdot M_2 = (0,1), \quad \overline{x} \cdot M_3 = (1,1);$$

$$\bar{x} = (0,1), \quad \bar{x} \cdot M_1 = (0,1), \quad \bar{x} \cdot M_2 = (1,1), \quad \bar{x} \cdot M_3 = (1,0);$$

$$\bar{x} = (1,1), \quad \bar{x} \cdot M_1 = (1,1), \quad \bar{x} \cdot M_2 = (1,0), \quad \bar{x} \cdot M_3 = (0,1).$$

Согласно утверждению 3.3 такой шифр является сильно совершенным в том и только том случае, когда

$$P(K) = (1/3, 1/3, 1/3).$$

Для того чтобы ввести следующее понятие, сделаем также и множество K векторным пространством над полем F.

Определение 3.5. *Линейный шифр* $\sum_{\mathrm{B}}$ *назовем билинейным над* F, *если*

$$X = F^m \setminus \{\bar{0}\}, \; Y = F^n \setminus \{\bar{0}\}, \; K = F^s \setminus \{\bar{0}\},$$

для некоторых $m, n, s \in \mathrm{N}$, *и выполняется равенство*

$$e_{c_1 \cdot \bar{k}_1 + c_2 \cdot \bar{k}_2}(\bar{x}) = c_1 \cdot e_{\bar{k}_1}(\bar{x}) + c_2 \cdot e_{\bar{k}_2}(\bar{x}) \qquad (3.5)$$

для тех $\bar{x} \in X$, $\bar{k}_1, \bar{k}_2 \in K$, $c_1, c_2 \in F$, *при которых определены все выражения в данном равенстве.*

Заметим, что мы вынуждены были исключить из множества F^s элемент $\bar{0}$, поскольку из (3.5) следовало бы, что $e_{\bar{0}}(\bar{x}) = \bar{0}$ для любого $\bar{x} \in X$. Поэтому для ключа $\bar{k} = \bar{0}$ требование однозначности расшифрования не выполняется.

Как и для линейного шифра, правило зашифрования билинейного над F шифра можно представить в виде

$$\bar{y} = \bar{x} \cdot M_{\bar{k}}, \tag{3.6}$$

где $M_{\bar{k}}$ — $m \times n$-матрица ранга m, причем такая, что для любых $c_1, c_2 \in F$, $\bar{k}_1, \bar{k}_2 \in K$ выполняется равенство

$$M_{c_1 \cdot \bar{k}_1 + c_2 \cdot \bar{k}_2} = c_1 \cdot M_{\bar{k}_1} + c_2 \cdot M_{\bar{k}_2}. \tag{3.7}$$

Заметим, что условие (3.7) эквивалентно тому факту, что каждый элемент матрицы $M_{\bar{k}}$, где $\bar{k} = (k_1, \ldots, k_s)$, линеен по $\bar{k}$, т. е. является линейной комбинацией компонент $k_1, \ldots, k_s$. В самом деле, пусть $f_{ij}(k_1, \ldots, k_s)$ — элемент матрицы $M_{\bar{k}}$, выраженный в виде некоторой функции f_{ij} от компонент ключа (элементы матрицы $M_{\bar{k}}$ должны определяться лишь самим $\bar{k}$), и $\bar{k} = c_1\bar{k}_1 + c_2\bar{k}_2$. Тогда соответствующий элемент матрицы $M_{\bar{k}_r}$, $r = 1, 2$, имеет вид

$$f_{ij}(k_1^{(r)}, \ldots, k_s^{(r)}),$$

и, согласно (3.7),

$$f_{ij}(c_1 k_1^{(1)} + c_2 k_1^{(2)}, \ldots, c_1 k_s^{(1)} + c_2 k_s^{(2)}) =$$

$$= c_1 f_{ij}(k_1^{(1)}, \ldots, k_s^{(1)}) + c_2 f_{ij}(k_1^{(2)}, \ldots, k_s^{(2)}),$$

то есть

$$f_{ij}(c_1\bar{k}_1 + c_2\bar{k}_2) = c_1 f_{ij}(\bar{k}_1) + c_2 f_{ij}(\bar{k}_2).$$

Это означает, что каждая функция f_{ij} линейна по всем своим переменным.

Пример 3.6. Рассмотрим билинейный над полем $GF(2)$ шифр $\sum_{\mathrm{B}}$ с параметрами $m = n = s = 2$. Правило зашифрования для $\sum_{\mathrm{B}}$ определяется матрицей

$$M_{\bar{k}} = \begin{pmatrix} k_1 & k_2 \\ k_2 & k_1 + k_2 \end{pmatrix}.$$

Чтобы проверить корректность определения правила зашифрования, достаточно убедиться в обратимости преобразования (3.6) для любого $\bar{k} \neq \bar{0}$. Непосредственно вычисляем:

$$\textit{при} \quad \bar{k} = (1,0) \quad - \quad M_{(1,0)} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

$$\textit{при} \quad \bar{k} = (0,1) \quad - \quad M_{(0,1)} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix},$$

$$\textit{при} \quad \bar{k} = (1,1) \quad - \quad M_{(1,1)} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

Каждая из этих матриц невырождена, что и требуется.

Заметим, что шифр, приведенный в примере 3.6, совпадает с шифром из примера 3.4. при кодировании ключей двоичными векторами. Пример 3.6 дает идею построения общей конструкции билинейного минимального сильно совершенного шифра.

Конструкция 1

1) Пусть $\bar{k} = (k_1,...,k_m) \neq \bar{0}$ — начальный вектор линейной рекуррентной последовательности (ранга m) максимального периода над полем $GF(q)$.

2) Пользуясь законом рекурсии, выразим каждый из следующих $m-1$ знаков $k_{m+1}, k_{m+2},..., k_{2m-1}$ ЛРП в виде линейных комбинаций переменных $k_1,...,k_m$.

3) В качестве i-й строки матрицы $M_{\bar{k}}$ возьмем вектор $(k_i, k_{i+1},..., k_{i+m-1})$, каждая координата k_j, $j > m$, которого записана в виде полученной на этапе 2) линейной комбинации.

Пример 3.7. Рассмотрим ЛРП, порожденную линейным регистром сдвига длины 2 над полем $F = GF(2)$ (рис. 3):

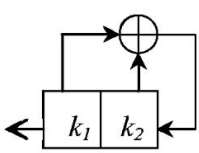


Рис. 3

Пользуясь конструкцией 1, получим матрицу

$$M_{\bar{k}} = \begin{pmatrix} k_1 & k_2 \\ k_2 & k_1 + k_2 \end{pmatrix},$$

совпадающую с матрицей из примера 3.6.

Пример 3.8. Рассмотрим ЛПР, порожденную линейным регистром сдвига длины 3 над полем $F = GF(2)$ (рис. 4):

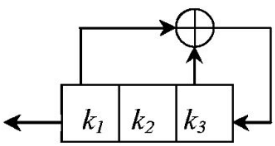


Рис. 4

Пользуясь конструкцией 1, получим следующую матрицу:

$$M_{\bar{k}} = \begin{pmatrix} k_1 & k_2 & k_3 \\ k_2 & k_3 & k_1 + k_3 \\ k_3 & k_1 + k_3 & k_1 + k_2 + k_3 \end{pmatrix}.$$

При кодировании векторов числами, двоичной записью которых они являются, получаем матрицу зашифрования рассматриваемого в этом примере билинейного шифра:

	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	4	1	5	6	2	7	3
3	5	3	6	2	7	1	4
4	6	4	2	7	1	3	5
5	7	6	1	3	4	5	2
6	2	5	7	1	3	4	6
7	3	7	4	5	6	2	1

Данная матрица является латинским квадратом. В случае когда все ключи равновероятны, рассматриваемый шифр является минимальным сильно совершенным шифром.

Утверждение 3.9. *Матрица $M_{\bar{k}}$, полученная с помощью конструкции 1, отвечает правилу зашифрования билинейного над F минимального сильно совершенного шифра в соответствии с формулой* (3.6).

Доказательство. Достаточно проверить, что выполняется условие (ii) утверждения 3.3.

Известно (см., например, [Глу90]), что матрица $M_{\bar{k}}$, построенная с помощью конструкции 1, обладает следующим свойством.

При любом фиксированном $\bar{x} \in F^m \setminus \{\bar{0}\}$ вектор $\bar{x} \cdot M_{\bar{k}}$ представляет собой состояние регистра, полученное после фиксированного числа $l = l(\bar{x})$ тактов его работы из начального состояния $\bar{k}$. Пусть $l(\bar{k}, \bar{x} \cdot M_{\bar{k}})$ — расстояние между векторами $\bar{k}$ и $\bar{x} \cdot M_{\bar{k}}$ на соответствующем цикле линейного преобразования. Тогда упомянутое свойство может быть записано в виде равенства

$$l(\bar{k}, \bar{x} \cdot M_{\bar{k}}) = l(\bar{k}', \bar{x} \cdot M_{\bar{k}'}). \qquad (3.8)$$

Для ЛРП максимального периода все ненулевые векторы образуют один цикл и входят в него ровно по одному разу. Пусть $\bar{k}$ пробегает всевозможные значения из $F^m \setminus \{\bar{0}\}$. Тогда и $\bar{x} \cdot M_{\bar{k}}$ пробегает то же множество значений. В самом деле, если $\bar{k}' \neq \bar{k}$, то, в силу (3.8), $\bar{x} \cdot M_{\bar{k}} \neq \bar{x} \cdot M_{\bar{k}'}$. Следовательно, для любых ненулевых $\bar{x}$ и $\bar{y}$ найдется единственное

значение $\bar{k}$, удовлетворяющее условию (ii) утверждения 3.3. Утверждение доказано.

Конечное поле $GF(q^m)$ можно рассматривать как векторное пространство над подполем $F = GF(q)$. При заданном базисе его элементы представляются векторами из F^m. Так что, если $\beta_1, \beta_2 \in GF(q^m)$ представлены векторами $\bar{v}_1$ и $\bar{v}_2$ соответственно, и $c_1, c_2 \in F$, то $c_1\beta_1 + c_2\beta_2$ представляется вектором $c_1\bar{v}_1 + c_2\bar{v}_2$. Если минимальный многочлен элемента $\alpha \in GF(q^m)$ над F имеет степень m, то получаем канонический базис $e, \alpha, \alpha^2, \ldots, \alpha^{m-1}$.

Пример 3.10. Пусть α — примитивный элемент поля $GF(2^2)$, имеющий минимальный многочлен $x^2 + x + 1$ над $F = GF(2)$. Представим элементы базиса 1 и α векторами (1,0) и (0,1) соответственно. Так как $\alpha^2 = \alpha + 1$, то умножение элементов в $GF(2^2)$ может быть записано в виде

$$(x_1 + x_2 \cdot \alpha)(z_1 + z_2 \cdot \alpha) =$$

$$= (x_1 \cdot z_1 + x_2 \cdot z_2) + (x_1 \cdot z_2 + x_2 \cdot z_1 + x_2 \cdot z_2) \cdot \alpha$$

или в координатной форме

$$(x_1, x_2)(z_1, z_2) = (x_1 \cdot z_1 + x_2 \cdot z_2,\ x_1 \cdot z_2 + x_2 \cdot z_1 + x_2 \cdot z_2).$$

С использованием координатной формы записи элементов поля $GF(q^m)$ можно предложить следующую конструк-

цию билинейного над F минимального сильно совершенного шифра $\sum_{\text{B}}$, для которого

$$X = Y = K = GF(q^m) \setminus \{0\}.$$

Конструкция 2

1) Пусть $\bar{x} = (x_1, \ldots, x_m)$, $\bar{k} = (k_1, \ldots, k_m)$ — ненулевые элементы поля $GF(q^m)$, представленные в координатной форме.

2) Определим правило зашифрования $\bar{y} = e_{\bar{k}}(\bar{x})$ в соответствии с соотношением

$$\bar{y} = \bar{x} \cdot \bar{k} \tag{3.9}$$

в поле $GF(q^m)$.

Пример 3.11. Пусть $(1, \alpha)$ — базис поля $GF(2^2)$ над $F = GF(2)$ из примера 3.10. Конструкция 2 дает билинейный над F шифр с правилом зашифрования

$$(y_1, y_2) = (x_1 \cdot k_1 + x_2 \cdot k_2, x_1 \cdot k_2 + x_2 \cdot k_1 + x_2 \cdot k_2) =$$

$$= \begin{pmatrix} k_1 & k_2 \\ k_2 & k_1 + k_2 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}.$$

Этот шифр совпадает с шифром из примера 3.6.

Утверждение 3.12. *Конструкция 2 строит минимальный билинейный над F сильно совершенный шифр.*

Доказательство. Свойство билинейности шифра следует из аксиом правой и левой дистрибутивности, выполняющихся в поле. Кроме того, в поле для ненулевых элементов x и y однозначно разрешимо уравнение (3.9). Тем самым можно использовать утверждение 3.3.

Конструкцию 2 можно естественным образом обобщить.

Конструкция 3

1) Пусть $\bar{x} = (x_1,...,x_m), \bar{k} = (k_1,...,k_m)$ — ненулевые элементы поля $GF(q^m)$, представленные в координатной форме.

2) Определим правило зашифрования $\bar{y} = e_{\bar{k}}(\bar{x})$ в соответствии с соотношением

$$\tilde{y} = \tilde{x} \cdot \tilde{k}$$

в поле $GF(q^m)$. Здесь

$$\tilde{x} = \bar{x} \cdot A, \ \tilde{k} = \bar{k} \cdot B, \ \tilde{y} = \bar{y} \cdot C,$$

а A, B, C — невырожденные $m \times m$-матрицы над $GF(q)$.

Таким образом, для вычисления $e_{\bar{k}}(\bar{x})$ следует вычислить $\tilde{x} = \bar{x} \cdot A$ и $\tilde{k} = \bar{k} \cdot B$, перемножить их в координатной форме, и по произведению $\tilde{y} = \tilde{x} \cdot \tilde{k}$ вычислить $\bar{y} = \tilde{y} \cdot C^{-1}$.

Очевидно, что конструкция 3 также дает билинейный над F минимальный сильно совершенный шифр. Такие шифры названы *мультипликативными*. В [Mas87] сформулирован ряд нерешенных задач:

- Является ли сильно совершенный билинейный шифр, построенный с помощью конструкции 1, мультипликативным шифром?
- Является ли любой сильно совершенный билинейный шифр мультипликативным шифром?
- Является ли любой сильно совершенный линейный шифр билинейным шифром?

Глава 4

Обобщения теоремы Шеннона

Теорема Шеннона может быть обобщена и для некоторых других криптоатак. Рассмотрим криптоатаки на основе нескольких шифртекстов, полученных на одном ключе.

§ 4.1. Вероятностные распределения

Будем предполагать, что выбор открытых текстов из X осуществляется по схеме случайной выборки с возвращением. Тем самым, для любого $L \in N$ на множестве X^L, состоящем из всевозможных упорядоченных строк длины L элементов, принадлежащих X, вводится распределение вероятностей $P(X^L)$, так что вероятность $p_{X^L}(\bar{x})$ выбора строки $\bar{x}=(x_1,\ldots,x_L)$ открытых текстов равна

$$p_{X^L}(\bar{x})=\prod_{i=1}^{L} p_X(x_i),$$

где $p_X(x)$ — априорная вероятность выбора $x \in X$. Легко проверить, что

$$\sum_{\bar{x} \in X^L} p_{X^L}(\bar{x})=1 .$$

Нас будут интересовать лишь размещения или сочетания из L элементов множеств X или Y. Через $\bar{X}(L)$ и $X(L)$

будем обозначать соответственно множества всех размещений и сочетаний из L элементов множества X. Распределение $P(X^L)$ индуцирует распределения вероятностей $P(\overline{X}(L))$ и $P(X(L))$ на множествах $\overline{X}(L)$ и $X(L)$, так что для $\overline{x} \in \overline{X}(L)$

$$p(\overline{x}) = \frac{p_{X^L}(\overline{x})}{\sum\limits_{\overline{x} \in \overline{X}(L)} p_{X^L}(\overline{x})}, \qquad (4.1.1)$$

а для $X' \in X(L)$

$$p(X') = L! \cdot p(\overline{x}), \qquad (4.1.1')$$

где $\overline{x}$ — любое размещение из элементов множества X'. Можно проверить, что

$$\sum_{\overline{x} \in \overline{X}(L)} p(\overline{x}) = 1 \quad \text{и} \quad \sum_{X' \in X(L)} p(X') = 1.$$

Отметим, что при $L = |X|$ получаем $X(L) = \{X\}$ — множество, состоящее из одного элемента, и тогда, согласно (4.1.1′), $p(X) = 1$.

Элемент $Y' \in Y(L)$ ($\overline{y} \in \overline{Y}(L)$), $L \in \mathbb{N}$, назовем *разрешенным*, если найдутся такие $X' \in X(L)$ ($\overline{x} \in \overline{X}(L)$) и $k \in K$, что $e_k(X') = Y'$ ($e_k(\overline{x}) = \overline{y}$). Обозначим через $Y_{\mathrm{P}}(L)$ ($\overline{Y}_{\mathrm{P}}(L)$) множество всех разрешенных $Y' \in Y(L)$ ($\overline{y} \in \overline{Y}(L)$).

Априорные распределения $P(X(L))$ ($P(\overline{X}(L))$) и $P(K)$ индуцируют распределение вероятностей $P(Y_{\mathrm{P}}(L))$

($P(\overline{Y}_{\mathrm{P}}(L))$) на множестве разрешенных совокупностей из L элементов множества Y по формуле

$$p(Y') = \sum_{X' \in X(L)} \left(p(X') \cdot \sum_{k \in K(X', Y')} p(k) \right), \qquad (4.1.2)$$

$$\left(p(\overline{y}) = \sum_{\overline{x} \in \overline{X}(L)} p(\overline{x}) \cdot \left(\sum_{k \in K(\overline{x}, \overline{y})} p(k) \right) \right), \qquad (4.1.2')$$

где $K(X', Y')$ ($K(\overline{x}, \overline{y})$) — множество возможных ключей, связывающих данные совокупности текстов. Можно проверить, что

$$\sum_{Y' \in Y_{\mathrm{P}}(L)} p(Y') = 1, \quad \left(\sum_{\overline{y} \in \overline{Y}_{\mathrm{P}}(L)} p(\overline{y}) = 1 \right),$$

хотя это следует и из общих соображений.

Для

$$X' \in X(L) \ (\overline{x} \in \overline{X}(L)) \text{ и } Y' \in Y_{\mathrm{P}}(L) \ (\overline{y} \in \overline{Y}_{\mathrm{P}}(L))$$

через $p(X'/Y')$ ($p(\overline{x}/\overline{y})$) обозначим вероятность того, что *на некотором ключе* была зашифрована совокупность открытых текстов X' ($\overline{x}$) при условии, что получена совокупность шифртекстов Y' ($\overline{y}$). Эта вероятность вычисляется по формуле

$$p(X'/Y') = \frac{p(X') \cdot p(Y'/X')}{p(Y')}, \qquad (4.1.3)$$

$$\left(p(\bar{x}/\bar{y}) = \frac{p(\bar{x}) \cdot p(\bar{y}/\bar{x})}{p(\bar{y})} \right), \qquad (4.1.3')$$

где

$$p(Y'/X') = \begin{cases} \sum\limits_{k \in K(X',Y')} p(k), & \text{если } K(X',Y') \neq \varnothing, \\ 0, & \text{если } K(X',Y') = \varnothing. \end{cases} \qquad (4.1.4)$$

$$\left(p(\bar{y}/\bar{x}) = \begin{cases} \sum\limits_{k \in K(\bar{x},\bar{y})} p(k), & \text{если } K(\bar{x},\bar{y}) \neq \varnothing, \\ 0, & \text{если } K(\bar{x},\bar{y}) = \varnothing. \end{cases} \right) \qquad (4.1.4')$$

§ 4.2. Шифры, стойкие к атакам на основе неупорядоченной совокупности шифртекстов, полученных на одном ключе

Следуя [God90], введем

Определение 4.2.1. *Будем говорить, что шифр* Σ_{B} *удовлетворяет условию* $U(L)$*-стойкости (или является* $U(L)$*-стойким), если для любого* $Y' \in Y_{\mathrm{P}}(L)$ *и для любого* $X' \in X(L)$ *выполняется равенство*

$$p(X'/Y') = p(X'). \qquad (4.2.1)$$

Свойство $U(L)$-стойкости можно было назвать точнее свойством *неупорядоченной* L*-кратной совершенной стой-*

кости шифра, однако это намного длиннее. Буква U в названии условия — это первая буква слова *Unordered* (неупорядоченный).

Далее для упрощения записи будем вместо $e_k, k \in K$, использовать запись $e \in E$, имея в виду, что имеется взаимно однозначное соответствие между множествами K и E.

Как и совершенные по Шеннону шифры, $U(L)$-стойкие шифры должны быть транзитивными.

Лемма 4.2.2. *Если шифр* $\sum_{\text{B}}$ *удовлетворяет условию* $U(L)$*-стойкости, то для любых* $Y' \in Y_{\text{P}}(L)$, $X' \in X(L)$ *справедливо неравенство* $|K(X', Y')| \geq 1$.

Доказательство. От противного: предположим, что $e(X') \neq Y'$ для некоторой пары подмножеств X', Y' и любого $e \in E$. Но тогда, очевидно, $p(X'/Y') = 0$, в то время как $p(X') > 0$. Получили противоречие с условием $U(L)$-стойкости.

Как и в § 2.2, далее будем использовать обозначения $|X| = \lambda$, $|Y| = \mu$, $|K| = \pi$.

Лемма 4.2.3. *Если шифр* $\sum_{\text{B}}$ *удовлетворяет условию* $U(L)$*-стойкости, то для числа его ключей* π *выполняется неравенство*

$$\pi \geq |Y_{\text{P}}(L)|.$$

Более того, если $\pi = |Y_{\text{P}}(L)|$,

то

(i) $|K(X', Y')| = 1$ *для любых* $X' \in X(L)$, $Y' \in Y_{\text{P}}(L)$;

(ii) *если* $Y' \in Y_{\mathrm{P}}(L)$ *и* $Y' \subset e(X)$ *для некоторых* $e \in E$, *то* $p(Y') = p(e)$.

Доказательство. Пусть $X' \in X(L)$. По лемме 4.2.2 для любого $Y' \subset e(X)$ найдется такой $e \in E$, что $e(X') = Y'$. Зафиксировав X' и заставив Y' пробегать все множество $Y_{\mathrm{P}}(L)$, получим, по меньшей мере, $|Y_{\mathrm{P}}(L)|$ ключей. Отсюда следует, что $\pi \geq |Y_{\mathrm{P}}(L)|$.

Пусть теперь $\pi = |Y_{\mathrm{P}}(L)|$. Рассуждения, проведенные при доказательстве неравенства, сразу дают единственность соответствующего ключа, что дает (i).

Пусть $Y' \in Y_{\mathrm{P}}(L)$ и $X' \in X(L)$ — такие совокупности, что $Y' \subset e(X)$ и $e(X') = Y'$. Тогда, согласно (i), e — единственный такой элемент из E. По условию

$$p(X'/Y') = \frac{P(Y'/X') \cdot P(X')}{P(Y')} = P(X'),$$

откуда $p(Y'/X') = p(Y')$. Так как $P(Y'/X') = P(e)$, то $p(Y') = p(e)$, что и требуется.

Теорема 4.2.4. *Если шифр* Σ_{B} *удовлетворяет условию* $U(L)$*-стойкости,* $(L \leq \lambda)$, *то*

$$\pi \geq \frac{\mu}{\lambda} \cdot C_{\lambda}^{L}. \qquad (4.2.2)$$

Более того, если

$$\pi = \frac{\mu}{\lambda} \cdot C_{\lambda}^{L},$$

то

(i) *при* $L>1$ *для любых* $e_1, e_2 \in E$ *выполняется одно из равенств:* $e_1(X)=e_2(X)$, *или* $e_1(X)\cap e_2(X)=\varnothing$;

(ii) *если* $e_1(X)=e_2(X)$, *то* $p(e_1)=p(e_2)=p(Y')$ *при любом* $Y'\in Y_{\mathrm{P}}(L)$, *для которого* $Y'\subset e_1(X)$.

Доказательство. Согласно лемме 4.2.3, достаточно показать, что

$$\left|Y_{\mathrm{P}}(L)\right| \geq \frac{\mu}{\lambda}\cdot C_{\lambda}^{L}.$$

Выберем любой шифртекст y. Найдутся $e\in E$, $x\in X$, такие, что $e(x)=y$. Для наглядности дальнейших рассуждений приведем рисунок:

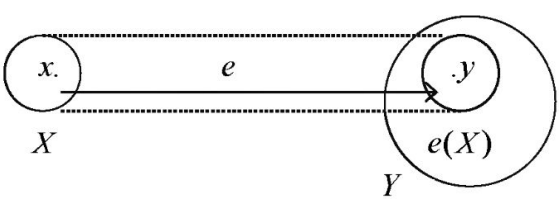


Рис. 5

Оценим число разрешенных L-множеств Y' из $e(X)$, содержащих y. Так как $\left|e(X)\right|=\lambda$, то имеется $C_{\lambda-1}^{L-1}$ дополнений $\{y\}$ до L-множества. В свою очередь, выбор y можно осуществить μ способами. Всего набирается $\mu\cdot C_{\lambda-1}^{L-1}$ L-

множеств. Каждое из таких L-множеств встретится при нашем построении ровно L раз. В самом деле, если

$$Y' = \{y = y_0, y_1, \ldots, y_{L-1}\},$$

то такое множество Y' можно также представить в виде

$$Y' = \{y = y_1, y_0, y_2, \ldots, y_{L-1}\},$$

$$Y' = \{y = y_2, y_0, y_1, \ldots, y_{L-1}\}, \ldots,$$

или, наконец, в виде

$$Y' = \{y = y_{L-1}, y_0, y_1, \ldots, y_{L-2}\}.$$

Поэтому

$$|Y_{\mathrm{P}}(L)| \geq \frac{\mu}{L} \cdot C_{\lambda-1}^{L-1} = \frac{\mu \cdot (\lambda-1)!}{L \cdot (L-1)!(\lambda-L)!} =$$

$$= \frac{\mu \cdot \lambda!}{\lambda \cdot L!(\lambda-L)!} = \frac{\mu}{\lambda} \cdot C_L^{\lambda},$$

что и требуется.

Обратимся к проверке свойств (i) и (ii). Предположим, что

$$\pi = \frac{\mu}{\lambda} \cdot C_{\lambda}^{L}.$$

Тогда и

$$|Y_{\mathrm{P}}(L)| = \frac{\mu}{\lambda} \cdot C_{\lambda}^{L}.$$

Пусть $L > 1$ (тогда $L - 1 > 0$).

Мы заметили, что каждый $y \in Y$ входит, по крайней мере, в $C_{\lambda-1}^{L-1}$ разрешенных L-множеств (из $e(X)$). Всего же их (по условию) имеется

$$\frac{\mu}{\lambda} \cdot C_{\lambda}^{L} = \frac{\mu}{L} \cdot C_{\lambda-1}^{L-1}.$$

Если бы некоторый y содержался более чем в $C_{\lambda-1}^{L-1}$ L-множествах, то отсюда следовало бы неравенство

$$\left|Y_{\mathrm{P}}(L)\right| > \frac{\mu \cdot C_{\lambda-1}^{L-1}}{L},$$

что не так. Значит каждый y содержится в точности в $C_{\lambda-1}^{L-1}$ разрешенных L-множествах. Поэтому если $y \in e'(X)$, то обязательно

$$e'(X) = e(X).$$

В самом деле, мы насчитали $C_{\lambda-1}^{L-1}$ подмножеств в множестве $e(X)$, содержащих y. Поэтому, если $e'(X) \neq e(X)$, то в $e'(X) \cup e(X)$ можно было найти еще некоторое число подмножеств, чего быть не может. Отсюда следует (i). Условие (ii) сразу следует из леммы 4.2.3. Заметим, что при $L = 1$ утверждение пункта (i) неверно.

Рассмотрим нижнюю границу из теоремы 4.2.4 применительно к случаю, когда $\lambda = \mu$. При этом условии $\pi = C_{\lambda}^{L}$ — минимально возможное число ключей, необходимое для обеспечения $U(L)$-стойкости. Заметим, что в случае, когда $\lambda < \mu$, изучение $U(L)$-стойких шифров, для которых

$\pi = \frac{\mu}{\lambda} \cdot C_\lambda^L$, сводится по теореме 4.2.4 к случаю, когда $\lambda = \mu$.

Пусть для простоты $X = Y$. Тогда каждое правило зашифрования — это некоторая подстановка на X и, согласно условию (ii) теоремы 4.2.4, все ключи $U(L)$-стойкого шифра *равновероятны*. В этих условиях можно сформулировать критерий того, что C_λ^L подстановок на X образуют множество E, отвечающее $U(L)$-стойкой шифрсистеме. Заметим, что в таком случае $Y_{\mathrm{P}}(L)$ состоит из всех L-подмножеств из $Y = X$, то есть что все L-подмножества из X — разрешенные. В самом деле,

$$\pi = \left|X_{\mathrm{P}}(L)\right| = C_\lambda^L = \left|X(L)\right|.$$

Так как $X_{\mathrm{P}}(L) \subseteq X(L)$, то $X_{\mathrm{P}}(L) = X(L)$.

Теорема 4.2.5. *Пусть $Y = X$ и E — множество подстановок на X, рассматриваемое как множество правил зашифрования для шифра Σ_{B} с числом ключей $\pi = C_\lambda^L$. Тогда такой шифр является $U(L)$-стойким тогда и только тогда, когда*

(i) $\left|E(X', Y')\right| = 1$ *для любой пары L-подмножеств X', Y' (из X);*

(ii) $p(e) = 1/C_\lambda^L$ *для любого $e \in E$.*

Доказательство. Необходимость следует из условий (ii) теоремы 4.2.4 и (i) леммы 4.2.3. Для проверки достаточности рассмотрим вероятность $P(Y'/X')$:

$$p(Y'/X') = \sum_{e \in E(X',Y')} p(e) = p(e) = 1/C_\lambda^L.$$

Вместе с тем,

$$P(Y') = \sum_{\substack{(e,X''):\\ e(X'')=Y'}} P(e)\cdot P(X'') = \frac{\sum_{X'' \in X(L)} P(X'')}{C_\lambda^L} = \frac{1}{C_\lambda^L}.$$

В результате получаем равенство $P(Y'/X') = P(Y')$, что и требуется.

Заметим, что в случае $L = 1$ теорема 4.2.5 в точности совпадает с теоремой Шеннона.

Определение 4.2.6. *Множество подстановок E на X называется (t,ω)-однородным на X, если для любых $X_1, X_2 \in X(t)$ существует ровно ω подстановок $e \in E$, для которых $e(X_1) = X_2$.*

Однородные множества подстановок изучались в ряде работ, например [Nom85], [StiTei90], [Bie92], [Bie95].

Согласно пункту (ii) теоремы 4.2.5, задача построения $U(L)$-стойких шифров в случае, когда $X = Y$, $\pi = C_\lambda^L$, эквивалентна задаче построения $(L,1)$-однородных множеств подстановок на множестве из λ элементов. Эта задача эквивалентна также задаче построения так называемых перпендикулярных массивов специального вида.

Определение 4.2.7. *Перпендикулярным массивом $PA_\omega(t,\lambda,\mu)$ называется всякая матрица A размеров*

$\omega \cdot C_\mu^t \times \lambda$ с элементами из множества Y мощности μ, каждая строка которой состоит из λ различных элементов, и любые t различных элементов множества Y содержатся точно в ω строках подматрицы, составленной любыми t столбцами матрицы A.

Непосредственно из определений 4.2.1, 4.2.7 и теоремы 4.2.5 следует

Теорема 4.2.8. *Если существует перпендикулярный массив $PA_\omega(t,\lambda,\mu)$, то существует и $U(t)$-стойкий шифр $\sum_{\text{В}}$ с параметрами*

$$|X| = \lambda,\ |Y| = \mu,\ |K| = \omega \cdot C_\mu^t.$$

Для доказательства достаточно рассмотреть массив $PA_\omega(t,\lambda,\mu)$ как матрицу зашифрования искомого шифра с равновероятными ключами. При этом строки и столбцы матрицы можно пронумеровать их порядковыми номерами, тогда

$$X = \{1,2,...,\lambda\},\ Y = \{1,2,...,\mu\}.$$

В случае когда $X = Y$, $\pi = C_\lambda^L$, построение $U(L)$-стойкого шифра эквивалентно построению перпендикулярного массива $PA_1(L,\lambda,\lambda)$. Попутно отметим, что если выписать друг под другом подстановки (t,ω)-однородного множества подстановок степени λ, то получится перпендикулярный массив $PA_\omega(t,\lambda,\lambda)$.

Известно, что при $L \le 4$, $\omega \le 4$, существуют перпендикулярные массивы $PA_\omega(L,\lambda,\lambda)$ ([Sti90]). Например, сущест-

вует $PA_1(3,\lambda,\lambda)$ при $\lambda=8$ и $\lambda=32$. Имеется бесконечный класс массивов $PA_3(3,q+1,q+1)$ для любой степени простого числа q, где $q\equiv 3(\mathrm{mod}\,4)$. При $\lambda=9$ и $\lambda=33$ существуют массивы $PA_4(4,\lambda,\lambda)$. Все эти примеры получены на основе (t,ω)-однородных множеств подстановок, являющихся группами.

Глубокие результаты по теории перпендикулярных массивов изложены в [Bie94].

Далее мы отдельно рассмотрим случай $L=2$. Используем для построения $U(2)$-стойкого шифра перпендикулярный массив $PA_1(2,\lambda,\lambda)$, где λ — нечетное простое число.

Лемма 4.2.9. *В любом перпендикулярном массиве $PA_1(2,\lambda,\lambda)$ при $\lambda>2$ каждый элемент из Y входит ровно $(\lambda-1)/2$ раз в каждый столбец (и, следовательно, λ — нечетно).*

Доказательство. Рассмотрим произвольные столбцы матрицы $PA_1(2,\lambda,\lambda)$ с номерами i, j, h. Пусть произвольный элемент $y\in Y$ содержится в этих столбцах k_i, k_j, k_h раз соответственно. Из определения перпендикулярного массива следует, что в строках подматриц, состоящих из столбцов (i,j) и (i,h), число пар элементов, содержащих y, выражается в виде

$$k_i+k_j=k_i+k_h=\lambda-1.$$

Аналогично

$$k_j+k_i=k_j+k_h=\lambda-1.$$

Из полученных соотношений следует равенство

$$k_i = k_j = k_h = (\lambda - 1)/2,$$

что и требуется.

Пусть λ — нечетное простое число и

$$P = GF(\lambda) = \{a_0, \ldots, a_{\lambda-1}\}$$

— конечное поле. Рассмотрим матрицу M размеров $C_\lambda^2 \times \lambda$, у которой столбцы занумерованы элементами $x \in P$, а строки некоторым множеством Ω из C_λ^2 *упорядоченных* пар $(i, j) \in P^2$. На пересечении столбца x и строки (i, j) в M расположим элемент $i \cdot x + j \in P$.

Теорема 4.2.10. *Множество Ω можно выбрать таким образом, что матрица M является перпендикулярным массивом $PA_1(2, \lambda, \lambda)$.*

Доказательство. Сделаем ряд замечаний.

Поле P содержит единицу ε и противоположный к ней элемент $(-\varepsilon)$. По лемме 4.2.9 в столбце матрицы M с номером $(-\varepsilon)$ каждый элемент поля встречается ровно $(\lambda - 1)/2$ раз. Это касается и нуля поля — 0. Таким образом, среди номеров строк должно быть ровно $(\lambda - 1)/2$ пар (i, j) таких, что $i \cdot (-\varepsilon) + j = 0$, то есть $i = j$.

При $i = 0$ соответствующая строка матрицы M состоит из одинаковых элементов (равных j). Поэтому для построения перпендикулярного массива необходимо условие, при котором каждая строка была бы пронумерована парой (i, j), в которой $i \neq 0$.

Покажем, что если для некоторого $i \in P$ пара (i,i) принадлежит Ω, и M — перпендикулярный массив, то $(-i,k) \notin \Omega$.

В самом деле, пусть, наряду с парой (i,i), множество Ω содержит также пару $(-i,k)$, в которой $k \neq i$. Рассмотрим тогда элементы матрицы M, стоящие на пересечении столбца с номером 0 и строк с номерами (i,i) и $(-i,k)$. Они равны соответственно i и k. Аналогично в столбце с номером $(k-i)\cdot i^{-1}$ на позициях с теми же номерами расположены соответственно k и i. Это противоречит определению перпендикулярного массива, так как в выделенных строках находятся пары, отличающиеся лишь перестановкой своих элементов. Заметим, что среди "забракованных" пар $(-i,k)$ содержатся пары вида $(-i,-i)$. Если же Ω содержит пары $(i,i),(-i,i)$, то на пересечении строк матрицы M с этими номерами и столбцов с номерами a и $-a$ окажутся пары

$$(i\cdot a+i,-i\cdot a+i) \text{ и } (-i\cdot a+i,i\cdot a+i),$$

что также невозможно.

Из сделанных замечаний следует вывод о том, что для построения перпендикулярного массива M при фиксации $(\lambda-1)/2$ пар вида (i,i), служащих номерами строк M, остальные пары могут иметь лишь вид (i,k), где i — элемент одной из фиксированных пар. В самом деле, все элементы поля оказываются разложенными на три части: множество элементов i, входящих в выбранные пары (их ровно $(\lambda-1)/2$), множество элементов $-i$ (их также $(\lambda-1)/2$), и отдельно элемент 0.

Заметим, что всего мы сможем набрать таким образом ровно $\lambda(\lambda-1)/2$ таких пар: по λ пар (i, j), $j \in P$, определяемых выбором пары (i,i). Именно столько пар требуется для нумерации столбцов матрицы M. Покажем, что любая такая матрица M является перпендикулярным массивом. Если это не так, то возможны лишь два случая:

1) Найдутся два столбца (скажем, с номерами a и b) и две строки (скажем, с номерами (i, j) и (i', j')) такие, что образованная ими подматрица состоит из одинаковых векторов-строк.

2) Найдутся два столбца (скажем, с номерами a и b) и две строки (скажем, с номерами (i, j) и (i', j')) такие, что образованная ими подматрица состоит из одинаковых после перестановки элементов векторов-строк.

В первом случае получаем равенства

$$a \cdot i + j = a \cdot i' + j'$$

и

$$b \cdot i + j = b \cdot i' + j',$$

с помощью которых получаем соотношение

$$(a-b) \cdot i' = (a-b) \cdot i$$

или

$$(a-b) \cdot (i-i') = 0.$$

Так как по условию $a \neq b$, то

$$i = i' \text{ и } j = j'.$$

Отсюда следует, что первый случай невозможен.

Во втором случае

$$a \cdot i + j = b \cdot i' + j'$$

и

$$b \cdot i + j = a \cdot i' + j',$$

откуда

$$(a - b) \cdot i = (b - a) \cdot i'$$

или

$$(i + i') \cdot (a - b) = 0.$$

Так как по условию $a \neq b$, то $i = -i'$, что противоречит нашему выбору множества пар Ω.

Тем самым мы показали, что матрица M является перпендикулярным массивом. Теорема доказана.

Вопрос о существовании $U(L)$-стойких шифров с минимальным числом ключей при $L > 2$ является открытым. Если отказаться от условия минимальности числа ключей, то при любом L несложно указать пример $U(L)$-стойкого шифра. Это будет ясно из дальнейших рассмотрений.

Рассмотрим теперь неэндоморфные $U(L)$-стойкие шифры. Ослабим требование $\lambda = \mu$ и рассмотрим случай, когда

$$\mu \geq \lambda \text{ и } \pi = \frac{\mu \cdot C_\lambda^L}{\lambda}.$$

Пусть сначала $L = 1$. Тогда

$$\pi = \frac{\mu \cdot C_\lambda^1}{\lambda} = \mu.$$

Для $U(1)$-стойкого шифра по лемме 4.2.3 выполняется неравенство $\pi \geq |Y_{\mathrm{P}}(1)|$. Но $Y_{\mathrm{P}}(1) = Y$, поэтому

$$\left|Y_{\mathrm{P}}(1)\right| = \left|Y\right| = \mu = \pi.$$

Согласно утверждению (i) леммы 4.2.3, $\pi = \left|Y_{\mathrm{P}}(1)\right|$ тогда и только тогда, когда для любого $x \in X$ и любого $y \in Y$ найдется единственный элемент $e \in E$, такой, что $e(x) = y$. Составим матрицу зашифрования:

$E \setminus X$	x_1	$\cdots$	x_λ
e_1	y_{i_1}	$\cdots$	y_{j_1}
$\cdots$	$\cdots$	$\cdots$	$\cdots$
e_μ	y_{i_μ}	$\cdots$	y_{j_μ}

Из сказанного следует, что любой столбец матрицы не может содержать совпадающих элементов. Другими словами, каждый столбец матрицы — некоторая перестановка элементов множества Y. Кроме того, и каждая строка состоит из различных элементов.

Прямоугольная матрица, составленная из элементов множества Y, в которой строки и столбцы не содержат одинаковых элементов, называется *латинским прямоугольником*. Таким образом, в рассматриваемом случае матрица зашифрования $U(1)$-стойкого шифра является латинским прямоугольником.

Известна приближенная формула для числа $L(\lambda, \mu)$ латинских прямоугольников, доказанная в 1946 году П.Эрдешем и И.Капланским ([Коф75]):

$$L(\lambda,\mu) \approx (\mu!)^{\lambda} \cdot e^{-\frac{(\lambda-1)\lambda}{2}},$$

имеющая место при условии $\lambda < (\ln \mu)^{1,5}$. Позже К. Ямамото доказал справедливость этой формулы при условии $\lambda < \sqrt[3]{\mu}$ ([Рио63]).

Пусть теперь $L > 1$. По утверждению (i) теоремы 4.2.4 число ключей π достигает минимального значения $\frac{\mu}{\lambda} \cdot C_{\lambda}^{L}$ при $\mu = \lambda \cdot t$ $(t \in \mathrm{Z})$, причем множество Y разбивается на t подмножеств $Y_1,\ldots,Y_t$, каждое мощности λ, и такие, что для любого $e \in E$ имеет место равенство $e(X) = Y_i$ для некоторого $i \in \overline{1,t}$.

Введем обозначение

$$E_i = \{e \in E : e(X) = Y_i\}, \ i = \overline{1,t}.$$

Тогда

$$E = \bigcup_i E_i$$

— разбиение множества E. Согласно утверждению (ii) теоремы 4.2.4, из равенства $e_1(X) = e_2(X)$ следует, что $p(e_1) = p(e_2)$. Легко видеть, что каждая тройка $(\widetilde{X}, \widetilde{Y}_i, \widetilde{E}_i)$ образует $U(L)$-стойкий шифр, $i = \overline{1,t}$, для которого $\mu = \lambda$. Тем самым, изучение $U(L)$-стойких шифров в случае, когда

$$\pi = \mu \cdot C_{\lambda}^{L} / \lambda \text{ и } \mu > \lambda$$

сводится к изучению $U(L)$-стойких шифров, для которых $\mu = \lambda$.

В заключение докажем, что совершенная стойкость $U(L)$-стойкого шифра не зависит от распределения вероятностей на множестве открытых текстов.

Теорема 4.2.11. *Пусть* Σ_{B}^{0} *— шифр с априорным распределением вероятностей* $P_0(X)$, *удовлетворяющий условию* $U(L)$*-стойкости, и* Σ_{B}^{1} *— шифр, отличающийся от* Σ_{B}^{0} *лишь распределением вероятностей* $P_1(X)$. *Тогда* Σ_{B}^{1} *также удовлетворяет условию* $U(L)$*-стойкости.*

Доказательство. Воспользуемся критерием $U(L)$-стойкости шифра Σ_{B}^{0} в форме равенства

$$p(Y_1/X_1) = p(Y_1),$$

записанного в виде

$$\sum_{k\in K(X_1,Y_1)} p(k) = \sum_{k\in K(Y_1)} p(k)\cdot p_0(d_k(Y_1)). \qquad (4.2.3)$$

Проверим аналогичное равенство применительно к шифру Σ_{B}^{1}. Для этого заметим, что

$$\sum_{k\in K(Y_1)} p(k)\cdot p_1(d_k(Y_1)) =$$

$$= \sum_{X'\in X(L)} \left(p_1(X')\cdot \sum_{k\in K(X',Y_1)} p(k) \right) =$$

$$= \left(\sum_{X' \in X(L)} p_1(X') \right) \cdot \left(\sum_{k \in K(X'', Y_1)} p(k) \right), \qquad (4.2.4)$$

где X'' — любой фиксированный элемент из $X(L)$. Это следует из того, что $\sum_{k \in K(X', Y_1)} p(k)$ не зависит от X'.

Согласно (4.2.3), правую часть (4.2.4) можно записать в виде

$$\sum_{X' \in X(L)} p_1(X') \cdot \sum_{k \in K(Y_1)} p(k) \cdot p_0(d_k(Y_1)) =$$

$$= \sum_{k \in K(Y_1)} p(k) \cdot p_0(d_k(Y_1)) = \sum_{k \in K(X_1, Y_1)} p(k),$$

поскольку

$$\sum_{X' \in X(L)} p_1(X') = 1.$$

Отсюда следует

$$\sum_{k \in K(Y_1)} p(k) \cdot p_1(d_k(Y_1)) = \sum_{k \in K(X_1, Y_1)} p(k),$$

что и требуется.

§ 4.3. Имитостойкие $U(L)$-стойкие шифры

Нас будут интересовать $U(L)$-стойкие шифры, имеющие наилучшие параметры имитостойкости. Помимо упомянутых в главе 2 параметров p_0 и p_1 рассматривают также вероятность p_L, $L \geq 2$, успеха противника *в попытке обмана порядка* L. Имеется в виду ситуация, когда противник может наблюдать L различных криптограмм, полученных на одном ключе, и заменять их на некое "поддельное" сообщение по своему усмотрению.

В [Sti88], [Soe88] получена простая нижняя оценка вероятности p_L.

Теорема 4.3.1. *Имеет место достижимая оценка*

$$p_L \geq \frac{\lambda - L}{\mu - L}. \tag{4.3.1}$$

Доказательство. Пусть противник наблюдает в канале связи множество шифртекстов $Y' = \{y_1, ..., y_L\}$. Обозначим через $p(y, Y')$ вероятность того, что шифртекст $y \in Y \setminus Y'$ будет принят получателем сообщений как аутентичный. Тогда

$$p(y, Y') = \frac{\sum\limits_{k \in K(Y' \cup \{y\})} p(k) \cdot p(d_k(Y'))}{\sum\limits_{k \in K(Y')} p(k) \cdot p(d_k(Y'))}, \tag{4.3.2}$$

где

$$K(\overset{\backslash}{Y}) = \{k \in K : \exists \overset{\backslash}{X} \subset X, \ |\overset{\backslash}{X}| = |\overset{\backslash}{Y}|, \ e_k(\overset{\backslash}{X}) = \overset{\backslash}{Y}\}.$$

Аналогично тому, как это делалось в теореме 2.2.3, проверяется равенство

$$\sum_{y \in Y \setminus Y'} p(y, Y') = \lambda - L, \tag{4.3.3}$$

из которого следует искомое неравенство:

$$p_L = \max_{y \in Y \setminus Y'} p(y, Y') \geq \frac{\lambda - L}{\mu - L}.$$

Если этот максимум достигается на y_0, то противник выбирает его в своей попытке обмана.

Определение 4.3.2. *Будем говорить, что шифр удовлетворяет условию L-стойкости к попытке обмана, если для любого i, $0 \leq i \leq L$, выполняется равенство*

$$p_i = \frac{\lambda - i}{\mu - i}. \tag{4.3.4}$$

В ряде работ (например, [Soe88], [Sti90], [Mitt94], [Cas98]) изучались шифры, одновременно удовлетворяющие условию $U(L')$-стойкости и условию L-стойкости к попытке обмана. Наибольшее внимание уделялось случаям, когда $L' = L - 1$ или $L' = L$. Первое сочетание наиболее естественно в случае, когда противник может вставить новое сообщение в канал связи, но не может модифицировать наблюдаемые сообщения. Если же противник может модифицировать сообщения, то естественно изучать второй случай.

Сформулируем ряд результатов в этом направлении.

Теорема 4.3.3. *Если шифр* Σ_{B} *удовлетворяет условию* $U(L)$*-стойкости и условию* $(L-1)$*-стойкости к попытке обмана, то* $\pi \geq C_{\mu}^{L}$.

Доказательство. Пусть $Y' \in Y_{\mathrm{P}}(L-1)$, $y_0 \notin Y'$. Предположим, что $Y' \cup \{y_0\} \notin Y_{\mathrm{P}}(L)$.

Как и в теореме 4.3.1, вероятность того что при попытке обмана шифртекст y будет принят как аутентичный, при условии что наблюдается множество криптограмм Y', вычисляется по формуле (4.3.2). Аналогично (4.3.3), справедливо равенство

$$\sum_{y \in Y \setminus Y'} p(y, Y') = \lambda - L + 1,$$

причем одно из слагаемых этой суммы — $p(y_0, Y')$ равно нулю. Если бы все остальные слагаемые были не больше отношения

$$(\lambda - L + 1) : (\mu - L + 1),$$

то их сумма была бы строго меньше $\lambda - L + 1$. Значит, для некоторого $y \in Y \setminus Y'$

$$p(y, Y') > \frac{\lambda - L + 1}{\mu - L + 1},$$

и

$$p_{L-1} = \max_{y} p(y, Y') > \frac{\lambda - L + 1}{\mu - L + 1},$$

что противоречит условию $(L-1)$-стойкости к попытке обмана. Следовательно, $Y_{\mathrm{P}}(L)=Y(L)$.

Так как шифр $\sum_{\mathrm{B}}$ удовлетворяет условию $U(L)$-стойкости, для любого $Y'\in Y_{\mathrm{P}}(L)$ и любого $X'\in X(L)$ справедливо неравенство $|K(X',Y')|\geq 1$, откуда

$$\pi \geq |Y_{\mathrm{P}}(L)| = |Y(L)| = C_{\mu}^{L},$$

что и требуется.

В [Soe88] шифр $\sum_{\mathrm{B}}$, имеющий ровно C_{μ}^{L} ключей, удовлетворяющий условию $U(L)$-стойкости и условию $(L-1)$-стойкости к попытке обмана, назван *оптимальным* $(L,L-1)$-*шифром*.

Примеры $U(L)$-стойких шифров, выдерживающих попытки обмана, дает конструкция перпендикулярного массива $PA_1(2,\lambda,\mu)$. Имеет место, например, следующий результат.

Теорема 4.3.4. *Если существует перпендикулярный массив* $PA_1(2,\lambda,\mu)$, $\lambda>2$, *то существует шифр* $\sum_{\mathrm{B}}$, *для которого*

$$|X|=\lambda,\ |Y|=\mu,\ \text{и}\ |K|=C_{\mu}^{2},$$

причем $U(2)$-*стойкий и* 0-*стойкий к попытке обмана.*

Доказательство. Рассмотрим данный перпендикулярный массив в качестве матрицы зашифрования для $\sum_{\mathrm{B}}$. Если строка матрицы с номером k имеет вид $(y_1,\ldots,y_{\lambda})$, то пола-

гаем $e_k(x_i) = y_i$, $i = \overline{1,\lambda}$. Будем использовать ключ k с вероятностью

$$p(k) = 2/\mu(\mu-1).$$

Как и в лемме 4.2.9, при $\lambda > 2$ каждый символ содержится ровно $(\mu-1)/2$ раз в каждом столбце массива. Отсюда следует, что

$$p_0 = \max_y \sum_{k \in K(y)} p(k) = \lambda \cdot \frac{\mu-1}{2} \cdot \frac{2}{\mu(\mu-1)} = \lambda/\mu.$$

Из определения перпендикулярного массива $PA_1(2,\lambda,\mu)$ следует, что для любых y, y' и любых x, x' в матрице имеется лишь одна строка (пусть ее номер — k) такая, что

$$X' = \{e_k(x), e_k(x')\} = \{y, y'\} = Y'$$

или, что то же самое,

$$\left|K(X', Y')\right| = 1.$$

Тогда

$$p(Y'/X') = \sum_{k \in K(X',Y')} p(k) = p(k) = \frac{2}{\mu(\mu-1)} =$$

$$= \frac{2}{\mu(\mu-1)} \cdot \sum_{X' \in X(2)} p(X') =$$

$$= \sum_{(X',k):e_k(X')=Y'} p(X') \cdot p(k) = p(Y').$$

Следовательно, $\sum_{\mathrm{B}}$ является $U(2)$-стойким шифром.

Частные виды перпендикулярных массивов $PA_1(2,\lambda,\mu)$ можно использовать для построения оптимальных $(2,1)$-шифров $\sum_{\mathrm{B}}$.

Следуя [Sti88], назовем перпендикулярный массив $PA_1(2,\lambda,\mu)$ *циклическим* (и обозначим его $CPA_1(2,\lambda,\mu)$), если вместе с каждой строкой он содержит в качестве строк все ее циклические сдвиги.

Примером $CPA_1(2,5,5)$ является следующая матрица:

0	1	2	3	4
1	2	3	4	0
2	3	4	0	1
3	4	0	1	2
4	0	1	2	3
0	2	4	1	3
1	3	0	2	4
2	4	1	3	0
3	0	2	4	1
4	1	3	0	2

Теорема 4.3.5. *Если существует перпендикулярный массив* $CPA_1(2,\lambda,\mu)$, *то существует оптимальный* $(2,1)$*-шифр* $\sum_{\mathrm{B}}$ *с параметрами* $|X| = \lambda,\ |Y| = \mu$.

Доказательство. Пусть $A = CPA_1(2, \lambda, \mu)$. Построим $\sum_B$ так же, как в теореме 4.3.3. Достаточно проверить, что $p_1 = (\lambda - 1)/(\mu - 1)$.

Имеем:

$$p(y, y') = \frac{\sum\limits_{k \in K(y,y')} p(k) \cdot p(d_k(y))}{\sum\limits_{k \in K(y)} p(k) \cdot p(d_k(y))} = \qquad (4.3.5)$$

$$= \frac{\sum\limits_{k \in K(y,y')} p(d_k(y))}{\sum\limits_{k \in K(y)} p(d_k(y))}.$$

Так как y встречается в каждом столбце матрицы A ровно $(\mu - 1)/2$ раз,

$$\sum_{k \in K(y)} p(d_k(y)) = \left(\sum_{x \in X} p(x) \right) \frac{\mu - 1}{2} = \frac{\mu - 1}{2}.$$

Вычислим сумму в числителе (4.3.5).

Из определения перпендикулярного массива следует, что

$$\left| K(y, y') \right| = C_\lambda^2,$$

так как в любой паре столбцов множество $\{y, y'\}$ содержится в некоторой строке, и ровно один раз. Множество строк с номерами из $K(y, y')$ разбивается на подмножества по λ строк, отличающихся друг от друга лишь циклическими сдви-

гами. При этом в каждом таком подмножестве $d_k(y)$ пробегает все X. Поэтому

$$\sum_{k\in K(y,y')} p(d_k(y)) = \left(\sum_{x\in X} p(x)\right)\frac{C_\lambda^2}{\lambda} = \frac{\lambda-1}{2}.$$

Тем самым,

$$p_1 = (\lambda-1)/(\mu-1),$$

что и требуется.

Относительно вопроса о существовании циклических перпендикулярных массивов известно не слишком много. В [Sti88], например, указывается следующий результат (приведем его без доказательства).

Теорема 4.3.6. *Пусть* λ *четно,* $\mu = p^m, \mu \equiv 1(\mathrm{mod}\, 2\lambda)$. *Тогда существует циклический перпендикулярный массив* $CPA_1(2,\lambda,\mu)$.

В [Soe88] для построения оптимальных $(L, L-1)$-шифров использованы штейнеровы системы (см. определение 2.3.3) и конечные геометрии. Имеет место, например, следующий результат (который мы приводим без доказательства).

Теорема 4.3.7. *Штейнерова система* $L-(\mu,\lambda,1)$ *определяет оптимальный* $(L, L-1)$*-шифр* $\sum_{\mathrm{B}}$ *с параметрами*

$$|X| = \lambda,\ |Y| = \mu,\ |K| = \mu!(\lambda-L)!/(\mu-L)!.$$

В [Soe88] теорема 4.3.2 уточняется следующим образом.

Теорема 4.3.8. *Если шифр* $\sum_{\text{В}}$ *удовлетворяет условию* $U(L')$*-стойкости и условию* L*-стойкости к попытке обмана, то*

$$\pi \geq \frac{C_{\mu}^{L+1} \cdot C_{\lambda}^{L'}}{C_{\lambda}^{L+1}}. \tag{4.3.6}$$

Доказательство. Так же как в теореме 4.3.2, доказывается, что

$$Y_{\text{р}}(L+1) = Y(L+1). \tag{4.3.7}$$

Выберем произвольное подмножество $Y' \in Y_{\text{р}}(L+1)$, а в нем — произвольное подмножество Y'' мощности L'. Так как шифр $\sum_{\text{В}}$ является $U(L')$-стойким, для любого $X'' \in X(L')$ справедливо неравенство

$$\left|K(X'', Y'')\right| \geq 1. \tag{4.3.8}$$

Заметим, что если $X_1'' \neq X_2''$, то

$$K(X_1'', Y'') \cap K(X_2'', Y'') = \varnothing. \tag{4.3.9}$$

Из (4.3.7) — (4.3.9) следует, что при всех возможных выборах подмножеств Y', Y'', X'' мы получим не менее

$$C_{\mu}^{L+1} \cdot C_{L+1}^{L'} \cdot C_{\lambda}^{L'}$$

(не обязательно различных!) ключей. Очевидно, что при этом подсчете один и тот же ключ k будет учтен столько раз, сколько имеется различных дополнений множества Y'' до

некоторого подмножества $L+1$ мощности $L+1$ внутри множества $e_k(X)$. Поскольку число указанных дополнений равно $C_{\lambda-L'}^{L+1-L'}$, то

$$\pi \geq \frac{C_{\mu}^{L+1} \cdot C_{L+1}^{L'} \cdot C_{\lambda}^{L'}}{C_{\lambda-L'}^{L+1-L'}},$$

откуда следует неравенство (4.3.6).

Отметим в заключение, что для построения имитостойких $U(L)$-стойких шифров помимо циклических перпендикулярных массивов, в [Sti90] использован еще один частный класс перпендикулярных массивов.

Определение 4.3.9. *Перпендикулярный массив $A = PA_{\omega}(t,\lambda,\mu)$ называется аутентификационным перпендикулярным массивом (и обозначается $APA_{\omega}(t,\lambda,\mu)$). если выполняется следующее условие:*

"для любого t', $t' \leq t$, и любого подмножества элементов $Y' = \{y_1, \Lambda, y_{t'+1}\}$ в строках матрицы A, содержащих Y', любое подмножество из Y', состоящее из t' элементов, входит во все возможные подмножества из t' столбцов матрицы одинаковое число раз".

Приведем (без доказательства) обзор некоторых результатов из [Sti90].

Теорема 4.3.10. *Если существует ортогональный массив $APA_{\omega}(t,\lambda,\mu)$, то существует шифр $\sum_{\mathrm{B}}$, удовлетворяющий*

условиям $U(L)$*-стойкости,* $(L-1)$*-стойкости к попытке обмана, и имеющий параметры*

$$|X| = \lambda,\ |Y| = \mu,\ |K| = \omega \cdot C_\mu^t.$$

Доказывается частичное обращение этой теоремы:

Теорема 4.3.11. *Если существует шифр* Σ_B *с параметрами*

$$|X| = \lambda,\ |Y| = \mu,\ |K| = C_\mu^t,$$

удовлетворяющий условиям $U(L)$*-стойкости и* $(L-1)$*-стойкости к попытке обмана для любого распределения* $P(X)$ *и* $\lambda \geq 2t-1$*, то существует перпендикулярный массив* $APA_1(t, \lambda, \mu)$.

Имеется ряд частных результатов о оптимальных $(L, L-1)$- и (L, L)-шифрах.

Теорема 4.3.12. *Перпендикулярный массив* $APA_1(2, \lambda, \mu)$ *существует тогда и только тогда, когда* λ *нечетно и* $\mu \equiv 1 (\mathrm{mod}\, 2\lambda)$ *является степенью простого числа. Следовательно, для любых указанных значений* λ, μ *существует оптимальный* $(2,1)$*-шифр.*

Теорема 4.3.13. *Для любого натурального числа* d *существуют перпендикулярные массивы* $APA_1(3,8,7^d+1)$ *и* $APA_1(3,32,31^d+1)$*. Следовательно, существуют оптимальные* $(3,2)$*-шифры с параметрами*

$$\lambda = q+1,\ \ \mu = q^d + 1,$$

где $q \in \{7,31\}$.

Теорема 4.3.14. *Для любого числа* q, *являющегося степенью простого числа, и для любого* $d \geq 2$ *существует оптимальный* $(1,1)$*-шифр с произвольным распределением* $P(X)$, *имеющий параметры*

$$\lambda = q+1,\ \ \mu = (q^{d+1}-1)/(q-1),\ \ \pi = \mu(\mu-1)/(\lambda-1).$$

Теорема 4.3.15. *Для любого простого числа Ферма* $q = 2^n + 1$ *существует оптимальный* $(2,2)$*-шифр с произвольным распределением* $P(X)$, *имеющий параметры*

$$\lambda = q,\ \ \mu = (q-1)^d + 1,\ \ \pi = \mu(\mu-1)(\mu-2)/2(\lambda-2).$$

Дальнейшие результаты о свойствах аутентификационных перпендикулярных массивов $APA_\omega(t,\lambda,\mu)$, основанные на теории схем и теории групп подстановок, получены в [Bie94], [Tr95] и [Bi96]. В [Tr95] приведена таблица (состоящая из 154 позиций) известных массивов $APA_\omega(t,\lambda,\mu)$ для $t \geq 3$.

В [Cas98] изучаются, в частности, $U(L)$-стойкие шифры с минимальными значениями вероятностей p_i, $i = \overline{0,L}$, и обладающие минимальным (в определенном смысле) числом ключей. Предлагаются конструкции таких шифров на основе ортогональных массивов. В связи с их громоздкостью мы их не приводим.

В [Cas98] уточняется также теорема 4.2.11:

Теорема 4.3.16. *Пусть* $\sum_{\text{B}}$ — $U(L)$*-стойкий шифр и шифр* $\sum'_{\text{B}}$ *отличается от* $\sum_{\text{B}}$ *лишь распределением вероятностей на множестве открытых текстов. Тогда шифр* $\sum'_{\text{B}}$ *также* $U(L)$*-стоек и имеет равное с* $\sum_{\text{B}}$ *значение вероятности* p_{L-1}.

Глава 5

Понятие совершенного шифра для других криптоатак

Выше рассматривались условные вероятности $p(X'/Y')$, $P(Y'/X')$ в случае, когда $|X'|=|Y'|$. Рассмотрим подобные величины для множеств X', Y', не обязательно имеющих одинаковые мощности. При этом будем рассматривать лишь случай, когда $|X'|\le|Y'|$, исходя из естественного предположения о том, что все, что шифруется и передается по линии связи, перехватывается оппонентом.

Пусть X', X'' — подмножества множества X и $P\{X'/X'\subset X''\}$ — вероятность выбора X' из X, при условии, что $X'\subset X''$. Обозначим эту вероятность $p(X'/X'')$. Она вычисляется по формуле

$$p(X'/X'')=\frac{p(X')}{\sum\limits_{X\in X(L_1)\cap B(X'')}p(X)}, \qquad (5.1)$$

где

$$|X'|=L_1,\ |X''|=L_2,\ L_1\le L_2,$$

и $B(X'')$ — множество всех подмножеств множества X''.

Пусть $X'\in X(L_1)$, $Y'\in Y_{\mathrm{P}}(L_2)$, причем $L_1\le L_2$. Тогда вероятность $p(Y'/X')$ того, что получено множество криптограмм Y' при условии, что на некотором ключе шифровалось множество открытых текстов, содержащее X', вычисляется согласно формуле полной вероятности:

$$p(Y'/X') = \sum_{X''\in X(L_2),\, X'\subset X''} p(Y'/X'')\cdot p(X', X''), \quad (5.2)$$

где через $p(X', X'')$ обозначена вероятность

$$p((X''\setminus X')/(X\setminus X')).$$

Это так, поскольку при заданном подмножестве открытых текстов X' получение множества криптограмм Y' возможно лишь при зашифровании на некотором ключе множества открытых текстов X'' той же мощности, что и Y', содержащего X'. В связи с этим вероятность $p(Y'/X'')$ следует "взвесить" условной вероятностью $p((X''\setminus X')/(X\setminus X'))$.

Можно проверить, что

$$\sum_{Y'\in Y_{\mathrm{P}}(L_2)} p(Y'/X') = 1.$$

В самом деле, в соответствии с (5.2) и (5.1)

$$\sum_{Y'\in Y_{\mathrm{P}}(L_2)} p(Y'/X') = \sum_{Y'\in Y_{\mathrm{P}}(L_2)} \sum_{\substack{X''\in X(L_2)\\ X'\subset X''}} p(Y'/X'')\cdot p(X', X'') =$$

$$= \sum_{Y'\in Y_{\mathrm{P}}(L_2)} \left(\sum_{\substack{X''\in X(L_2)\\ X'\subset X''}} \frac{p(X''\setminus X')}{\sum_{X\in X(L_2-L_1)\cap B(X\setminus X')} p(X)} \cdot \left(\sum_{e\in E(X'',Y')} p(e) \right) \right) =$$

$$= \frac{1}{\sum\limits_{\tilde{X}} p(\tilde{X})} \cdot \left(\sum_{Y' \in Y_{\mathrm{p}}(L_2)} \sum_{\substack{X'' \in X(L_2) \\ X' \subset X''}} \sum_{e \in E(X'', Y')} p(X'' \setminus X') \cdot p(e) \right) =$$

$$= \frac{1}{\sum\limits_{\tilde{X}} p(\tilde{X})} \cdot \left(\sum_{\substack{X'' \in X(L_2) \\ X' \subset X''}} \sum_{Y' \in Y_{\mathrm{p}}(L_2)} \sum_{e \in E(X'', Y')} p(X'' \setminus X') \cdot p(e) \right) =$$

$$= \frac{1}{\sum\limits_{\tilde{X}} p(\tilde{X})} \cdot \left(\sum_{\substack{X'' \in X(L_2) \\ X' \subset X''}} p(X'' \setminus X') \left(\sum_{Y' \in Y_{\mathrm{p}}(L_2)} \sum_{e \in E(X'', Y')} p(e) \right) \right) =$$

$$= \frac{1}{\sum\limits_{\tilde{X}} p(\tilde{X})} \left(\sum_{\substack{X'' \in X(L_2) \\ X' \subset X''}} p(X'' \setminus X') \cdot 1 \right) = 1,$$

где во внешней сумме $\tilde{X}$ пробегает множество значений из $X(L_2 - L_1) \cap B(X \setminus X')$.

Условная вероятность $p(X'/Y')$ определяется через вероятность $p(Y'/X')$ обычным образом.

Теперь, следуя [Sti88], введем еще одно условие совершенной стойкости шифра.

Определение 5.1. *Будем говорить, что шифр* Σ_{B} *удовлетворяет условию* $S(L)$*-стойкости (или является* $S(L)$*-стойким), если при любых* $Y' \in Y_{\mathrm{p}}(L')$ *и* $X' \in X(L'')$, *таких что* $L' \le L$ *и* $L'' \le L'$ *выполняется равенство*

$$p(X'/Y') = p(X'). \tag{5.3}$$

Буква S в названии условия (которое можно было назвать также *совершенной L-кратной стойкости по Стинсону*) – это первая буква фамилии *Stinson*.

Ясно, что (5.3) равносильно равенству

$$p(Y'/X') = p(Y'), \tag{5.4}$$

которым бывает удобнее пользоваться.

Непосредственно из введенных определений следует

Лемма 5.2. *Если шифр $\sum_{\mathrm{B}}$ удовлетворяет условию $S(L)$-стойкости, то он удовлетворяет и условиям $U(L')$- и $S(L')$-стойкости для любого L' из интервала $1 \le L' \le L$.*

Заметим, что условие $S(L)$-стойкости, вообще говоря, сильнее условия $U(L)$-стойкости. В самом деле, любой шифр $\sum_{\mathrm{B}}$ удовлетворяет условию $U(\lambda)$-стойкости (где $\lambda = |E|$). Это следует из того, что для любого $Y' \in Y_{\mathrm{P}}(\lambda)$

$$p(Y') = \sum_{(X',e):e(X')=Y'} p(X') \cdot p(e) =$$

$$= \sum_{e:e(X)=Y'} p(X) \cdot p(e) = \sum_{e:e(X)=Y'} p(e) = p(Y'/X).$$

При этом мы воспользовались упомянутым в § 4.1 равенством $p(X) = 1$.

Вместе с тем, шифр $\sum_{\mathrm{B}}$ не обязан быть $S(\lambda)$-стойким. Чтобы убедиться в этом, достаточно рассмотреть любой не совершенный (по Шеннону) шифр, который, тем самым, не является $U(1)$-стойким, и тем более — $S(\lambda)$-стойким.

Лемма 5.3. *Шифр* $\Sigma_{\text{В}}$ *удовлетворяет условию* $S(L)$*-стойкости тогда и только тогда, когда он удовлетворяет условию* $U(L')$*-стойкости для любого* L', $1 \le L' \le L$.

Доказательство. Необходимость условия была отмечена в лемме 5.2. Проверим достаточность. Пусть $X' \in X(L_2), Y' \in Y_{\text{Р}}(L_1)$, причем $L_2 \le L_1$. В соответствии с формулой (5.2),

$$p(Y'/X') = \sum_{\substack{X'' \in X(L_1), \\ X' \subset X''}} p(Y'/X'') \cdot p(X', X'') \underset{(U(L_1)-\text{ст.})}{=}$$

$$= \sum_{\substack{X'' \in X(L_1), \\ X' \subset X''}} p(Y') \cdot p(X', X'') =$$

$$= p(Y') \cdot \sum_{\substack{X'' \in X(L_1), \\ X' \subset X''}} p(X', X'') = p(Y').$$

Это доказывает достаточность условия леммы.

Следующее определение вводит условие стойкости шифра для упорядоченных наборов открытых и шифрованных текстов. Пусть $\bar{x} \in \bar{X}(L)$.

Определение 5.4. *Будем говорить, что шифр* $\Sigma_{\text{В}}$ *удовлетворяет условию* $O(L)$*-стойкости, если при любых* $\bar{x} \in \bar{X}(L)$, $\bar{y} \in \bar{Y}_{\text{Р}}(L)$ *выполняется равенство*

$$p(\bar{x}/\bar{y}) = p(\bar{x}). \tag{5.5}$$

Отметим, что буква O в этом определении — это первая буква слова *Ordered* (упорядоченный).

Ясно, что вместо равенства (5.5) может быть использовано равенство $p(\bar{y}/\bar{x}) = p(\bar{y})$. Очевидно также, что $O(L)$-стойкий шифр обязан обладать свойством транзитивности, согласно которому для любых $\bar{x} \in \bar{X}(L)$, $\bar{y} \in \bar{Y}_{\mathrm{P}}(L)$ должен существовать элемент $e \in E$ такой, что $e(\bar{x}) = \bar{y}$.

Лемма 5.5. *Если эндоморфный шифр* $\sum_{\mathrm{B}}$ *удовлетворяет условию* $O(L)$*-стойкости, то он удовлетворяет и условию* $O(L')$*-стойкости для любого* $L' < L$.

Доказательство. Пусть $\bar{x} \in \bar{X}(L-1)$, $\bar{y} \in \bar{Y}_{\mathrm{P}}(L-1)$, и $(\bar{x}, x) \in \bar{X}(L)$ — вектор, полученный добавлением к $\bar{x}$ дополнительной координаты $x \in X \setminus \mathrm{supp}(\bar{x})$, где $\mathrm{supp}(\bar{x})$ — множество элементов, составляющих вектор $\bar{x}$. Пусть также $(\bar{y}, y)$ — вектор из $\bar{Y}_{\mathrm{P}}(L)$, полученный аналогичным образом из вектора $\bar{y}$. Введем обозначение

$$E(\bar{x}, \bar{y}) = \{e \in E : e(\bar{x}) = \bar{y}\}.$$

По условию $e(X) = X$ для любого $e \in E$, поэтому выполняется равенство

$$\mathop{\mathrm{I}}_{e \in E(\bar{x}, \bar{y})} e(X) = X.$$

Выберем произвольный элемент

$$y_0 \in \left(\mathop{\mathrm{I}}_{e \in E(\bar{x}, \bar{y})} e(X) \right) \setminus \mathrm{supp}(\bar{y}).$$

Непосредственно проверяется равенство множеств

$$E(\bar{x},\bar{y}) = \mathop{\mathrm{Y}}_{x\in X\setminus \mathrm{supp}(\bar{x})} E((\bar{x},x),(\bar{y},y_0)),$$

причем, если $x \neq x'$, то

$$E((\bar{x},x),(\bar{y},y_0)) \cap E((\bar{x},x'),(\bar{y},y_0)) = \varnothing.$$

Рассмотрим вероятность $p(\bar{y}/\bar{x})$. Согласно (4.1.3′),

$$p(\bar{y}/\bar{x}) = \sum_{e\in E(\bar{x},\bar{y})} p(e).$$

Отсюда следует, что

$$p(\bar{y}/\bar{x}) = \sum_{x\in X\setminus \mathrm{supp}(\bar{x})} p\big((\bar{y},y_0)/(\bar{x},x)\big).$$

Пользуясь условием $O(L)$-стойкости, получаем:

$$p(\bar{y}/\bar{x}) = \sum_{x\in X\setminus \mathrm{supp}(\bar{x})} p(\bar{y},y_0) = (\lambda - L + 1)\cdot p((\bar{y},y_0)) =$$

$$= \sum_{x\in X\setminus \mathrm{supp}(\bar{x}')} p\big((\bar{y},y_0)/(\bar{x}',x)\big) = p(\bar{y}/\bar{x}'),$$

где $\bar{x}'$ — любой вектор из $\overline{X}(L-1)$.

Пусть $p(\bar{y}/\bar{x}) = q$ для любого $\bar{x}\in \overline{X}(L-1)$. Тогда, пользуясь свойством транзитивности шифра, получаем равенства

$$p(\bar{y}) = \sum_{\bar{x}\in \overline{X}(L-1)} p(\bar{y}/\bar{x})\cdot p(\bar{x}) = q\cdot \sum_{\bar{x}\in \overline{X}(L-1)} p(\bar{x}) = q.$$

Следовательно, для любых элементов $\bar{x} \in \overline{X}(L-1)$, $\bar{y} \in \overline{Y}_{\mathrm{P}}(L-1)$ выполняется равенство $p(\bar{y}/\bar{x}) = p(\bar{y})$, что и требуется.

По-видимому, лемма 5.5 справедлива и без условия эндоморфности шифра.

Лемма 5.6. *Если эндоморфный шифр* $\sum_{\mathrm{B}}$ *удовлетворяет условию* $O(L)$*-стойкости, то он удовлетворяет и условию* $S(L)$*-стойкости.*

Доказательство. Согласно леммам 5.3 и 5.5, достаточно доказать, что условие $O(L)$-стойкости влечет условие $U(L)$-стойкости.

Пусть $X' \in X(L)$, $Y' \in Y_{\mathrm{P}}(L)$. Рассмотрим вероятность $p(Y'/X')$. Непосредственно проверяется, что для любого вектора $\bar{y}$ такого, что $\mathrm{supp}(\bar{y}) = Y'$ выполняется соотношение

$$E(X', Y') = \bigcup_{\bar{x}:\mathrm{supp}(\bar{x})=X'} E(\bar{x}, \bar{y}),$$

причем

$$E(\bar{x}, \bar{y}) \cap E(\bar{x}', \bar{y}) = \varnothing,$$

если $\bar{x} \neq \bar{x}'$. В силу этого, если $\mathrm{supp}(\bar{y}) = Y'$, то

$$p(Y'/X') = \sum_{e \in E(X', Y')} p(e) =$$

$$= \sum_{\bar{x}:\mathrm{supp}(\bar{x})=X'} \sum_{e \in E(\bar{x}, \bar{y})} p(e) = \sum_{\bar{x}:\mathrm{supp}(\bar{x})=X'} p(\bar{y}/\bar{x}) \underset{(O(L)\text{–ст.})}{=}$$

$$= L! \cdot p(\bar{y}) = p(Y'),$$

что и требуется. Лемма доказана.

Отметим, что, вообще говоря, условие $O(L)$-стойкости сильнее условия $S(L)$-стойкости. Это вытекает из следующего примера.

Пример 5.7. Рассмотрим шифр Σ_{B}, для которого

$$X=\{x_0,x_1,x_2\},\ Y=\{y_0,y_1,y_2\},\ E=\{e_0,e_1,e_2\},$$
$$e_i(x_j)=y_k,$$

где $k=i+j(\mathrm{mod}\,3)$. Пусть $p(e_i)=1/3$ для любого $i=\overline{0,2}$.

Покажем, что (независимо от распределения вероятностей на X) данный шифр удовлетворяет условию $S(2)$-стойкости, но не удовлетворяет условиям $S(3)$-стойкости и $O(2)$-стойкости.

Для удобства рассмотрим матрицу зашифрования:

	x_0	x_1	x_2
e_0	y_0	y_1	y_2
e_1	y_1	y_2	y_0
e_2	y_2	y_0	y_1

В определении 5.1 будем различать три случая:

1) $L''=L'=1$; 2) $L''=1, L'=2$; 3) $L''=L'=2$.

В случае 1) надо показать, что $p(x_i/y_j)=p(x_i)$. Имеем:

$$p(x_i / y_j) = \frac{p(y_j / x_i) \cdot p(x_i)}{p(y_j)}.$$

Из условия следует, что найдется единственный элемент e_{j-i}, связывающий x_i и y_j: $e_{j-i}(x_i) = y_j$. Поэтому

$$p(y_j / x_i) = p(e_{j-i}) = 1/3.$$

С другой стороны,

$$p(y_j) = 1/3 \cdot \sum_{i=0}^{2} p(x_i) = 1/3,$$

что и требуется.

Пусть в случае 2)

$$Y_1 = \{y_0, y_1\},\ Y_2 = \{y_0, y_2\},\ Y_3 = \{y_1, y_2\}.$$

Тогда $Y_{\mathrm{P}}(2) = \{Y_1, Y_2, Y_3\}$.

Вероятность $p(x_i / Y_j)$ вычислим по формуле

$$p(x_i / Y_j) = \frac{p(Y_j / x_i) \cdot p(x_i)}{p(Y_j)},$$

где для любого $j = \overline{0,2}$

$$p(Y_j) = 1/3 \cdot [p(\{x_0, x_1\}) + p(\{x_0, x_1\}) + p(\{x_1, x_2\})] = 1/3.$$

Вычислим $p(Y_j / x_i)$. Пусть, например, $Y_j = Y_1$, $x_i = x_0$. Тогда

$$p(Y_j / x_i) = \frac{p(\{x_0, x_1\}) \cdot p(\{y_0, y_1\}/\{x_0, x_1\})}{p(\{x_0, x_1\}) + p(\{x_0, x_2\})} +$$

$$+ \frac{p(\{x_0, x_2\}) \cdot p(\{y_0, y_1\}/\{x_0, x_2\})}{p(\{x_0, x_1\}) + p(\{x_0, x_2\})} = \frac{1}{3},$$

поскольку

$$p(\{y_0, y_1\}/\{x_0, x_2\}) = p(e_1) =$$

$$= 1/3 = p(e_0) = p(\{y_0, y_1\}/\{x_0, x_1\}).$$

Таким образом,

$$p(x_i / Y_j) = p(x_i).$$

Пусть в случае 3)

$$X_1 = \{x_0, x_1\}, \ X_2 = \{x_0, x_2\}, \ X_3 = \{x_1, x_2\}.$$

Тогда

$$p(X_i / Y_j) = \frac{p(Y_j / X_i) \cdot p(X_i)}{p(Y_j)} = \frac{1/3 \cdot p(X_i)}{1/3} = p(X_i).$$

Тем самым, условие $S(2)$-стойкости для данного шифра выполнено. Вместе с тем, условие $O(2)$-стойкости не выполняется. В самом деле,

$$p((x_0, x_1)/(y_1, y_0)) = \frac{p((y_1, y_0)/(x_0, x_1)) \cdot p((x_0, x_1))}{p((y_1, y_0))} = 0,$$

так как

$$p((y_1, y_0)/(x_0, x_1)) = 0.$$

С другой стороны, $p((x_0, x_1)) > 0$.

Несложно проверить, что рассматриваемый шифр не удовлетворяет условию $S(3)$-стойкости.

Определения 4.2.1, 5.1 и 5.4 относились лишь к атакам на основе шифртекста, когда по L данным криптограммам требовалось получить информацию о передаваемых открытых сообщениях. Далее рассмотрим вопрос о совершенной стойкости шифра к атаке на основе известного открытого текста.

По Мэсси ([God90]) суть такой *атаки порядка* L состоит в том, чтобы на основании данных $L-1$ пар открытых и шифрованных текстов, полученных на одном ключе, определить открытый текст еще одной криптограммы y, полученной на том же ключе. Атака считается успешной, если найдется открытый текст x, для которого апостериорная вероятность того, что он соответствует y, отлична от его априорной вероятности. Такая постановка задачи возникает, например, при использовании блочного шифра в режиме простой замены.

Формализуем сказанное. Пусть $\sum_{\mathrm{B}}$ — рассматриваемый шифр;

$$\bar{x}' \in \bar{X}(L'-1),\ \bar{y}' \in \bar{Y}_{\mathrm{p}}(L'-1)$$

— данные совокупности открытых и соответствующих им шифрованных текстов, полученных на некотором одном (неизвестном) ключе; y — еще одна данная криптограмма, полученная на том же ключе из некоторого (неизвестного) открытого текста $x \in X \setminus \mathrm{supp}(\bar{x}')$. Пусть $\bar{y} = (\bar{y}', y)$, $\bar{x} = (\bar{x}', x)$. Будем случайно выбирать $\bar{x}'$ и $\bar{y}$, после чего случайно выбирать $x \in X \setminus \mathrm{supp}(\bar{x}')$. Этот выбор

определяет условные вероятности $p(\bar{x}/\bar{x}')$ и $p(\bar{x}/\bar{y},\bar{x}')$, исходя из формул

$$p(\bar{x}/\bar{x}') = \frac{p(\bar{x},\bar{x}')}{p(\bar{x}')},$$

$$p(\bar{x}/\bar{y},\bar{x}') = \frac{p(\bar{x},\bar{y},\bar{x}')}{p(\bar{y},\bar{x}')} = \frac{p(\bar{x},\bar{x}')\cdot p(\bar{y}/\bar{x},\bar{x}')}{p(\bar{x}')\cdot p(\bar{y}/\bar{x}')} =$$

$$= \frac{p(\bar{x}/\bar{x}')\cdot p(\bar{y}/\bar{x})}{p(\bar{y}/\bar{x}')},$$

где (по аналогии с (5.2)) вероятность $p(\bar{y}/\bar{x}')$ определяется формулой

$$p(\bar{y}/\bar{x}') = \sum_{x\in X\setminus \mathrm{supp}(\bar{x}')} p(\bar{y}/(\bar{x}',x))\cdot p\big(\{x\}/\big(X\setminus \mathrm{supp}(\bar{x}')\big)\big).$$

Определение 5.8. *Будем говорить, что шифр* Σ_{B} *удовлетворяет условию* $M(L)$*-стойкости (или является* $M(L)$*-стойким), если для любых указанных выше* $\bar{x},\bar{y},$ *и любого* $L'\le L$ *выполняется равенство*

$$p(\bar{x}/\bar{y},\bar{x}') = p(\bar{x}/\bar{x}'). \tag{5.6}$$

Ясно, что равенство (5.6) равносильно равенству

$$p(\bar{y}/\bar{x}) = p(\bar{y}/\bar{x}'). \tag{5.6'}$$

Легко видеть, что из условия $M(L)$-стойкости следует условие $M(L')$-стойкости для любого $L'\le L$.

Лемма 5.9. *Если шифр* $\sum_{\mathrm{B}}$ *удовлетворяет условию* $O(L)$*-стойкости, то он удовлетворяет и условию* $M(L)$*-стойкости.*

Доказательство. Проверим для подходящих $\bar{x}, \bar{x}', \bar{y}$ справедливость равенства (5.6′). Согласно условию, $p(\bar{y}/\bar{x}) = p(\bar{y})$. Следовательно,

$$p(\bar{y}/\bar{x}') = \sum_{x \in X \setminus \mathrm{supp}(\bar{x}')} p(\bar{y}/(\bar{x}', x)) \cdot p(\{x\}/(X \setminus \mathrm{supp}(\bar{x}'))) =$$

$$\sum_{x \in X \setminus \mathrm{supp}(\bar{x}')} p(\bar{y}) \cdot p(\{x\}/(X \setminus \mathrm{supp}(\bar{x}'))) =$$

$$= p(\bar{y}) \cdot \sum_{x \in X \setminus \mathrm{supp}(\bar{x}')} p(\{x\}/(X \setminus \mathrm{supp}(\bar{x}'))) = p(\bar{y}) = p(\bar{y}/\bar{x}),$$

откуда следует (5.6′).

Заметим, что обратное утверждение неверно. Чтобы убедиться в этом, достаточно рассмотреть следующий пример.

Пример 5.10. Пусть шифр $\sum_{\mathrm{B}}$ таков, что

$$X = \{x_0, x_1\},\ Y = \{y_0, y_1, y_2\},\ E = \{e_0, e_1, e_2\},$$

причем

$$e_i(x_j) = y_k,\ i + j = k (\mathrm{mod}\, 3);\ p(e_i) = 1/3,\ i = \overline{0,2}.$$

Данный шифр удовлетворяет условиям $S(2)$- и $M(2)$-стойкости, но не удовлетворяет условию $O(2)$-стойкости.

Для проверки свойства $S(2)$-стойкости будем использовать те же обозначения и рассуждения, что и в примере 5.7. Матрица зашифрования имеет следующий вид:

	x_0	x_1
e_0	y_0	y_1
e_1	y_1	y_2
e_2	y_2	y_0

В определении 5.1 рассмотрим три случая:

1) $L'' = L' = 1$; 2) $L'' = 1$, $L' = 2$; 3) $L' = L'' = 2$.

В случае 1) рассуждения те же, что и в примере 5.7. В случае 2) для любого $j = \overline{1,3}$

$$p(Y_j) = \sum_{\substack{(X',e):\\ e(X')=Y_j}} p(X') \cdot p(e) = p(X) \cdot \sum_{e:e(X)=Y_j} p(e)$$

$$= p(X) \cdot p(e_{j-1}) = 1/3.$$

Вместе с тем,

$$p(Y_j / x_i) = p(Y_j / X) = p(e_{j-1}) = 1/3.$$

Поэтому $p(x_i / Y_j) = p(x_i)$.

В случае 3):

$$p(X / Y_j) = \frac{p(Y_j / X) \cdot p(X)}{p(Y_j)} = \frac{1/3 \cdot p(X)}{1/3} = p(X).$$

Обратимся к проверке условия $M(2)$-стойкости.

Имеет смысл рассматривать лишь строки $\bar{x}$ и $\bar{y}$ длины 2. По условию $\bar{x}$ и $\bar{y}$ таковы, что найдутся $e \in E$ и

$\bar{t} = (\bar{x}', t)$, для которых $e(\bar{t}) = \bar{y}$. Строкой $\bar{x}$ может быть либо (x_0, x_1), либо (x_1, x_0). Если $\bar{x} = (x_0, x_1)$, то $\bar{x}' = (x_0)$ и $\bar{t} = \bar{x}$. Тогда $\bar{y}$ может быть одной из трех строк: (y_0, y_1), (y_1, y_2), (y_2, y_0). Аналогично для $\bar{x} = (x_1, x_0)$ получается $\bar{t} = \bar{x}$ и

$$\bar{y} \in \{(y_1 y_0), (y_2, y_1), (y_2, y_0)\}.$$

Имеем равенства:

$$p((y_0, y_1)/(x_0)) = p(e_0) = 1/3 = p((y_0, y_1)/(x_0, x_1)).$$

Аналогично можно убедиться в том, что равенство (5.6′) выполняется и во всех других случаях.

Как и в примере 5.7,

$$p((y_1, y_0)/(x_0, x_1)) = 0,$$

хотя $p((y_1, y_0)) = 1/3$. Тем самым, свойство $O(2)$-стойкости и в данном случае не выполняется.

Подведем некоторые итоги.

Имеет место следующая иерархия различных понятий стойкости шифров к атакам, основанным на совокупности криптограмм, полученных на одном ключе:

$$\begin{array}{ccccccc} M(L) & \Leftarrow & O(L) & \Rightarrow & S(L) & \Rightarrow & U(L) \\ \Downarrow & & \Downarrow & & \Downarrow & & \not\Downarrow \\ M(L-1) & \Leftarrow & O(L-1) & \Rightarrow & S(L-1) & \Rightarrow & U(L-1) \end{array}$$

Стрелки означают, что одно условие стойкости является следствием другого. Импликации

$$O(L) \Rightarrow S(L) \text{ и } O(L) \Rightarrow O(L-1)$$

доказаны лишь для эндоморфных шифров. По-видимому, они справедливы и без требования эндоморфности. Импликация $U(L) \Rightarrow U(L-1)$ может не выполняться. Далее будут указаны дополнительные условия, при которых она имеет место.

Глава 6

Свойства $U(L)$- и $S(L)$-стойких шифров

Теорема 4.3.1, дающая комбинаторное описание множества E для $U(L)$-стойкого шифра, может быть уточнена и использована для описания конструкции $S(L)$-стойкого шифра.

Теорема 6.1. *Пусть $Y = X$ и E — множество подстановок на X, рассматриваемое как множество правил зашифрования для шифра Σ_{B} с числом ключей $\pi = C_\lambda^L$, удовлетворяющего условию $U(L)$-стойкости. Тогда при $L' \le L$ шифр удовлетворяет также условию $U(L')$-стойкости тогда и только тогда, когда число C_λ^L делится на число $C_\lambda^{L'}$, и для любой пары X', $Y' \in X(L)$ существует в точности $\omega = C_\lambda^L : C_\lambda^{L'}$ подстановок $e \in E$ таких, что $e(X') = Y'$.*

Доказательство. Пусть $L' \le L$ и, как и ранее,

$$E(X', Y') = \{e \in E : e(X') = Y'\}$$

для L'-подмножеств X', Y'. Шифр Σ_{B} является $U(L')$-стойким тогда и только тогда, когда для любых $X', Y' \in X(L')$

$$p(X'/Y') = p(X') \Leftrightarrow p(Y'/X') = p(Y') \Leftrightarrow$$

$$\Leftrightarrow \sum_{e \in E(X', Y')} p(e) = p(Y') \Leftrightarrow \frac{|E(X', Y')|}{C_\lambda^L} = p(Y'). \qquad (6.1)$$

При этом мы воспользовались условием $U(L)$-стойкости, а также свойством (i) теоремы 4.3.1, согласно которому $p(e) = 1/C_\lambda^L$.

Пусть выполняется условие $U(L')$-стойкости. Зафиксируем Y' и заставим X' пробегать все $C_\lambda^{L'}$ возможные L'-подмножества из X. Тогда подмножества $E(X',Y')$ образуют разбиение множества E. В самом деле, из условия $X' \neq X''$ следует, что

$$E(X',Y') \cap E(X'',Y') = \varnothing.$$

Любая биекция $e \in E$ отображает некоторое подмножество X' на данное Y', поэтому

$$\bigcup_{X'} E(X',Y') = E.$$

Из (6.1) и сказанного выше следует, что условие $U(L')$-стойкости влечет равенство

$$\left|E(X',Y')\right| = p(Y') \cdot C_\lambda^L$$

для любого $X' \in X(L')$. Поэтому, во-первых,

$$E(X',Y') \neq \varnothing,$$

и, во-вторых,

$$\left|E(X',Y')\right| = \left|E(X'',Y')\right|$$

для любых $X', X'' \in X(L')$. Отсюда следует, что

$$\left|E(X',Y')\right| = \frac{|E|}{C_\lambda^{L'}}.$$

($C_\lambda^{L'}$ — это число различных L'-подмножеств X' из X.) Таким образом

$$\omega = \left|E(X',Y')\right| = \frac{C_\lambda^{L}}{C_\lambda^{L'}}, \tag{6.2}$$

что и требуется.

Достаточность. Пусть для любых X', Y' выполняется условие (6.2). Тогда (с учетом того, что $E(X',Y') \neq \varnothing$ для любых X', Y')

$$p(Y') = \sum_{X' \in X(L')} \sum_{e \in E(X',Y')} p(X') \cdot p(e) =$$

$$= \sum_{X' \in X(L')} p(X') \cdot \left(\frac{1}{C_\lambda^{L}} \cdot \frac{C_\lambda^{L}}{C_\lambda^{L'}} \right) = \frac{1}{C_\lambda^{L'}}.$$

Отсюда следует (6.1), а также условие $U(L')$-стойкости. Теорема доказана.

Следствие 6.2. *Пусть $Y = X$ и E — множество подстановок на X, рассматриваемое как множество правил зашифрования для шифра Σ_{B} с числом ключей $\pi = C_\lambda^L$, удовлетворяющего условию $U(L)$-стойкости. Тогда если Σ_{B} удовлетворяет условию $S(L)$-стойкости, то*

$$\frac{\lambda - L + 1}{L}, \frac{\lambda - L + 2}{L - 1}, \ldots, \frac{\lambda - 1}{2}, \lambda \tag{6.3}$$

— возрастающая последовательность целых чисел.

Доказательство следует из теоремы 6.1 и леммы 5.3.

Условие (6.3) является, таким образом, необходимым условием $S(L)$-стойкости шифра с параметрами

$$|X| = |Y| = \lambda,\ \pi = |E| = C_\lambda^L.$$

Можно заметить, что для любого $L \in \mathrm{N}$ существует $\lambda \in \mathrm{N}$, для которого выполнено условие (6.3). Например, в качестве такого λ можно взять число

$$H.O.K.(2,3,\ldots,L) - 1.$$

Рассмотрим более подробно множество подстановок, удовлетворяющих свойству (ii) теоремы 4.2.4.

Согласно теореме 6.1, изучение $S(L)$-стойких шифров в случае, когда

$$X = Y,\ |X| = \lambda,\ \pi = C_\lambda^L,$$

эквивалентно изучению $(L,1)$-однородных множеств подстановок[19] на множестве из λ элементов, которые являются также $\left(L', C_\lambda^L : C_\lambda^{L'}\right)$-однородными для каждого $L' \le L$.

Рассмотрим более подробно некоторые свойства (t,ω)-однородных множеств подстановок.

Лемма 6.3. *Если множество подстановок E является (t,ω)-однородным на X, то E является также $(\lambda - t,\omega)$-однородным на X.*

[19] Определение дано в п.4.2.6.

Доказательство. Пусть E является (t,ω)-однородным множеством подстановок на X и пусть X', X'' — произвольные $(\lambda - t)$-подмножества из X. Обозначим $\neg X' = X \setminus X'$. Тогда легко заметить, что

$$e(X') = e(X'') \Leftrightarrow e(\neg X') = e(\neg X''),$$

откуда и следует требуемое утверждение.

Лемма 6.4. *Если E является (t,ω)-однородным множеством подстановок на X, то $\pi = \omega \cdot C_\lambda^t$.*

Доказательство. По условию при фиксированном $X' \in X(t)$ и любом $X'' \in X(t)$ существует в точности ω подстановок $e \in E$, для которых $e(X') = X''$. Поэтому $|E(X', X'')| = \omega$. Всего же имеется C_λ^t t-подмножеств X''. Коль скоро при $X'' \neq X'''$

$$E(X', X'') \cap E(X', X''') = \varnothing,$$

и

$$\bigcup_{X''} E(X', X'') = E,$$

откуда следует требуемое равенство.

Лемма 6.5. *Если E является (t,ω)-однородным множеством подстановок на X, причем $1 \le t \le (\lambda+1):2$, то E является также (t',ω')-однородным на X для любого $t' \le t$, где*

$$\omega' = \left(\omega \cdot C_\lambda^t\right) : C_\lambda^{t'}.$$

Доказательство. Пусть множество подстановок E является (t,ω)-однородным на X. Для $(t-1)$-подмножеств X', Y' и числа s, $s=\overline{0,t-1}$, обозначим через $N(X',Y',s)$ величину

$$\left|\{e\in E:\left|e(X')\cap Y'\right|=s\}\right|.$$

Методом индукции по s покажем, что (при $1\le t\le(\lambda+1):2$) величина $N(X',Y',s)$ не зависит от выбора X', Y'.

Пусть $s=0$. Рассмотрим такой элемент $e\in E$ что $e(X')\cap Y'=\varnothing$. Выберем $x\in X$ таким, чтобы

$$e(x)\in X\setminus\left(e(X')\cup Y'\right).$$

Ясно, что $x\in X\setminus X'$. Дальнейшие рассуждения проиллюстрируем рисунком 6.

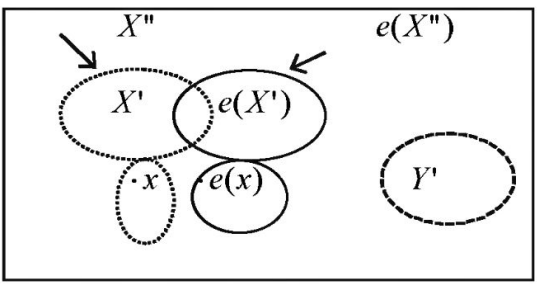


Рис.6

Всего имеется $\lambda-2(t-1)$ способов выбора такого $x\in X$ (по сути, выбирается $e(x)$, а по нему восстанавливается x), поэтому в X имеется ровно столько же t-

подмножеств X'' таких, что $X'' \supset X'$ и $e(X'') \cap Y' = \varnothing$. Отсюда следует, что при заданных

$$X',\ Y',\ |X'| = |Y'| = t-1,$$

число пар (X'', e) таких, что

$$|X''| = t,\ X'' \supset X',\ e(X'') \cap Y' = \varnothing,$$

равно

$$(\lambda - 2(t-1)) \cdot N(X', Y', 0).$$

Подсчитаем число таких пар (X'', e) другим способом, воспользовавшись тем, что E является (t, ω)-однородным множеством подстановок. Для фиксированного Y' число способов выбрать $e(X'')$ таким, чтобы $e(X'') \cap Y' = \varnothing$, равно

$$C^t_{\lambda-(t-1)}.$$

Число способов выбора $X'' = X' \cup \{x\}$ совпадает с числом способов выбора $\{x\} \in X \setminus X'$ и равно $\lambda - (t-1)$. Для каждой из выбранных пар X'', $e(X'')$ имеется (в силу однородности) ровно ω подстановок e, для которых $e : X'' \to e(X'')$. Поэтому искомое число пар (X'', e) равно

$$(\lambda - (t-1)) \cdot C^t_{\lambda-(t-1)} \cdot \omega.$$

В результате получаем равенство

$$N(X', Y', 0) = \frac{\omega \cdot C^t_{\lambda-(t-1)} \cdot (\lambda - (t-1))}{\lambda - 2(t-1)}.$$

(Обратим внимание на то, что при этом $\lambda - 2(t-1) > 0$, так как $t \le (\lambda+1):2$.)

Шаг индукции: предположим, что $s > 0$, и что проверяемое утверждение верно для любого s', $0 \le s' < s$. Подсчитаем число пар (X'', e), для которых выполняются условия

$$|X''| = t,\ X'' \supset X',\ |e(X'') \cap Y'| = s. \qquad (6.4)$$

При этом возможны два случая: когда

$$e(X') \cap Y' = e(X'') \cap Y',$$

и когда

$$e(X') \cap Y' \neq e(X'') \cap Y'.$$

В первом случае e таково, что $|e(X') \cap Y'| = s$. Соответствующее множество X'' получается дополнением к X' одного элемента x, такого, что $e(x)$ не лежит ни в X', ни в $Y' \cup e(X')$. Поэтому имеется $\lambda - 2(t-1) + s$ способов выбора такого x.

Ясно, что во втором случае

$$|e(X') \cap Y'| = s - 1.$$

Выберем опять X'' так, чтобы выполнялись условия (6.4). При этом X'' получается добавлением к X' любого одного элемента x, такого что $e(x) \in Y' \setminus e(X')$. Поэтому всего имеется

$$t - 1 - (s-1) = t - s$$

таких подмножеств X''. Таким образом, имеется в точности

$$(\lambda - 2(t-1) + s) \cdot N(X', Y', s) + (t-s) \cdot N(X', Y', s-1) \quad (6.5)$$

пар (X'', e), для которых выполняются условия (6.4).

Найдем число таких пар (X'', e) другим способом, пользуясь тем, что E является (t, ω)-однородным множеством подстановок.

При фиксированных X', Y' $t-s$ элементов в $e(X'')$ выбираются из $X \setminus Y'$ и s элементов — из Y'. Поэтому имеется

$$C_{\lambda-(t-1)}^{t-s} \cdot C_{t-1}^{s}$$

различных множеств $e(X'')$. Далее, $X'' = X' \cup \{x\}$ можно выбрать $\lambda - (t-1)$ способами (при этом x — любой элемент из $X \setminus X'$). Для каждой пары X'', $e(X'')$ имеется ровно ω различных подстановок. Поэтому число искомых пар (X'', e) равно

$$(\lambda - (t-1)) \cdot C_{\lambda-(t-1)}^{t-s} \cdot C_{t-1}^{s} \cdot \omega. \quad (6.6)$$

Получаем равенство (6.5) = (6.6), в котором величина $N(X', Y', s-1)$ не зависит от выбора X', Y' по предположению индукции. Следовательно, и $N(X', Y', s)$ также не зависит от выбора X', Y', что и требуется.

Положив теперь $s = t-1$, получим искомый результат. В самом деле, равенство $e(X') = Y'$ выполняется тогда и только тогда, когда $|e(X') \cap Y'| = t-1$. Согласно сказанному выше, число таких подстановок $e \in E$ не зависит от X', Y', что свидетельствует об однородности множества E. Число ω' находится применением леммы 6.4:

$$\pi = \omega \cdot C_\lambda^t = \omega' \cdot C_\lambda^{t-1},$$

откуда следует требуемая формула для $t' = t - 1$. Переходя от $t-1$ к $t-2$ и т. д., аналогичным образом получаем формулу для любого $t' \le t$.

Теорема 6.6. *Пусть $Y = X$ и E — множество подстановок на X, рассматриваемое как множество правил зашифрования для шифра $\sum_{\mathrm{B}}$ с числом ключей $\pi = C_\lambda^L$, удовлетворяющего условию $U(L)$-стойкости, и*

$$1 \le L \le (\lambda + 1) : 2. \tag{6.7}$$

Тогда $\sum_{\mathrm{B}}$ удовлетворяет также условию $U(L')$-стойкости при любом L', таком что

$$1 \le L' \le L \text{ или } \lambda - L \le L' \le \lambda.$$

Доказательство. По теореме 4.2.5 E является $(L,1)$-однородным множеством подстановок. Согласно лемме 6.5, при выполнении условий (6.7), E является также и (L', ω')-однородным, где $1 \le L' \le L$ и

$$\omega' = \frac{C_\lambda^L}{C_\lambda^{L'}}.$$

Тогда, согласно теореме 6.1, $\sum_{\mathrm{B}}$ является $U(L')$-стойким шифром.

Кроме того, по лемме 6.3 E является также $(\lambda - L', \omega')$-однородным множеством подстановок. Если $\lambda - L' \le L$, то,

согласно теореме 6.1, Σ_{B} является $U(\lambda - L')$-стойким шифром, что и требуется.

В заключение отметим (см. [Sti90]), что для $S(L)$-стойких шифров справедливы все результаты § 4.3 по оценке вероятностей имитации и подмены, которые были сформулированы для $U(L)$-стойких шифров. В дополнение к этому в [Cas98] получена нижняя оценка числа ключей $S(L)$-стойкого шифра, имеющего минимальное значение вероятности p_{L-1}.

Теорема 6.7. *Если для шифра* Σ_{B} *выполняется условие* $S(L)$*-стойкости,* $1 \le L \le \lambda$, *и выполняется равенство*

$$p_{L-1} = \lambda/\mu,$$

то имеет место оценка

$$\pi \ge C_{\lambda}^{L} \cdot \left(\frac{\mu}{\lambda}\right)^{L}.$$

Глава 7

Построение $O(L)$- и $M(L)$-стойких шифров

Для шифров, удовлетворяющих условию $O(L)$-стойкости, справедливы следующие аналоги лемм 4.2.2 и 4.2.3, которые доказываются совершенно аналогично.

Лемма 7.1. *Если шифр* Σ_{B} *удовлетворяет условию* $O(L)$*-стойкости, то для любого* L', $1 \le L' \le L$, *и любых строк* $\overline{y} \in \overline{Y}_{\mathrm{P}}(L')$ *и* $\overline{x} \in \overline{X}(L')$ *справедливо неравенство* $\left|E(\overline{x}, \overline{y})\right| \ge 1$.

Лемма 7.2. *Если шифр* Σ_{B} *удовлетворяет условию* $O(L)$*-стойкости, то*

$$\pi \ge \left|\overline{Y}_{\mathrm{P}}(L)\right|.$$

Более того, если $\pi = \left|\overline{Y}_{\mathrm{P}}(L)\right|$, *то*

(i) $\left|E(\overline{x}, \overline{y})\right| = 1$ *для любых* $\overline{x} \in \overline{X}(L)$, $\overline{y} \in \overline{Y}_{\mathrm{P}}(L)$;

(ii) $p(e) = p(\overline{y})$ *для любых* $e \in E$, $\overline{y} \in \overline{Y}_{\mathrm{P}}(L)$, *таких, что* $\operatorname{supp} \overline{y} \subset e(X)$.

Теорема 7.3. *Если шифр* Σ_{B} *удовлетворяет условию* $O(L)$*-стойкости, то*

$$\pi \ge \frac{\mu \cdot (\lambda - 1)!}{(\lambda - L)!}.$$

Более того, если

$$\pi = \frac{\mu \cdot (\lambda - 1)!}{(\lambda - L)!},$$

то

(i) *при* $p(e_1) = p(e_2) = p(\bar{y})$ *для любых* $e_1, e_2 \in E$ *либо* $e_1(X) = e_2(X)$, *либо* $e_1(X) \cap e_2(X) = \varnothing$;

(ii) *если* $e_1(X) = e_2(X)$, *то* $p(e_1) = p(e_2) = p(\bar{y})$ *для любого* $\bar{y} \in \overline{Y}_{\mathrm{P}}(L)$, *такого что* $\operatorname{supp} \bar{y} \subset e_1(X)$.

Доказательство. Согласно лемме 7.2 достаточно доказать, что

$$\left|\overline{Y}_{\mathrm{P}}(L)\right| \geq \frac{\mu \cdot (\lambda - 1)!}{(\lambda - L)!}. \tag{7.1}$$

Выберем $y \in Y$ и соответствующие $e \in E$, $x \in X$ такие, что $e(x) = y$. Так как $\left|e(X)\right| = \lambda$, то в $e(X)$ можно построить $A_{\lambda-1}^{L-1}$ различных продолжений множества $\{y\}$ до L-строки разрешенных элементов. В свою очередь, имеется ровно μ способов выбора y. Отсюда следует неравенство (7.1).

Пусть

$$\pi = \frac{\mu \cdot (\lambda - 1)!}{(\lambda - L)!},$$

и, следовательно,

$$\left|\overline{Y}_{\mathrm{P}}(L)\right| = \frac{\mu \cdot (\lambda - 1)!}{(\lambda - L)!}.$$

Так как каждый y является первым элементом в не менее чем $(\lambda-1)!:(\lambda-L)!$ разрешенных L-строках, и всего их ровно

$$\frac{\mu\cdot(\lambda-1)!}{(\lambda-L)!},$$

то ясно, что y начинает в точности $(\lambda-1)!:(\lambda-L)!$ разрешенных L-строк.

Пусть $L>1$. Если $y\in e(X)\cap e'(X)$, то в $e(X)$ и $e'(X)$ можно построить больше, чем $(\lambda-1)!:(\lambda-L)!$ разрешенных L-строк, чего быть не может. Следовательно, $e'(X)=e(X)$, откуда следует (i). Свойство (ii) следует из утверждения (ii) леммы 7.2.

Нижняя оценка числа ключей $O(L)$-стойкого шифра приводится в теореме 7.3. Рассмотрим сначала случай, отвечающий минимальным значениям параметров, когда

$$\mu=\lambda \text{ и } \pi=\frac{\lambda!}{(\lambda-L)!}.$$

В этом случае можно отождествить X и Y, рассматривая отображения $e\in E$ как подстановки на множестве X. Кроме того, согласно (ii) теоремы 7.3 все ключи должны быть равновероятными. При такой договоренности имеется возможность получить чисто комбинаторный критерий того, что A_λ^L подстановок на X образуют $O(L)$-стойкий шифр.

Теорема 7.4. *Пусть E — множество подстановок на множестве $X=Y$, отвечающих ключам шифра Σ_B, для которого $\pi=\lambda!:(\lambda-L)!$. Тогда такой шифр является*

$O(L)$-стойким в том и только том случае, когда выполняются следующие условия:

(i) *для любой пары* $(\bar{x}, \bar{y})$ L*-строк из* $\bar{X}(L)$ *выполняется равенство* $|E(\bar{x}, \bar{y})| = 1$;

(ii) $p(e) = (\lambda - L)!:\lambda!$ *при любом* $e \in E$.

Доказательство. Необходимость (i) следует из (ii) теоремы 7.3, а необходимость (ii) следует из (i) леммы 7.2.

Пусть выполняются (i) и (ii) и $\bar{x}, \bar{y} \in \bar{X}(L)$. Тогда

$$p(\bar{x}/\bar{y}) \underset{(опр.)}{=} \frac{p(\bar{y}/\bar{x}) \cdot p(\bar{x})}{p(\bar{y})} \underset{\substack{(e(\bar{x})=\bar{y} \\ \text{лемма 7.2})}}{=} \frac{p(e) \cdot p(\bar{x})}{p(\bar{y})} \underset{((i))}{=}$$

$$= \frac{p(\bar{x}) \cdot (\lambda - L)!}{\lambda! \cdot p(\bar{y})}.$$

Кроме того,

$$p(\bar{y}) = \sum_{\substack{(e,\bar{x}'): \\ e(\bar{x}')=\bar{y}}} p(\bar{x}') \cdot p(e) =$$

$$= \sum_{\substack{(e,\bar{x}'): \\ e(\bar{x}')=\bar{y}}} p(\bar{x}') \cdot \frac{(\lambda - L)!}{\lambda!} \underset{((ii))}{=} \frac{(\lambda - L)!}{\lambda!}.$$

В последнем равенстве используется то обстоятельство, что для любого $\bar{x}' \in \bar{X}(L)$ существует единственная подстановка $e \in E$, для которой $e(\bar{x}') = \bar{y}$, поэтому в сумме

$$\sum_{(e,\bar{x}'): e(\bar{x}')=\bar{y}} p(\bar{x}')$$

будет учтен каждый $\bar{x}'$ и ровно один раз. Отсюда получаем равенство $p(\bar{x}/\bar{y}) = p(\bar{x})$, что и требуется.

Уточнением теоремы 7.4 является следующее утверждение.

Теорема 7.5. *Пусть E – множество подстановок на множестве X, отвечающих ключам шифра Σ_B, такого что $\pi = \lambda!:(\lambda - L)!$ и удовлетворяющего условию $O(L)$-стойкости. Тогда для любого $L' \le L$ и для любых $\bar{x},\ \bar{y} \in \overline{X}(L')$ существует ровно*

$$\omega = \frac{(\lambda - L')!}{(\lambda - L)!}$$

подстановок $e \in E$, для которых $e(\bar{x}) = \bar{y}$.

Доказательство. Согласно лемме 5.5, любой эндоморфный $O(L)$-стойкий шифр является и $O(L')$-стойким при $L' \le L$. Пусть $\bar{x}, \bar{y} \in \overline{X}(L')$ и пусть, как и ранее, $E(\bar{x}, \bar{y}) = \{e \in E : e(\bar{x}) = \bar{y}\}$.

Из условия $O(L')$-стойкости имеем равенство

$$\begin{aligned} p(\bar{y}) &= p(\bar{y}/\bar{x}) = \\ &= \sum_{e \in E(\bar{x},\bar{y})} p(e) \underset{(ii)\text{т.}7.3}{=} \left|E(\bar{x},\bar{y})\right| \cdot \frac{(\lambda - L')!}{\lambda!}. \end{aligned} \tag{7.2}$$

Если зафиксировать $\bar{y}$ и заставить $\bar{x}$ пробегать все $\lambda!:(\lambda - L')!$ возможных значений элементов из $\overline{X}(L')$, то получим разбиение

$$E = \bigcup_{\bar{x} \in \bar{X}(L')} E(\bar{x}, \bar{y})$$

множества E. А так как левая часть в (7.2) постоянна, то

$$|E| = |E(\bar{x}, \bar{y})| \cdot |\bar{X}(L')|$$

и

$$E(\bar{x}, \bar{y}) = \frac{|E| \cdot (\lambda - L')!}{\lambda!} = \frac{(\lambda - L')!}{(\lambda - L)!},$$

что и требуется.

Определение 7.6. *Множество E подстановок на множестве X называется (t, ω)-транзитивным в том и только том случае, если для любой пары строк $\bar{x}, \bar{y} \in \bar{X}(t)$ существует ровно ω подстановок из E, для которых $e(\bar{x}) = \bar{y}$.*

Согласно теореме 7.4, выяснение свойства $O(L)$-стойкости шифра с $\pi = \lambda!:(\lambda - L)!$ ключами в точности эквивалентно выяснению свойства $(L,1)$-транзитивности множества подстановок на множестве из λ элементов. Поэтому задача построения $O(L)$-стойкого шифра с минимальным числом ключей (а по лемме 5.9 — и $M(L)$-стойкого шифра) равносильна задаче построения $(L,1)$-транзитивного множества подстановок мощности $\lambda!:(\lambda - L')!$. Из теоремы 7.5 следует также, что всякое $(L,1)$-транзитивное множество подстановок является и

$$\left(i, \frac{(\lambda - i)!}{(\lambda - L)!}\right)\text{-транзитивным}$$

для любого i, $1 \le i \le L$.

Случай $L = 1$ был уже рассмотрен ранее. При $L \ge 2$ примеры соответствующих множеств подстановок дает теория групп подстановок.

Если E — подгруппа симметрической группы S_λ, то E является (t, ω)-транзитивным множеством подстановок тогда и только тогда, когда E является t-транзитивной группой. В самом деле, очевидно, что условие (t, ω)-транзитивности множества подстановок E влечет условие его t-транзитивности. Обратно, пусть E — t-транзитивная группа подстановок и $\bar{x} \in \bar{X}(t)$. Рассмотрим стабилизатор

$$E_{\bar{x}} = \{e \in E : e(\bar{x}) = \bar{x}\} < E$$

точки $\bar{x}$ в группе E и разложим E в смежные классы по подгруппе $E_{\bar{x}}$:

$$E = E_{\bar{x}} \cdot e_1 \cup \ldots \cup E_{\bar{x}} \cdot e_n,$$

где

$$n = \left|\bar{X}(t)\right|, \quad e_i(\bar{x}) = \bar{x}_i \in \bar{X}(t).$$

Тогда

$$E_{\bar{x}} \cdot e_i = E(\bar{x}, \bar{x}_i)$$

и

$$\left|E_{\bar{x}}\right| = \left|E_{\bar{x}} \cdot e\right| = \left|E(\bar{x}, \bar{y})\right| = \omega.$$

Свойство $(t,1)$-транзитивности отвечает точно t-транзитивной группе. Известны два семейства простых примеров t-транзитивных групп — это группы S_λ и A_λ. Симметрическая группа S_λ точно λ-транзитивна. Она дает примеры минимальных по ключам $O(\lambda)$- и $M(\lambda)$-стойких шифров. Знакопеременная группа A_λ точно $(\lambda-2)$-транзитивна и дает примеры минимальных по ключам $O(\lambda-2)$- и $M(\lambda-2)$-стойких шифров.

Точно 2- и 3-транзитивные группы известны для бесконечного множества значений λ. Например (см. [Глу90]), при $\lambda = p^n$, где p — простое число, *полная аффинная группа* $AGL(1,\lambda)$ точно 2-транзитивна, а *проективная линейная группа* $PGL(2,\lambda)$ точно 3-транзитивна.

Ситуация резко меняется для $t \geq 4$. Кроме S_λ и A_λ, t-транзитивными группами являются только *группы Матье*[20]: M_{11}, M_{12}, M_{23}, M_{24} (группа M_i действует на множестве из i элементов). Группы M_{11}, M_{23} — 4-транзитивны, группы M_{12}, M_{24} — 5-транзитивны. При этом M_{11} — точно 4-транзитивна, M_{12} — точно 5-транзитивна, M_{23}, M_{24} не являются точно 4-транзитивными (и 5-транзитивными).

В 1873 г. К.Жорданом доказано, что при $t \geq 6$ точно t-транзитивных групп, отличных от S_t, A_t, не существует. Таким образом, M_{11} и M_{12} (порядков 7920 и 95040) — единственные нетривиальные примеры точно t-транзитивных групп для $t \geq 4$.

---

[20] Они были найдены французским математиком Э.П.Матье (1835–1890) и носят его имя.

Укажем задание групп Матье образующими элементами, как подгрупп симметрических групп соответствующих степеней ([Холл62]):

$M_{11} =< a_1, a_2, a_3, a_4, a_5 >$, где

$a_1 = (1,2,3)(4,5,6)(7,8,9),$
$a_2 = (2,4,3,7)(5,6,9,8),$
$a_3 = (2,5,3,9)(4,8,7,6),$
$a_4 = (1,10)(4,5)(6,8)(7,9),$
$a_5 = (1,11)(4,6)(5,9)(7,8),$
$a_6 = (1,12)(4,7)(5,6)(8,9).$

$M_{12} =< M_{11}, a_6 >$, причем стабилизатор точки 12 в M_{12} совпадает с M_{11}.

$M_{23} =< a, b >,$

где

$a = (0,1,2,...,21,22),$
$b = (2,16,9,6,8)(3,12,13,18,4)(7,17,10,11,22) \cdot$
$\cdot (14,19,21,20,15).$

$M_{24} =< M_{23}, c >,$

где

$c = (0,23)(1,22)(2,11)(3,15)(4,17)(5,9)(6,19)(7,13)(8,20) \cdot$
$\cdot (10,16)(12,21)(14,18),$

причем стабилизатор точки 23 в M_{24} совпадает с M_{23}.

Для получения других примеров $(t,1)$-транзитивных множеств подстановок нужно отказаться от групповой струк-

туры множества E. Конструкция таких множеств, называемых *точно t-транзитивными множествами подстановок*, рассматривалась, например, в [Nom85], [Bie96]. В [Nom85] приводятся примеры $(t,1)$-транзитивных множеств, не являющихся смежными классами по подгруппе группы S_λ.

Теперь несколько слов об $O(L)$-стойких шифрах, для которых

$$\pi = \frac{\mu}{\lambda} \cdot \frac{\lambda!}{(\lambda - L)!} \text{ и } \mu \geq \lambda.$$

Рассмотрения в случае $L = 1$ совпадают с проведенными ранее рассуждениями для $U(L)$-стойких шифров. При $L > 1$, $\mu = \lambda \cdot t$ для $t \in \mathbf{Z}$, согласно пункту (i) теоремы 7.3. Кроме того,

$$Y = \bigcup_{i=1}^{t} Y_i, \ |Y_i| = \lambda,$$

— разбиение множества Y, такое что $e(X) = Y_i$ для любого $e \in E$ и $i \in \overline{1,t}$.

Если $E_i = \{e \in E : e(X) = Y_i\}$, то

$$E = \bigcup_{i=1}^{t} E_i$$

— разбиение множества E. Согласно (ii) теоремы 7.3, из равенства $e_1(X) = e_2(X)$ следует, что $p(e_1) = p(e_2)$. Тогда каждая тройка $(\widetilde{X}, \widetilde{Y}_i, \widetilde{E}_i)$ образует $O(L)$-стойкий шифр. Поэтому изучение $O(L)$-стойких шифров с параметрами

$$\pi = \frac{\mu}{\lambda} \cdot \frac{\lambda!}{(\lambda - L)!} \text{ и } \mu \geq \lambda$$

сводится к уже рассмотренному случаю $\mu = \lambda$.

Для $O(L)$-стойких шифров справедлив аналог теоремы 4.3.16 ([Cas98]).

Теорема 7.7. *Пусть* $\sum_{\text{В}}$ — $O(L)$*-стойкий шифр и шифр* $\sum'_{\text{В}}$ *отличается от* $\sum_{\text{В}}$ *лишь распределением вероятностей на множестве открытых текстов. Тогда шифр* $\sum'_{\text{В}}$ *также* $O(L)$*-стоек и имеет равные с* $\sum_{\text{В}}$ *значения вероятностей* p_i, $i = \overline{0, L-1}$.

В [Cas98] предложены конструкции на основе ортогональных массивов $O(L)$-стойких шифров, обладающих наименьшими значениями вероятностей p_i, $i = \overline{0, L}$, и минимальным (в некотором смысле) числом ключей.

В [Mit96] получена нижняя оценка ключей $M(L)$-стойкого шифра.

Теорема 7.8. *Число ключей* π $M(L)$*-стойкого шифра удовлетворяет неравенству*

$$\pi \geq \prod_{i=0}^{L-1} (\lambda - i).$$

Дополнение

Шифртекст несет не только информацию об открытом тексте, но и об использованном ключе. Поэтому целью криптоаналитика может быть получение информации о ключе. Лучшими для защиты от криптоатаки на основе одной криптограммы являются условия, при которых

$$p(k/y) = p(k) \tag{1}$$

для любых $k \in K$, $y \in Y$.

Назовем шифр $\sum_{\text{B}}$, удовлетворяющий условиям (1), *совершенным по ключу*. В связи с этим совершенный шифр будем называть *совершенным по открытому тексту*.

Поскольку условное вероятностное распределение $P(Y/K)$ определяется формулой

$$p(y/k) = \begin{cases} p(x), \text{если } \exists x \in X : e_k(x) = y, \\ 0, \quad \text{в противном случае,} \end{cases}$$

то (1) равносильно равенству

$$p(d_k(y)) = p(y) \tag{2}$$

для любых $k \in K$, $y \in Y$.

Выражая вероятность $p(y)$ по формуле (2.2.7), получаем критерий совершенности шифра в форме равенства

$$\sum_{k' \in K(y)} p(k') \cdot p(d_{k'}(y)) = p(d_k(y)) \tag{3}$$

для любых $k \in K$, $y \in Y$.

Теорема 1. *Если транзитивный шифр* $\sum_{\text{В}}$ *является совершенным по ключу, то* $|Y| = |X|$ *и* $P(X)$, $P(Y)$ — *равномерные распределения.*

Доказательство. Пусть $y \in Y$ и $K(Y) = \{k_1, ..., k_N\}$. Тогда из (3) следует цепочка равенств

$$\begin{aligned} & p(d_{k_1}(y)) = ... = p(d_{k_N}(y)) = \\ & = p(k_1)p(d_{k_1}(y)) + ... + p(k_N)p(d_{k_N}(y)). \end{aligned} \tag{4}$$

Пусть $p = p(d_{k_i}(y))$, $i = \overline{1, N}$. Тогда

$$p = p\left(\sum_{k \in K(y)} p(k)\right) \Leftrightarrow \sum_{k \in K(y)} p(k) = 1 \Leftrightarrow K(y) = K.$$

Равенство $K(y) = K$ означает, что y содержится в каждой строке матрицы зашифрования. Поскольку это верно для любого $y \in Y$, то $|Y| \le |X|$, так как длина строки матрицы зашифрования равна $|X|$. С другой стороны, для любого шифра $|Y| \ge |X|$, следовательно, $|Y| = |X|$.

Условие транзитивности шифра означает, что в (4)

$$\{d_{k_1}(y), ..., d_{k_N}(y)\} = X,$$

откуда следует равномерность распределения $P(X)$.

Равномерность распределения $P(Y)$ следует из того, что для любого $y \in Y$

$$p(y) = \sum_{k \in K(y)} p(k) \cdot p(d_k(y)) = \frac{1}{|X|} \sum_{k \in K} p(K) = \frac{1}{|X|}.$$

Совершенный по ключу шифр может не быть транзитивным и может иметь не равномерное распределение $P(X)$.

Пример. Рассмотрим шифр $\sum_{\text{B}}$, для которого $X = Y = \{1,2,3,4\}$, а матрица зашифрования имеет вид

	1	2	3	4
k_1	1	2	3	4
k_2	2	1	3	4
k_3	1	2	4	3

Пусть $p(x_1) = p(x_2) = 1/8$, $p(x_3) = p(x_4) = 3/8$, а распределение $P(K)$ — произвольно. Непосредственно проверяется, что этот шифр не является транзитивным, но является совершенным по ключу.

Представляют интерес шифры, обеспечивающие совершенную стойкость по открытому тексту и по ключу.

Теорема 2. *Если шифр* $\sum_{\text{B}}$ *является совершенным по открытому тексту и по ключу, то* $|Y| = |X|$ *и* $P(X)$, $P(Y)$ *— равномерные распределения. Если при этом* $|K| = |X|$, *то и распределение* $P(K)$ *— равномерное.*

Доказательство. Первое утверждение следует из теоремы 1. Пользуясь критерием совершенности шифра по открытому тексту, имеем:

$$p(y/x) = p(y) \Leftrightarrow \sum_{k \in K(x,y)} p(k) = 1/|X|.$$

Согласно теореме Шеннона, из условия следует равенство $|K(x,y)|=1$ для любых $x\in X$, $y\in Y$. Отсюда следует равномерность распределения $P(K)$, что и требуется.

Справедливо частичное обращение теоремы 2.

Теорема 3. *Пусть* $\Sigma_{\text{В}}$ — *транзитивный шифр, удовлетворяющий условиям* $|X|=|Y|=|K|$, *и имеющий равномерные распределения* $P(X)$, $P(K)$. *Тогда* $\Sigma_{\text{В}}$ *является совершенным по открытому тексту и по ключу.*

Отметим, что свойства шифра быть совершенным по открытому тексту и по ключу являются независимыми. В самом деле, как мы знаем, свойство совершенности шифра по открытому тексту не зависит от распределения $P(X)$, в то время как совершенным по ключу шифр может быть лишь в случае, когда $P(X)$ — равномерное распределение. Приведенный выше пример показывает, что совершенный по ключу шифр может быть не транзитивным, и, следовательно, не совершенным по открытому тексту.

В более общей форме можно ставить задачу о нахождении ключа на основе ряда криптограмм, полученных на одном ключе.

Литература

[Алф01] *Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В.* Основы криптографии. — М.: "Гелиос АРВ", 2001.

[Анд99] *Андреев Н.Н., Петерсон А.П., Прянишников К.В., Старовойтов А.В.* Основоположник отечественной засекреченной телефонной связи. — Радиотехника (1998) № 8, 8 — 12.

[Баб02] *Бабаш А.В., Шанкин Г.П.* Криптография (аспекты защиты). — М.: СОЛОН-Р, 2002.

[Бра99] *Брассар Ж.* Современная криптология. — М.: ПОЛИМЕД, 1999.

[Глу90] *Глухов М.М., Елизаров В.П., Нечаев А.А.* Алгебра (учебник). — М.: в/ч 33965, 1990.

[Гор86] *Горбатов В.А.* Основы дискретной математики. — М.: Высшая школа, 1986.

[Коф75] *Кофман А.* Введение в прикладную комбинаторику. — М.: Наука, 1975.

[Мэс88] *Мэсси Жд.Л.* Введение в современную криптологию. — ТИИЭР, т. 76, № 5 (1988), 24 — 42.

[Неч99] *Нечаев В. И.* Элементы криптографии. Основы теории защиты информации. — М.: Высшая школа, 1999.

[Рио63] *Риордан Дж.* Введение в комбинаторный анализ. — М.: ИЛ, 1963.

[Сач77] *Сачков В.Н.* Комбинаторные методы дискретной математики. — М.: Наука, 1977.

[Хол62] *Холл М.* Теория групп. — М.: ИЛ, 1962.

[Хол70] *Холл М.* Комбинаторика. — М.: Мир, 1970.

[Шен63] *Шеннон К.* Теория связи в секретных системах // В кн.: Работы по теории информации и кибернетике. — М.: ИЛ, 1963.

[Bie95] *Bierbrauer J.* Monotypical uniformly homogeneous sets of permutations. — Arch. Math. (1992)

V.58, 338 — 344.

[Bie94] *Bierbrauer J., Edel Y.* Theory of perpendicular arrays. — Journal of combinatorial designs (1994) V.6, 375 — 406.

[Bie95] *Bierbrauer J.* The uniformly 3-homogeneous subsets of $PGL_2(q)$. — Journal of algebraic combinatorics (1995) V.4, 99 — 102.

[Bie96] *Bierbrauer J., Black S., Edel Y.* Some t-homogeneous sets of permutations. — Designs, codes and cryptography (1996) V.9, №1, 25 — 38.

[Cas98] *Casse L.R.A., Martin K.M., Wild P.R.*. Bounds and characterizations of authentication/secrecy schemes. — Designs, codes and cryptography (1998) V.13, № 2, 107 — 129.

[God90] *Godlewsky P., Mitchell C.* Key-minimal cryptosystems for unconditional secrecy. — Journal of Cryptology (1990) № 1, 1 — 25.

[Mas87] *Massey J., Maurer U., Wang M.* Non-expanding, key-minimal, robustly-perfect, linear and bilinear ciphers. — Procceedings of Crypto'87; Advances in Cryptology (1987), 237 — 247.

[Mit94] *Mitchell C.J., Walker M., Wild P.* The combinatorics of perfect authentication schemes. — SIAM Journal 102 — 107.

[Mit96] *Mitchell C.J., Piper F.C., Walker M., Wild P.* Authentication schemes, perfect local randomizers, perfect secrecy and perfect sharing schemes. — Designs, codes and cryptography (1996) V.7, №1/2, 101 — 110.

[Nom85] *Nomura K.* On t-homogeneous permutation sets. — Archiv der mathematik, 44 (1985), 485 — 487.

[Ree96] *Rees R.S., Stinson D.R.*. Combinatorial characterizations of authentication codes II. — Designs, codes and cryptography (1996) V.7, № 3, 239 — 259.

[Ros93] *Rosenbaum U.* A lower bound on authentication after having observed a sequence of messagas. — Journal of Cryptology (1993) V.6, 135 — 156.

[Rub96] *Rubin F.* One-time pad cryptography. — Cryptologia, (1996) VXX, № 4, 359 — 364.

[Sim84] *Simmons G.J.* Authentication theory / coding theory // Procceedings of Crypto'84; Advances in Cryptology (1984), 411 — 431.

[Soe88] *De Soete M.* Some constructions for authentication-secrecy codes. — Procceedings of EuroCrypt'88; Advances in Cryptology (1988), 57 — 75.

[Sti95] *Stinson D.R.* Cryptography: Theory and practice. — CRC Press, N.Y., 1995.

[Sti92] *Stinson D.R.* Combinatorial characterizations of authentication codes. — Designs, codes and cryptography, (1992) № 2, 175 — 187.

[StiTei90] *Stinson D.R., Teirlinck L.* A construction for authentication secrecy codes from 3-homogeneous permutation groups. — European journal combinatorics (1990) V.11, 73— 79.

[Sti88] *Stinson D.R.* A construction for authentication secrecy codes from certain combinatorial designs. — Procceedings of Crypto'87; Advances in Cryptology (1988), 355 — 366.

[Sti90] *Stinson D.R.* The combinatorics of authentication and secrecy codes. — Journal of Cryptology (1990) № 2, 23 — 49.

[Tra95] *Tran van Trun.* On the constraction of authentication and secrecy codes. — Designs, codes and cryptography (1995) V.5, № 3, 269 — 280.

Оглавление

Совершенные шифры

Изложены свойства и конструкции безусловно стойких шифров, названных К. Шенноном совершенными по отношению к различным криптоатакам. Выделяются совершенные шифры с минимально возможным числом ключей, а также стойкие к попыткам обмана со стороны злоумышленника.

гелиос арв