Федеральное агентство по образованию

Ставропольский Государственный университет

Реферат

На тему:

«Исторические основы криптологии»

Выполнил:

Студент 4-го курса

Специальности «Математика»

Шевченко Виктор.

Ставрополь 2006.

**Содержание.**

1. Введение …………………………………………………………………………3
2. Предмет криптологии …………………………………………………………...7
3. Язык сообщения …………………………………………………………………8
4. Тайнопись ……………………………………………………………………….10
5. Коды и их назначение …………………………………………………………..14
6. Криптография и криптоанализ………………………………………………….19
7. История криптографии…………………………………………………………..22
8. Заключение……………………………………………………………………….48
9. Примечания ……………………………………………………………………...50
10. Список литературы……………………………………………………………...57

**Введение.**

«Сограждане!» — начал он взволнованным

голосом, но так как речь его была секретная,

то весьма естественно, что никто ее не слыхал.

М. Салтыков-Щедрин,

«История одного города».

История человеческой цивилизации стала также историей создания систем безопасной передачи информации. Искусство шифрования и тайной передачи информации было присуще практически всем государствам.

Что обычно приходит на ум при произнесении слова «криптография»? Спецслужбы, дипломатическая переписка, "математическое шаманство"? А при произнесении фразы «криптография в информационных технологиях»? Шифрование данных припомнят сразу. Про электронную подпись вспомнят. Кто то знает что то про «Сертификаты открытых ключей». Или про «взлом» чужих шифров. Попробуем разобраться со всеми этими, а заодно и другими, понятиями и подходами, которыми оперирует современная криптография.   
 Криптография в прошлом использовалась лишь в военных целях. Однако сейчас, по мере образования информационного общества, криптография становится одним из основных инструментов, обеспечивающих конфиденциальность, доверие, авторизацию, электронные платежи, корпоративную безопасность и бесчисленное множество других важных вещей. Справедливости ради надо отметить, что криптография — не панацея от всех бед. Криптографические методы могут помочь обеспечить безопасность, но только на эти методы надеяться не следует. Криптографические методы могут применяться для решений следующих проблем безопасности:

- конфиденциальности передаваемых/хранимых данных

- аутентификации



- целостности хранимых и передаваемых данных

- обеспечения подлинности документов Базовых методов преобразования информации, которыми располагает криптография, немного, среди них:



- шифрование (симметричное и несимметричное)

- вычисление хэш функций



- генерация электронной цифровой подписи

- генерация последовательности псевдослучайных чисел

Проблема защиты информации путем ее преобразования, исключающего ее прочтение посторонним лицом, волновала человеческий ум с давних времен. История криптографии - ровесница истории человеческого языка. Более того, первоначально

письменность сама по себе была своеобразной криптографической системой, так как в древних обществах ею владели только избранные. Священные книги древнего Египта, древней Индии тому примеры.

Историю криптографии условно можно разделить на 4 этапа.

1. Наивная криптография.

2. Формальная криптография.

3. Научная криптография.

4. Компьютерная криптография.

Для наивной криптографии (до нач. XVI века) характерно использование любых (обычно примитивных) способов запутывания противника относительно содержания шифруемых текстов. На начальном этапе для защиты информации использовались методы кодирования и стеганографии, которые родственны, но не тождественны криптографии. Большинство из используемых шифров сводились к перестановке или моноалфавитной подстановке. Одним из первых зафиксированных примеров является шифр Цезаря, состоящий в замене каждой буквы исходного текста на другую, отстоящую от нее в алфавите на определенное число позиций. Другой шифр, полибианский квадрат, авторство которого приписывается греческому писателю Полибию, является общей моноалфавитной подстановкой, которая проводится с помощью случайно заполненной алфавитом квадратной таблицей (для греческого алфавита размер составляет 5x5). Каждая буква исходного текста заменяется на букву, стоящую в квадрате снизу от нее. Этап формальной криптографии (кон. XV века - нач. XX века) связан с появлением формализованных и относительно стойких к ручному криптоанализу шифров. В европейских странах это произошло в эпоху Возрождения, когда развитие науки и торговли вызвало спрос на надежные способы защиты информации. Важная роль на этом этапе принадлежит Леону Батисте Альберти, итальянскому архитектору, который одним из первых предложил многоалфавитную подстановку. Данный шифр, получивший имя дипломата XVI века Блеза Вижинера, состоял в последовательном «сложении» букв исходного текста с ключом (процедуру можно облегчить с помощью специальной таблицы). Его работа «Трактат о шифре» A466) считается пер- первой научной работой по криптологии. Одной из первых печатных работ, в которой обобщены и сформулированы известные на тот момент алгоритмы шифрования является труд «Полиграфия» A508 г.) немецкого аббата Иоганна Трисемуса. Ему принадлежат два небольших, но важных открытия: способ заполнения полибианского квадрата (первые позиции заполняются с помощью легко запоминаемого ключевого слова, остальные - оставшимися буквами алфавита) и шифрование пар букв (биграмм). Простым но стойким способом многоалфавитной замены (подстановки биграмм) является шифр Плейфера, который был открыт в начале XIX века Чарльзом Уитстоном. Уитстону принадлежит и важное усовершенствование - шифрование ««двойным квадратом». Шифры Плейфера и Уитстона использовались вплоть до первой мировой войны, так как с трудом поддавались ручному криптоанализу. В XIX веке голландец Керкхофф сформулировал главное требование к криптографическим системам, которое остается актуальным и поныне: секретность шифров должна быть основана на секретности ключа, но не алгоритма. Наконец, последним словом в донаучной криптографии, которое обеспечили еще более высокую криптостойкосить, а также позволило автоматизировать (в смысле механизировать) процесс шифрования стали роторные криптосистемы. Одной из первых подобных систем стала изобретенная в 1790 году Томасом Джефферсоном, будущим президентом США механическая машина. Многоалфавитная подстановка с помощью роторной машины реализуется вариацией взаимного положения вращающихся роторов, каждый из которых осуществляет «прошитую» в нем подстановку. Практическое распространение роторные машины получили только в начале XX века. Одной из первых практически используемых машин, стала немецкая Enigma, разработанная в 1917 году Эдвардом Хеберном и усовершенствованная Артуром Кирхом. Роторные машины активно использовались во время второй мировой войны. Помимо немецкой машины Enigma использовались также устройства Sigaba (США), Турех (Великобритания), Red, Orange и Purple2 (Япония). Роторные системы - вершина формальной криптографии так как относительно просто реализовывали очень стойкие шифры. Успешные криптоатаки на роторные системы стали возможны только с появлением ЭВМ в начале 40-х годов. Главная отличительная черта научной криптографии 30-е - 60-е годы XX века) - появление криптосистем со строгим математическим обоснованием криптостойкости. К началу 30-х годов окончательно сформировались разделы математики, являющиеся научной основой криптологии: теория вероятностей и математическая статистика, общая алгебра, теория чисел, начали активно развиваться теория алгоритмов, теория информации, кибернетика. Своеобразным водоразделом стала работа Клода Шеннона «Теория связи в секретных системах» ), где сформулированы теоретические принципы криптографической защиты информации. Шеннон ввел понятия «рассеивание» и «перемешивание», обосновал возможность создания сколь угодно стойких криптосистем. В 60-х годах ведущие криптографические школы подошли к созданию блочных шифров, еще более стойких по сравнению с роторными криптосистемами, однако допускающие практическую реализацию только в виде цифровых электронных устройств. Компьютерная криптография (с 70-х годов XX века) обязана своим появлением вычислительным средствам с производительностью, достаточной для реализации критосистем, обеспечивающих при большой скорости шифрования на несколько Примерно в 1900 году до н. э. древние египтяне начали видоизменять и искажать иероглифы, чтобы закодировать определенные сообщения. порядков более высокую криптостойкость, чем «ручные» и «механические» шифры. Первым классом криптосистем, практическое применение которых стало возможно с появлением мощных и компактных вычислительных средств, стали блочные шифры. В 70-е годы был разработан американский стандарт шифрования DES (принят в 1978 году). Один из его авторов, Хорст Фейстел (сотрудник IBM), описал модель блочных шифров, на основе которой были построены другие, более стойкие симметричные криптосистемы, в том числе отечественный стандарт шифрования ГОСТ 28147-89. С появлением DES обогатился и криптоанализ, для атак на американский алгоритм был создано несколько новых видов криптоанализа (линейный, дифференциальный и т.д.), практическая реализация которых опять же была возможна только с появлением мощных вычислительных систем. В середине 70-х годов произошел настоящий прорыв в современной криптографии - появление асимметричных криптосистем, которые не требовали передачи секретного ключа между сторонами. Здесь отправной точкой принято считать работу, опубликованную Уитфилдом Диффи и Мартином Хеллманом в 1976 году под названием «Новые направления в современной криптографии». В ней впервые сформулированы принципы обмена шифрованной информацией без обмена секретным ключом. Независимо к идее асимметричных криптосистем подошел Ральф Меркли. Несколькими годами позже Рон Ривест, Ади Шамир и Леонард Адлеман открыли систему RSA, первую практическую асимметричную криптосистему, стойкость которой была основана на проблеме факторизации больших простых чисел. Асимметричная криптография открыла сразу несколько новых прикладных направлений, в частности системы электронной цифровой подписи (ЭЦП) и электронных денег. В 80-90-е годы появились совершенно новые направления криптографии: вероятностное шифрование, квантовая криптография и другие. Осознание их практической ценности еще впереди. Актуальной остается и задача совершенствования симметричных криптосистем. В 80-90-х годах были разработаны нефейстеловские шифры (SAFER, RC6 и др.), а в 2000 году после открытого международного конкурса был принят новый национальный стандарт шифрования США - AES.



В 600 - 500 годы до н. э. древние евреи создали упорядоченную систему криптографии "Атбаш" - в России известна под названием "тарабарская грамота". Суть метода проста: при письме одна буква алфавита заменяется другой, например, вместо буквы "а" всегда пишется буква "я".

Основные принципы разведки и контрразведки, включая и методы обработки информации, впервые сформулировал китайский ученый Сун Цзы в своей книге "Искусство войны" примерно в 500 году до н. э. Малоизвестно, что в известной древнеиндийской книге "Кама Сутра" криптография упоминается как одно из 64 искусств, обязательных к изучению.

Абу Яхмади, составитель первого словаря арабского языка в VIII веке научился взламывать византийские секретные депеши, написанные на основе греческого языка.

В XV веке итальянский математик Леон Батиста Альберти создал первую математическую модель криптографии. Он также создал первое механическое устройство для шифрования секретных документов. На основе его изобретения действовали все криптографические устройства, использовавшиеся до появление компьютеров. В частности, в 17 веке известный английский ученый сэр Фрэнсис Бэкон создал подобное устройство, где каждой букве алфавита могло соответствовать пять вариантов шифровки.

В XVII столетии криптографией увлекся Томас Джефферсон, один из отцов-основателей США, третий по счету президент страны и ученый. Он создал шифровальную машину цилиндрической формы, позволявшую использовать десятки вариантов кодирования. Подобные устройства использовались во всем мире вплоть до конца Второй мировой войны.

В XVIII веке английская разведка стала широко применять невидимые чернила - в частности молоко. Метод письма молоком (текст становится виден при нагревании листа бумаги) позже использовал Владимир Ленин.

**Предмет Криптологии.**

Описание предмета криптологии начнем с доуточнения обиходного понятия информация. Иностранному термину информация достаточно близко отвечает русское слово смысл. Очевидно, что одну и ту же информацию можно передать разными сообщениями, например, на разных языках, а также письмом, телеграфом или факсом.

С другой стороны, одно и то же сообщение разными людьми понимается по-разному. Например, при сообщении о победе «Спартака» иной футбольный болельщик обрадуется, а другой может и огорчиться. Значит, можно сделать вывод, что информация людьми извлекается из сообщения с помощью ключа, правила, придающего сообщению конкретный смысл. Для обычных сообщений такие правила дают здравый смысл и знание языка. Иногда же, ключом владеет лишь узкая группа лиц, знающая специальные термины или жаргон. Например, на блатном языке начала века сизюмаp пено означало число 75. Жаргон преферансистов хорошо иллюстрирует анекдот. Кассир спрашивает у мужчины, снимающего крупную сумму денег со счета: «Гарнитурчик собираетесь прикупить?», тот со вздохом отвечает: «Прикупил вчера, на мизере». У программистов на персональных компьютерах можно услышать массу специфических терминов: старая мама, кривой винт, косые флопы, полуось, огрызок. О’Генри в «Королях и капусте» привел пример, как написанная на Нью-Йоркском жаргоне телеграмма: «...главный с кисейным товаром держит курс на соль...» — была не понята туземными чиновниками, сколько ни ломали себе они над ней голову. Но ее смысл, что президент Анчурии бежал с любовницей к океану, сразу же разгадал американец Билли Кьоу, который «...как то ухитрился понять даже приказ улетучиться, произнесенный на классическом китайском языке и подтвержденный дулом мушкета...»

Особую роль ключ имеет в криптографии, где его знание гарантирует извлечение

истинного смысла сообщения. Вспомните смешные фигурки из рассказа «Пляшущие человечки» Конан Дойля. Их рисунок казался детской шалостью, но привел в ужас героиню, которая, зная ключ, прочла адресованную ей шифровку: «Илей, готовься к смерти».

**Язык сообщения.**

Исходное незнание языка сообщения обычно делает невозможным восприятие его смысла. Мужчина, привыкший к скромной символике на отечественных сигаретах, так и не смог правильно прочесть название их нового сорта: «ПОКТОБ». На пачке под красивым княжеским гербом была не английская, а русская надпись РОСТОВ.

Мало кто сможет понять запись «мана дерутумо», сделанную по-нганасански, ведь знающих этот язык во всем мире вряд ли больше тысячи. И уж совсем невероятной кажется возможность прочтения надписи на забытом языке. В Большом энциклопедическом словаре написано: «Расшифровка Ф. Шампольоном иероглифического текста Розеттского камня положила начало чтению древнеегипетских иероглифов». В этом высказывании все верно. Однако можно ли расшифровать письмена, которые не были зашифрованы? Паскаль в своих «Мыслях» высказался: «Языки суть шифры, в которых не буквы заменены буквами, а слова словами, так что неизвестный язык есть легко разгадываемый шифр». Но криптологи и языковеды не поддерживают это мнение. Поэтому далее употребление слова расшифровка будет относиться лишь к прочтению сообщений на известных языках, сделанных с помощью шифра, то есть системы изменения текста письма, чтобы сделать смысл его непонятным для непосвященных, не знающих ключа.

Стоит сделать небольшое, но важное замечание. Иногда необходимо русский текст напечатать на пишущей машинке с латинским алфавитом. Для этого можно воспользоваться соответствием русских букв латинским принятым для написания международных телеграмм. Например, SHESTOE POCHTOVOE OTDELENIE GORODA

IAROSLAVLIA.

Заметим, буква Э передается так же как и буква Е, тем не менее написанный так текст останется русским, просто изменится его кодировка. Язык существенно влияет на структуру текста и его понимание. Однако, даже определившись с языком сообщения, бывает подчас трудно решить сколько букв будет составлять алфавит: латинский насчитывает 24-25 букв, а русский 31-32. Неоднозначность возникает потому, что при письме часть букв заменяют другими, сходными по звучания или написанию. Обычно русскую букву Ё в письме заменяют на букву Е, а букву Й на И. Каждый язык имеет свой специфический алфавит, но, увы не единственный. Так, хотя болгарский и русский алфавиты, происшедшие от кириллицы, почти одинаковы, но в болгарском нет букв Ё, Ы, Э. Поэтому, набирая попеременно то русский, то болгарский тексты, обычно держатся лишь русского алфавита, включающего в себя болгарский.

Сложнее всего дело с алфавитом обстоит в Европе на территории эксреспублики Югославии, где для сербохорватского языка давно используются сразу две основные системы письменности. Одна из них, вуковица, названная по имени Вуко Кароджича, является подвидом кириллицы и употребляется главным образом сербами, другая же, гаевица, представляет подвид латиницы и используется хорватами. Соответствие между буквами вуковицы и гаевицы неоднозначно, поскольку сербской букве, обозначающей звук «дь», отвечают две, или даже три хорватские. Но это еще не все. Есть, как минимум, два варианта сербохорватского произношения: екавский и экавский, которые различно отображаются на письме. Из этого примера хорошо видно, что справиться с неопределенностью языка сообщения без его знания вовсе непросто. По этому поводу Герман Вейль удачно привел двустишие Готфрида Келлера: «Что это значит — каждый знает, кто во сне верхом скакал без коня». По этой причине язык сообщений криптологи считают заранее известным и алфавит его фиксированным. Интересно заметить, во время Второй мировой войны сделать свои шифровки нечитаемыми для японцев американцы смогли довольно простым путем: они набирали криптографов из небольшого индейского племени Навахо и те вели секретную связь только на своем родном языке.

**Тайнопись.**

Начиная с давних времен, люди обменивались информацией, посылая друг другу

письма. Древним новгородцам приходилось сворачивать свои берестяные грамотки

текстом наружу — только так они могли перевозиться и храниться, не разворачиваясь самопроизвольно от изменения влажности. Это походило на современные почтовые карточки, где текст тоже открыт для посторонних взоров. Пересылка берестяных

грамот была широко распространена, но имела серьезный изъян, содержимое посланий не было защищено ни от своекорыстных интересов, ни от неуемного любопытства иных людей. Поэтому со временем послания стали свертывать особо, так, чтобы текст оказывался внутри. Когда же и это казалось недостаточным, то письмо запечатывали восковой, а в позднейшее время сургучной личной печатью. Печати всегда были не столько в моде, сколько в повседневном обиходе. Они обычно выполнялись в виде перстней с рельефными изображениями, и Эрмитаж в античном отделе хранит их множество. Печати, придуманы по уверениям некоторых историков китайцами, хотя древние камеи Вавилона, Египта, Греции и Рима ничем от печатей не отличаются. Воск прежде, а сургуч и поныне помогают поддерживать секреты почтовой переписки.

Точных дат и бесспорных сведений о секретном письме в древности сохранилось очень мал. Однако вместе с шифрами были, само собой разумеется, и попытки сокрытия текста. В древней Греции для этого однажды обрили раба, написали на его голове, и, когда волосы отросли, отправили с поручением к адресату. Отзвук этой истории можно встретить в «Гиперболоиде инженера Гарина» Алексея Толстого, где текст нанесли на спину мальчика. Если же гонец был надежен и даже под пытками не выдал бы послания, то его изложение могло быть изустным. Боярин Иван Фрязин, в 1469 году выступая сватом Великого князя Иоанна к Софье (Софья — племянница и наследница последнего византийского императора Костантина Палеолога, принесшая России свой герб в виде двуглавого орла как приданое), имел грамоту следующего содержания: «Сиксту, Первосвятителю Римскому, Иоанн, Великий князь Белой Руси, кланяется и просит верить его послам».

Опишем кратко, но не будем дальше рассматривать сообщения симпатические, латентные или скрытые. Они могут быть сделаны специальными техническими средствами, как передача остронаправленным лучом, надпись бесцветными чернилами, проявляющаяся лишь после специального физического или химического воздействия. Именно скрытые сообщения принято называть тайнописью, но не шифры. Популярные исторические книжки сообщали, что российские революционеры в тюрьмах использовали в качестве симпатических чернил даже обычное молоко — и это правда. При нагревании на огне или горячим утюгом такие записи становились отчетливо видны. (Дейл Карнеги полагал, что для «проявления» такой тайнописи достаточно было погрузить письмо в горячий чай. Здесь он не прав.) Литератор Куканов в своей повести о Ленине «У истоков грядущего» рассуждал так: «Молоко в роли чернил — не самый хитрый способ тайнописи, но порой, чем проще уловка, тем она надежнее».

Заглянем же теперь в документ под номером 99312 из архива российской охранки: «Переписка химией состоит в следующем. Пишут на шероховатой, не глянцевой бумаге. Пишут сначала обыкновенными чернилами какой-нибудь безразличный текст, то есть что-либо совершенно безобидное, ни слова о делах. Когда это письмо написано, то берут совершенно чистое мягкое перо и пишут между строками, написанными чернилами, уже то, что хотят сказать о конспиративных делах. Это конспиративное письмо пишут химическими чернилами, то есть раствором какой-нибудь кислоты...». Была приведена выдержка из письма, сделанного химией революционерами партии РСДРП, которое было отправлено в Россию редакцией газеты «Правда» из Вены. Выявить и прочесть эту тайнопись Департаменту полиции не составляло никакого труда, ведь именно в России были разработаны и развиты способы чтения скрытых и стертых текстов с помощью фотографии и подбора освещения, применяемые и поныне. Интересно, зачем долгие годы упорно распространялась легенда о трудности прочтения «молочной» тайнописи?

Позднее, физик Роберт Вуд предложил использовать для чтения скрытых текстов явление люминесценции, потрясшее эффективностью английские секретные службы, занимавшиеся этой проблемой. Биограф Сибрук со слов Вуда описывает это так:

«Мне принесли большой гладкий чистый штамп военной цензуры. Я натер его вазелином, затем, как следует вытер платком, пока он не перестал оставлять следы на

бумаге. Затем, я плотно прижал его к шпионоупорной бумаге, не давая соскользнуть в сторону.

— Можете ли вы обнаружить здесь запись? — спросил я.

Они испытали бумагу в отраженном и поляризованном свете и сказали:

— Здесь ничего нет.

— Тогда давайте осветим ультрафиолетовыми лучами.

Мы взяли ее в кабинку и положили перед моим черным окошечком. На бумаге яркими голубыми буквами, как будто к ней приложили штамп, намазанный чернилами,

светились слова: секретных надписей нет.»

Сокрытие текста достигло своих вершин после Второй мировой войны, когда распространились сверхминиатюрные фотографии, называемые микроточками. Одна микроточка размером с обычную точку текста могла содержать сотни страниц документов и найти ее в книге среднего формата было много сложнее, чем пресловутую иголку в стоге сена. Адвокат Рудольфа Абеля, оказавшегося в американской каторжной тюрьме по обвинению в незаконном въезде в США (Обвинение Абелю (Вильям Фишер) в шпионаже не предъявили потому, что за шпионаж в США неизбежна смертная казнь, а его попытались обменять на американского шпиона, схваченного впоследствии в СССР. В 1962 году Абель, отсидев в каторжной тюрьме 5 лет из 30, был обменян на пилота Pшпиона Пауэрса, сбитого в советском воздушном пространстве.), хотел продать его конфискованные картины с аукциона, чтобы улучшить положение своего подзащитного хотя бы материально. Однако этого не удалось сделать, так как картины, написанные маслом с применением непрозрачных для рентгеновских лучей красок, при поиске микроточек непременно были бы разрушены, а сам поиск занял бы годы кропотливой работы ЦРУ. Поэтому в тюрьме Абелю пришлось подрабатывать, рисуя лишь прозрачные акварели. Сейчас нет технических проблем записать текст так мелко, что его вообще нельзя будет прочесть оптическими средствами, а придется рассматривать в электронный микроскоп. Такая технология используется при создании компьютерных микросхем сверхбольшой интеграции. На одном квадратном миллиметре их поверхности можно записать все книги, которые когда-либо были напечатаны человечеством.

Чтобы не сложилось впечатление, что симпатические сообщения бывают лишь у революционеров и шпионов, напомним ряд примеров из области компьютерных скрытых текстов. Наиболее ранняя идея их создания относится к предложению форматировать диск под размер секторов отличный от принятого DOS. Когда же все убедились, что такого рода сокрытие действует на хакеров как красная тряпка на быка, появились более глубокие приемы, где форматирование осуществляла специальная программа, напрямую обращающаяся к накопителю на гибких дисках. В ответ немедленно были созданы программы, которые могли читать любое форматирование. Для сокрытия информации на дискетах широко используются их инженерные дорожки, доступные для чтения, но не воспринимаемые дисковыми операционными системами, а также так называемые короткие зоны и неустойчивые биты (Weak bits — слабые, неустойчивые биты, которые специально записаны на уровне, промежуточном между 0 и 1). Вспомните сообщения о вирусах, которые прячутся в сбойных блоках — это тоже тайнопись своего рода. Кроме того, программой редакции диска можно очень просто дописать информацию в свободной части хвостового кластера файла. Только стоит ли? Уж слишком просто вскрывать. Симпатические сообщения имеют тот недостаток, что их скрытность обусловлена лишь состоянием развития техники, которая стремительно совершенствуется. Прибегая к симпатическим сообщениям, невольно приходится вступать в бесконечное состязание меча и щита, которому нет конца — на каждый щит найдется и поражающий его меч. Любой способ создания симпатического текста будет вскоре разрушен, и к этому нужно быть готовым. А что это за секретность без гарантий стойкости?

Стоит несколько слов сказать и о квантовой криптографии, которая недавно еще представлялась как фантастика, поскольку требуемая для ее реализации технология казалась фантастической. Но когда Беннет и Брэссард в 1982 году пришли к выводу: роль фотона состоит не в хранении, а передаче информации, и можно разработать квантовый канал открытого распределения секретных ключей. В криптографии считается, что линии связи всегда контролируются перехватчиком, которому , известно содержание всех передаваемых сообщений, о чем могут и не знать абоненты. Но, если информация кодируется неортогональными состояниями фотона, то нарушитель не может получить сведений даже о наличии передачи без нарушения целостности ее процесса, что будет сразу же обнаружено. Перехватив фотон, злоумышленник не сможет сделать над ним несколько измерений, так как от первого же фотон разрушится и не даст ключевой информации в необходимом объеме. Поэтому даже активный перехватчик не сможет правильно передать аналогичный фотон получателю так, чтобы перехват не был бы замечен.

Дискуссия о тайнописи в неожиданном аспекте прозвучала, когда правительство США попыталось недавно ограничить или вообще запретить свободное применение криптографии. Однако, возражали оппоненты, полный ее запрет не повлечет за собой прекращение секретной связи. Во многих каналах коммерческой связи поток помех значительно превышает долю шифруемой секретной информации. Поэтому шифрованные секретные биты станут прятать в обычных сообщениях, имитируя небольшое увеличение шума. Приводился пример: в одном цифровом снимке Kodak Photo содержится около 18 мегабайт информации, и умело произведенное сокрытие в нем мегабайта шифровки практически не ухудшит качества изображения. Прятать шифровки очень просто потому, что они ничем не отличимы от обычного шума или

помех в каналах связи. Если обычная тайнопись легко читается, то тайнопись шифрованного сообщения, замаскированного под шум или сбои, найти невозможно. Интересный вариант тайнописной шифровки был использован при печати на ЭВМ контрактов с клиентами в одной из московских компаний. За счет малозаметных искажений очертаний отдельных символов текста в него вносилась шифрованная информация об условиях составления контракта. Эта тайнопись выглядела как обычные незначительные дефекты печати и обеспечивала очень высокую степень защиты подлинности документа. В связи с указом Ельцина об аттестации шифрованной связи, пытающимся фактически предельно ограничить ее применение, можно предположить, что ФАПСИ теперь придется не только взламывать шифры, но и отыскивать их во тьме помех дрянных каналов связи, предоставляемых коммерсантам.

**Коды и их назначение.**

К шифрам не относятся и коды — системы условных обозначений или названий, применяемых при передаче информации в дипломатии, коммерции и военном деле. Кодирование часто применяется для повышения качества передачи. Хорошо известны и широко используются коды, исправляющие ошибки при передаче сообщений по каналам связи или хранении данных в памяти ЭВМ. Так, код Хемминга хорошо себя зарекомендовал себя в аппаратуре оперативной памяти ЭВМ СМP4. Другой многочисленный класс кодов представлен средствами сжатия данных, наподобие программ архивации ARC, ARJ, ICE, ZIP и сжатия дисков на IBM PC. Употребление этих кодов вызвано не секретностью, а стремлением сэкономить на стоимости передачи или хранения сообщения. Файлы текстов, изображений и программ содержат информацию с сильно отличающимися свойствами и программы их кодирования должны быть разными. Если архиватор хорошо сжимает текст, вовсе не значит, что он так же хорош для сжатия изображений или других данных.

Для текстовых файлов чаще других употребляется кодировка Хаффмена, заключающаяся в том, что символы текста заменяются цепочками бит разной длины. Чем чаще символ, тем короче обозначающая его цепочка. Рассмотрим пример кодирования Хаффмена текста МАМА МЫЛА РАМЫ с приведенной ниже таблицей кодирования.



Получим сообщение: 0100010010001101111001001100001101.

Легко теперь подсчитать, что поскольку исходный текст состоит из 14 символов, то при кодировке ASCII он занимает 112 бит, в то время как кодированный по Хаффмену лишь 34 бита. При кодировании Лемпела и Зива, представляющим собой развитие метода Хаффмена, кодируются не символы, а часто встречаемые последовательности бит вроде слов и отдельных фраз. Текстовые файлы сжимаются в 2-3 раза, но очень плохо, всего лишь на 10-15% сжимаются программы. Нередко используют готовые кодовые таблицы, так как статистические свойства языка сообщения обычно хорошо известны и довольно устойчивы.

Несколько особняком стоит сжатие звуковой информации, расширяющее мультимедийные возможности аппаратуры и программ. Кодирование Лемпела и Зива сжимает объем звуковой информации всего лишь на 10%. Несомненно, что для более эффективного ее уплотнения нужны специальные алгоритмы, учитывающие физическую природу звука. Практически все алгоритмы кодирования звуковой информации используют два основных приема: кодирование пауз между отдельными звуками и дельта-модуляцию. При записи человеческого голоса важнее кодирование пауз, так как не только фразы, но и слова разделены достаточно длительными перерывами. Эффективность такого кодирования может быть очень высока, но платить за нее приходится потерей четкости высоких коротких звуков, например, С и Ц. Это легко наблюдать при передаче естественной речи по голосовому модему. А вот дельта-модуляция чаще применяется для качественной записи музыки и очень похожа на замену представления чисел в формате фиксированной точки на формат с плавающей запятой. Потери от нее выражаются в некоторой приглушенности звуков, но мало искажаются тона.

Однако самая большая работа по кодированию ведется над изображениями, скажем, при передаче факсов. Если бы образ стандартного машинописного листа формата А4 не был бы сжат, то его передача даже при низком разрешении заняла около часа. В самых распространенных факсах, принадлежащих группе III по классификации Международного консультативного комитета по телеграфии и телефонии, использованы фиксированные таблицы кодировки. Похожую схему кодирования дает хорошо известный формат представления графических файлов PCX. В нем очередной байт кода может означать либо счетчик повторений, если он начинается битами 11, либо байтом точек исходного изображения. Число повторений задается младшими 6 битами байта повторения, то есть имеет значение до 63. Изображение чистого листа бумаги при этом будет сжато больше чем в 30 раз. Более сложные схемы сжатия дают форматы обмена и хранения графической информации GIF и TIF. Они кодируют уже не строки точек изображения, а полоски строк и тем самым достигают большего сжатия. Следует предостеречь читателей от попыток сжатия любой информации с помощью программ, оперирующих с изображениями. Ряд алгоритмов эффективного сжатия изображений, вроде JPEG могут искажать информацию, что почти незаметно в изображениях, но фатально для программ и числовых данных. Именно за счет некоторой «чистки» исходного сообщения JPEG удается достигать сжатия в 100 раз и больше. Без сжимающего объем сообщения кодирования невозможно было создать и приобретающий все большую популярность видеотелефон. Для использования в нем МККТТ ( MKKTT — международный консультативный комитет по телеграфии и телефонии) рекомендовал стандарт Н.261 — первую систему сжатия изображения.

Порой возникают затруднения в пересылке программ, ключей, шифротекста и других бинарных файлов по системам связи, допускающим лишь текстовые сообщения, например, в почте UNIX. Для этого файлы превращают в текст формата RADIXP50. Шифровку разбивают на группы по 3 байта из которых формируют 4 группы по 6 бит. Каждую группу из 6 бит, принимающую значения от 0 до 63, превращают в печатный символ ASCII в соответствии с нижеприведенной таблицей. Это увеличивает длину бинарного сообщения лишь на треть, в то время как привычная для программистов шестнадцатеричная запись удваивает его. Так, слово МОСКВА дает код AuMY886U. Если длина сообщения не кратна 3, то при кодировании в конец его добавляют нули. Точную длину сообщения приходится приписывать в конце. Вот как выгладит открытый пароль Филиппа Циммермана, переданный по Интернет в коде RADIXP64:



——BEGIN PGP MESSAGE——\_

Version: 2.6

iQBVAgUALeF27VUFZvpNDE7hAQFBFAH/Y

OQ52xOCH5yKSG/HgSV+N52HSm21zFEw

Ocu5LDhYxmOILr7Ab/KdxVA6LMIou2wKtyo.

ZVbYWXPCvhNXGDg7 4Mw==

=wstv

——END PGP MESSAGE——\_

Расчет на недоступность для посторонних смысла кодированного сообщения может окончиться конфузом. Напомним, что в стихотворении «Моральный кодекс» Киплинга описан телеграфист, не подумавший о вседоступности кода и приревновавший в разлуке свою молодую жену. Офицеры штаба заметили кодовую сигнализацию и вот что случилось:

*Молчит придурок адъютант, молчит штабная свита,*

*В свои блокноты странный текст все пишут деловито.*

*От смеха давятся они, читая с постной миной:*

*«Не вздумай с Бэнгзом танцевать — распутней нет мужчины!»*

Первый коммерческий код для уменьшения длины и стоимости телеграмм ввел в 1845 году Френсис Смит, компаньон Морзе. В конце XIX века Клаузен первым предложил для этой цели код АВС, a Маркони несколько позже первый многоязычный код. Сейчас аналогичных кодов тьма-тьмущая и все они представляют собой замену отдельных слов или фраз группами цифр или букв. Традиционно связисты, а не только шпионы, для этого обычно используют пятизначные группы букв или цифр, так как группы проще записывать. Широко применяется по настоящее время в связи и «Международный свод сигналов», который последний раз был пересмотрен в 1969 году.

Хотя криптологи различают шифры и коды, потому что для практических работ это разные системы, но коды представляют собой шифр простой замены слов. Обычно кодовые таблицы состоят из словаря, где каждому слову присвоен кодовый эквивалент. Фактически требуются две кодовые таблицы. Для кодирования применяется таблица алфавитно упорядоченная по словам, а для декодирования алфавитно упорядочивают коды — иначе поиск в таблице становится необычайно трудоемким. Для применяющегося в коммерции телеграфного кода Маркони на английском языке начала этих таблиц выглядят так:



В этом коде использованы не все возможные группы, например, нет группы ААААА. Это сделано для удобства их чтения и повышения устойчивости от отдельных ошибок. Для достижения секретности коды приходится шифровать. Например, сначала можно закодировать сообщение кодом Маркони, а потом применить шифр.

Коды часто похожи на шифры и это обстоятельство породило массу курьезных случаев. До революции был сорван шахматный турнир по переписке Петербург-Москва, так как непонятные жандармам почтовые карточки со знаками записи ходов перехватывались до тех пор, пока не попали начальнику, наложившему резолюцию:«Шахматы-с!» Не исключено, что среди репрессированных в советское время было немало любителей игры на гитаре, пытавшихся вести запись своих произведений необычным для музыкантов цифровым методом. Любопытно, каким образом могло НКВД отреагировать на срочную телеграмму за рубеж такого содержания: SER VAL MET LYS ARG ARG PHE LEU. Удалось бы доказать подозреваемому в шпионаже, что в телеграмме дан ряд аминокислот в сердечной мышце свиньи? Да и обнаруженный при аресте в записной книжке Н. И. Вавилова текст K3C7AO+3G5 вряд ли был бы воспринят следователем за формулу строения цветка. Интересно упомянуть о телефонном коде, применяемом некоторыми зарубежными фирмами. Так, встретив, номер телефона технической службы (1)206PDIDPDEMA, не надо смущаться — это телефон корпорации Aldus в Сиэтле. Кодовая таблица соответствия букв цифрам показана ниже.



Из таблицы определяем, что номер телефона корпорации 343P3362. Хотя, увидев на рекламном щите телефон предварительных заказов ночного клуба GUEPSTSPONLY, не пытайP тесь набирать 483P787P6659, а просто переведите с английского: «только для приглашенных». Эта запись в рекламе означает, что заказы принимаются по телефону, указанному в пригласительном или членском билете.

«Женя Дмитрий Ульяна Борис Ольга РобертИгорь Света», - сообщение принятое по плохо работавшему телефону. Хотя моряки говорили бы при этом так: «Живете Добро Ухо Буки Он Рцы Иже Слово» или «Juliet Delta Uniform Bravo Oscar Romeo India Sierra». Такое кодирование называется акрокодом (Akro — по-гречески край, первые буквы слов или строк.). А телеграфное сообщение: «Железная дорога уведомлена. Буду обмер работ исполнять сам» представляет собой особый код, вводящий неосведомленного получателя в заблуждение. Если читать только первые буквы слов, то получится скрытое сообщение «ЖДУ Борис». Одна армейская газета в начале шестидесятых годов к революционному празднику опубликовала стихотворение, начинающееся словами «Хвала тебе...» и последующим официозным содержанием. И что же? Редактор был немедленно уволен, тираж газеты изъят из читалок и библиотек, а вот автора найти не удалось. Первые буквы строк стихов складывались в нелестную для главы государства Хрущева фразу. Никите Сергеевичу неповезло и с инициалами — акрокодом имени и отчества. Произнесенные по-английски его инициалы NS на слух сильно напоминают слово an ass — осел. Поэтому для именования этого политика в прессе, употреблялось лишь режущее отечественные уши фамильярное обращение — Никита Хрущев.

Несомненно, что коды могут служить и для сокрытия смысла сообщений. Вспомним, в 1936 году сообщение «Над всей Испанией ясное небо» отнюдь не предвещало безоблачной погоды, а послужило кодовым сигналом начала гражданской войны. Однако область применения кодирования для сокрытия смысла ограничена одиночными сообщениями. Румынская разведка сигуранца могла читать в двадцатые годы радиограммы РККА лишь потому, что кодовые таблицы не менялись, пока не протирались до дыр. Краткое кодированное сообщение, не имея ключа в виде кодовых таблиц, вскрыть очень трудно, а то и невозможно. Практическое использование кодов стратегической авиацией США иллюстрируют кадры кинофильма «Доктор Стренджлав», когда пилот стратегического бомбардировщика, приняв радиограмму из группы цифр, достал секретную кодовую таблицу из сейфа и нашел там содержание приказа: ядерный удар по СССР.

**Криптография и криптоанализ.**

Дипломатические, военные и промышленные секреты обычно передаются или хранятся не в исходном виде, а после шифрования. В отличие от тайнописи, которая прячет сам факт наличия сообщения, шифровки передаются открыто, а прячется только смысл. Итак, криптография обеспечивает сокрытие смысла сообщения с помощью шифрования и открытие его расшифровыванием, которые выполняются по специальным криптографическим алгоритмам с помощью ключей у отправителя и получателя. Рассмотрим классическую схему передачи секретных сообщений криптографическим преобразованием, где указаны этапы и участники этого процесса:



Из схемы можно увидеть следующие особенности и отличия от обычных коммуникационных каналов. Отправителем сообщение шифруется с помощью ключа, и полученная шифровка передается по обычному открытому каналу связи получателю, в то время как ключ отправляется ему по закрытому каналу, гарантирующему секретность. Имея ключ и шифровку, получатель выполняет расшифровывание и восстанавливает исходное сообщение. В зависимости от целей засекречивания эта схема может несколько видоизменяться. Так, в компьютерной криптографии обычен случай, когда отправитель и получатель одно и то же лицо. Например, можно зашифровать данные, закрыв их от постороннего доступа при хранении, а потом расшифровать, когда это будет необходимо. В этом случае зачастую роль закрытого канала связи играет память. Тем не менее, налицо все элементы этой схемы.

Криптографические преобразования призваны для достижения двух целей по защите информации. Во-первых, они обеспечивают недоступность ее для лиц, не имеющих ключа и, во-вторых, поддерживают с требуемой надежностью обнаружение несанкционированных искажений. По сравнению с другими методами защиты информации классическая криптография гарантирует защиту лишь при условиях, что:

• использован эффективный криптографический алгоритм;

• соблюдены секретность и целостность ключа.

Некриптографические средства не в состоянии дать такую же степень защиты информации и требуют значительно больших затрат. Например, во что обходится подтверждение подлинности документа? Охрана, сейфы, сигнализация, секретные пакеты, индивидуальные печати, фирменные бланки, водяные знаки, факсимиле и личные подписи — вот далеко не полный набор обычных средств, предназначенных для поддержания доверия к секретности информации. В то же самое время, криптографический подход намного надежнее и проще, если ключ подошел, то информации можно доверять больше, чем маме или нотариусу.

Шифрование и расшифровывание, выполняемые криптографами, а также разработка и вскрытие шифров криптоаналитиками составляют предмет науки криптологии (от греческих слов криптос — тайный и логос — мысль) . В этой науке преобразование шифровки в открытый текст (сообщение на оригинальном языке, порой называемое «клер») может быть выполнено в зависимости от того, известен ключ или нет. Условно ее можно разделить на криптографию и криптоанализ.

Криптография связана с шифрованием и расшифровыванием конфиденциальных данных в каналах коммуникаций. Она также применяется для того, чтобы исключить возможность искажения информации или подтвердить ее происхождение. Криптоанализ занимается в основном вскрытием шифровок без знания ключа и, порой, примененной системы шифрования. Эта процедура еще называется взломкой шифра. Итак, криптографы стремятся обеспечить секретность, а криптоаналитики ее сломать.

Однако терминология еще не устоялась даже зарубежом, где криптоаналитики называют себя то взломщиками кодов (breaker), то нападающими (attacker), а взломщики компьютерных систем нарекли себя воришками (sneaker). Вряд ли правильно выделять взлом шифров в отдельную дисциплину. Совершенствуя схему шифрования, неизбежно приходится рассматривать и пути ее взлома, а конструируя устройство засекречивания данных, необходимо предусмотреть в нем блок контроля качества. А ну как произошел сбой, и незащищенные данные попадут в открытую сеть коммуникаций! Поэтому часто говорят о криптографах, которые занимаются задачами шифрования, расшифровывания и анализа. Тем более, что ряд атак на шифры представляет собой обычное расшифровывание с подбором ключа путем анализа расшифрованного сообщения на близость связному тексту. Далее криптоанализ будет рассматриваться, как область криптологии, проверяющей и доказывающей устойчивость шифров как теоретически, так и практически. Возможность компьютера производить миллионы операций в секунду очень усложнила и криптографию, и криптоанализ. Поэтому в дальнейшем машинные шифры будем называть криптографическими системами. Криптографические системы становятся год от года все изощреннее и для их вскрытия требуется все более совершенная техника криптоанализа.

Изложение будет в основном ограничено рамками классической криптографии с симметричными ключами, когда ключ отправителя сообщения должен совпадать с ключом получателя. Обмен секретными ключами в ряде случаев представляет проблему. Поэтому в последние годы ведутся интенсивные исследования в направлении шифровальных систем с открытым ключом (у таких систем ключ для шифрования открытый, а для расшифрования секретный. Поэтому их еще называют двухключевыми системами или системами с несимметричными ключами). Хотя системы с открытыми ключами быстро развиваются, целый ряд преимуществ традиционных систем позволяет им надежно удерживать ведущее место. Например, ряд алгоритмов с открытыми ключами, наподобие «укладки ранца», повел себя при опробовании на сверхбыстродействующей ЭВМ Cray несолидно, расколовшись уже через час испытаний. Другие же алгоритмы принципиально ненадежны в классическом понимании с самого начала, никто всерьез не может гарантировать их стойкость при стремительно развивающихся вычислительных методах высшей арифметики и, кроме того, чрезвычайно медлительны. Тем не менее, их роль в таких областях, как пересылка ключей и цифровая подпись уникальна. Поэтому им будет уделено определенное внимание, хотя, далее с практической точки зрения будут рассматриваться в основном лишь два классических алгоритма шифрования: замены и перестановки. В шифре перестановки все буквы открытого текста остаются без изменений, но перемещаются с их нормальной позиции. Анаграмма (анаграмма — перестановка букв в слове или фразе) — это шифр перестановки. В шифре замены, наоборот, позиции букв в шифровке остаются теми же, что и у открытого текста, но символы заменяются. Комбинации этих двух типов образуют все многообразие практически используемых классических шифров.

К необходимым аксессуарам криптотрафической техники кроме алгоритмов шифрования и расшифрования принадлежат секретные ключи. Их роль такая же, как и у ключей от сейфа. А вот изготавливаются и хранятся криптографические ключи куда более тщательно, чем стальные аналоги. Заботу об их выпуске обычно берут на себя криптографические службы, лишь в этом случае гарантируя стойкость от взлома своих систем шифрования. Какие ухищрения только не предпринимаются, чтобы сделать ключи недоступными, а факт их чтения известным! Ключи хранят в криптографических блокнотах, которые всегда представляли собой крепость для посторонних. Во-первых, они открываются с предосторожностями, чтобы ключи не исчезли физически вместе с открывшим их человеком. Во-вторых, в блокноте находишь подобие отрывного календаря с прошитыми насквозь страницами, разделенными непрозрачными для любого подсматривания листами. Чтобы прочесть очередной ключ, нужно вырвать лист разделителя, а это не может впоследствии остаться незамеченным хозяином блокнота. Более того, как только страница с ключом открыта для чтения, то ее текст начинает бледнеть и через некоторое время пропадает бесследно. Но главное еще впереди — нередко в блокноты вносят не сами ключи, а их шифровки, сделанные по ключу, который шифровальщик хранит лишь в памяти. Ухищрениям в хранении ключей нет конца. У разведчика Абеля американскими спецслужбами был обнаружен криптографический блокнот размером с почтовую марку. Позднее, неподалеку от дома, где Абель жил, найдена монета, развинчивающаяся на две половинки, с тайником внутри. Очень возможно, что она служила контейнером для этого миниатюрного криптографического блокнота. Доставку ключей осуществляют специальные курьерские службы, к сотрудникам которых Петр 1 выдвинул лишь два требования: чтобы они сколь можно меньше знали вне пределов своей компетенции и были очень довольны оплатой своего труда. На этом закончим знакомство с сюжетом и персонажами дальнейшего действия и перейдем к рассмотрению истории криптографии.

**История криптографии.**

История криптографии насчитывает не одно тысячелетие. Уже в исторических документах древних цивилизаций – Индии, Египте, Китае, Месопотамии – имеются сведенья о системах и способах составления шифрованного письма. Видимо, первые системы шифрования появились одновременно с письменностью в четвёртом тысячелетии до нашей эры.

В древнеиндийских рукописях приводится более шестидесяти способов письма, среди которых есть и такие, которые можно рассматривать как криптографические. Имеется описание системы замены гласных букв согласными, и наоборот. Один из сохранившихся шифрованных текстов Месопотамии представляют собой табличку, написанную клинописью и содержащую рецепт изготовления глазури для гончарных изделий. В этом тексте использовались редко употребляемые значки, игнорировались некоторые буквы, употреблялись цифры вместо имён. В рукописях Древнего Египта шифровались религиозные тексты и медицинские рецепты. Шифрование использовалось в Библии. Некоторые фрагменты библейских текстов зашифрованы с помощью шифра, который называется атбаш. Правило зашифрования состояло в замене -й буквы алфавита (n-i+1), где n – число букв в алфавита. Происхождение слова атбаш объясняется принципом замены букв. Это слово составлено из букв Алеф, Тае, Бет и Шин, то есть первой и последней, второй и предпоследней букв древнесемитского алфавита.



Развитию криптографии способствовал переход от идеографического письма, основанного на использовании огромного числа иероглифов, к фонетическому письму. В древнем семитском алфавите во втором тысячелетии до нашей эры было уже 30 знаков. Ими обозначались согласные звуки, а также некоторые гласные и слоги. Упрощение письма стимулировало развитие криптографии.

В Древней Греции криптография уже широко использовалась в разных областях деятельности, в особенности в государственной сфере. Плутарх сообщает, что жрецы, например, хранили в форме тайнописи свои прорицания. В Спарте в 5-6 вв. до Н.Э. использовалось одно из первых шифровальных приспособлений – Сцитала. Это был жезл цилиндрической формы, на который наматывалась лента из пергамента. Кроме жезла могли использоваться рукоятки мечей, кинжалов, копий, и т.д. Вдоль оси цилиндра на пергамент построчно записывался текст, предназначенный для передачи. После записи текста лента сматывалась с жезла и передавалась адресату, который имел точно такую же Сциталу. Ясно, что такой способ шифрования осуществлял перестановку букв сообщения. Ключом шифра служит диаметр Сциталы. Известен также и метод вскрытия такого шифра, приписываемый Аристотелю. Предлагалось заточить на конус длинный брус и, обернув в него ленту, начать сдвигать её по конусу от малого диаметра до самого большого. В том месте, где диаметр конуса совпадал с диаметром Сциталы, буквы текста сочетались в слоги и слова. После этого оставалось лишь изготовить цилиндр нужного диаметра.

Другим шифровальным приспособлением времён Спарты была табличка Энея. На небольшой табличке горизонтально располагался алфавит, а по её боковым сторонам имелись выемки для наматыванья нити. При зашифровании нить закреплялась у одной из сторон таблички и наматывалась на неё. На нити делались отметки (например, узелки) в местах, которые находились напротив букв данного текста. По алфавиту можно было двигаться лишь в одну сторону, то есть делать по одной отметке на каждом витке. После зашифрования нить сматывалась и передавалась адресату. Этот шифр представлял собой шифр замены букв открытого текста знаками, которые означали расстояние между отметками нити. Ключом являлись геометрические размеры таблицы и порядок расположения букв алфавита. Это был довольно надёжный шифр: история не сохранила документов, подтверждающих сведенья о методах его вскрытия.



Греческий писатель Полибий использовал систему сигнализации, которая была широко принята как метод шифрования. Он записывал буквы алфавита в квадратную таблицу и заменял их координатами: парами чисел (i,j), где i – номер строки, j – номер столбца. Применительно к латинскому алфавиту квадрат Полибия имеет следующий вид:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | 1 | 2 | 3 | 4 | 5 |
| 1 | A | B | C | D | E |
| 2 | F | G | H | I,J | K |
| 3 | L | M | N | O | P |
| 4 | Q | R | S | T | U |
| 5 | V | W | X | Y | Z |

Пары (i,j) передавались с помощью факелов. Например, для передачи буквы О нужно было взять 3 факела в правую руку и 4 – в левую.

Подобные шифровальные приспособления, с небольшими изменениями просуществовали до эпохи военных походов Юлия Цезаря. Положение меняется в эпоху расцвета Рима, который первоначально представлял собой лишь небольшую гражданскую общину, со временем он разросся, подчинив себе Италию, а затем всё Средиземноморье. Чтобы управлять наместниками в многочисленных провинциях, шифрованная связь для римских органов власти стала жизненно необходимой. Особую роль в сохранении тайны сыграл способ шифрования, предложенный Юлием Цезарем и изложенным им в «Записках о галльской войне» (1 век до Н.Э.) Вот что пишет о нём Гай Светоний «…существуют и его письма к Цицерону и письма к близким о домашних делах: в них, если нужно было сообщить что-то негласно, он пользовался тайнописью, то есть менял буквы так, чтобы из них не складывалось ни одного слова. Чтобы разобрать и прочитать их, нужно читать всякий раз четвёртую букву вместо первой, например, D вместо А и так далее». Таким образом, Цезарь заменял буквы в соответствии с подстановкой, нижняя строка которой представляет собой алфавит открытого текста, сдвинутый циклически на 3 буквы влево.

Со времён Цезаря до 15 века шифровальное дело претерпело много изменений, однако нам мало известно о методах и системах шифрования, применяемых в этот период времени. В мрачные годы средневековья практика шифрования сохранялась в строжайшей тайне. Так, в годы крестовых походов, шифровальщики, служившие у Папы Римского, после года работы подлежали физическому уничтожению.

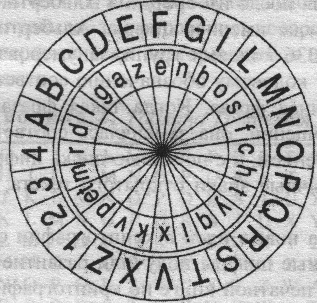
В эпоху Возрождения в итальянских городах-государствах параллельно с расцветом культуры и науки активно развивается криптография. Нередко учёные зашифровывали научные гипотезы, чтобы не прослыть еретиками и не подвергнуться преследованиям инквизиции.

Научные методы в криптографии впервые появились, по-видимому, в арабских странах. Арабского происхождения и само слово шифр. О тайнописи и её значении говорится даже в сказках «Тысячи и одной ночи». Первая книга, специально посвящённая описанию некоторых шифров, появилась в 855г., она называлась «Книга о большом стремлении человека разгадать загадки древней письменности». В 1412г. издаётся 14-томная энциклопедия, содержащая систематический обзор всех важнейших областей человеческого знания, - «Шауба аль-Аща». Её автор Шехаб аль-Кашканди. В этой энциклопедии есть раздел о криптографии, под заголовком «Относительно сокрытия в буквах тайных сообщений», в котором приводятся 7 способов шифрования. Там же даётся перечень букв в порядке частоты их употребления в арабском языке на основе изучения текста Корана, а также приводятся примеры раскрытия шифров методом частотного анализа встречаемости букв.

В 14 веке появилась книга о системах тайнописи, написанная сотрудником тайной канцелярии Папы Римского Чикко Симонетти. В этой книге приводятся шифры замены, в которых гласным буквам соответствуют несколько значковых выражений. Такие шифры позже стали называть шифрами многозначной замены или омофонами. Они получили развитие в 15 веке. Так, в книге «Трактат о шифрах» Габриеля де Лавинды – секретаря папы Климентия 12 – приводится описание шифра пропорциональной замены, в котором каждой букве ставится в соответствие несколько эквивалентов, число которых пропорционально частоте встречаемости буквы в открытом тексте. В 1469 году был предложен подобный шифр, получивший название «Миланский ключ». Появление омофонов свидетельствовало о том, что к этому времени уже хорошо осознавали слабости шифров простой замены. Такая модификация шифра разрушила статистику букв открытого сообщения, что явилось заметным шагом в развитии криптографии.

Ещё один значительный шаг вперёд криптография сделала благодаря труду Леона Альберти. Известный философ, живописец, архитектор, в 1466 году написал труд о шифрах. В этой работе был предложен шифр, основанный на использовании шифровального диска. Сам Альберти называл его шифром, «достойным королей».

Шифровальный диск представлял собой пару соосных дисков разного диаметра. Больший из них – неподвижный, его окружность разделена на 24 равных сектора, в которые вписаны 20 букв латинского алфавита в их естественном порядке и 4 цифры (от 1 до 4()4 цифрыственном порядке которые вписаны 20 букв латинского алфавитара. о диска. и. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_). При этом из 24-х буквенного алфавита были удалены 4 буквы, без которых можно обойтись, подобно тому, как в русском языке обходятся без Ъ, Ё, Й. Меньший диск – подвижный, по его окружности, разбитой также на 24 сектора, были вписаны все буквы смешанного латинского алфавита.



Диск Альберти.

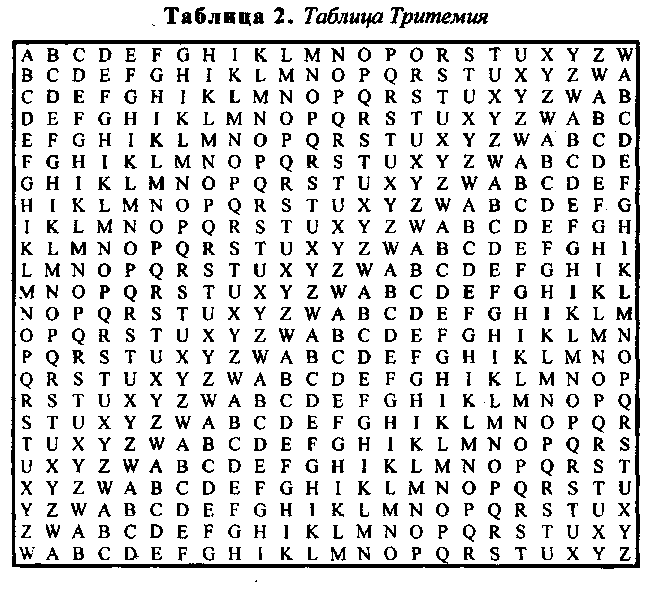
Имея два таких прибора, корреспонденты догадывались о первой индексной букве на подвижном диске. При шифровании сообщения отправитель ставил индексную букву против любой буквы большого диска. Он информировал корреспондента о таком положении диска, записывая эту букву внешнего диска в качестве первой буквы шифртекста. Очередная буква открытого текста отыскивалась на неподвижном диске и стоящая против неё буква меньшего диска являлась результатом её зашифрования. После того как были зашифрованы несколько букв текста, положение индексной буквы изменялось, о чём также сообщалось корреспонденту.

Такой шифр имел две особенности, которые делают изобретение Альберти событием в истории криптографии. Во-первых, в отличие от шифров простой замены шифровальный диск использовал не один, а несколько алфавитов для зашифрования. Такие шифры получили название многоалфавитных. Во-вторых, шифровальный диск позволял использовать так называемые коды с перешифрованием, которые получили широкое распространение лишь в конце XIX в., то есть спустя четыре столетия после изобретения Альберти. Для этой цели на внешнем диске имелись цифры. Альберти составил код, состоящий из 336 кодовых групп, занумерованных от 11 до 4444. Каждому кодовому обозначению соответствовала некоторая законченная фраза. Когда такая фраза встречалась в открытом сообщении, она заменялась соответствующим кодовым обозначением, а с помощью диска цифры зашифровы­вались как обычные знаки открытого текста, превращаясь в буквы.

Богатым на новые идеи в криптографии оказался XVI в. Многоалфавитные шифры получили развитие в вышедшей в 1518 г. первой печатной книге по криптографии под названием "Полиграфия". Автором книги был один из самых знаме­нитых ученых того времени аббат Иоганнес Тритемий. В этой книге впервые в криптографии появляется квадратная таблица. Шифралфавиты записаны в строки таблицы один под дру­гим, причем каждый из них сдвинут на одну позицию влево по сравнению с предыдущим (см. табл. 2).

Тритемий предлагал использовать эту таблицу для многоалфавитного зашифрования самым простым из возможных способов: первая буква текста шифруется первым алфавитом, вторая буква — вторым и т. д. В этой таблице не было отдельного алфавита открытого текста, для этой цели служил алфавит первой строки. Таким образом, открытый текст, начинающийся со слов HUNC CAVETO VIRUM ..., приобретал вид HXPF GFBMCZ FUEIB ... .

Преимущество этого метода шифрования по сравнению с методом Альберти состоит в том, что с каждой буквой задействуется новый алфавит. Альберти менял алфавиты лишь по­сле трех или четырех слов. Поэтому его шифртекст состоял из отрезков, каждый из которых обладал закономерностями открытого текста, которые помогали вскрыть криптограмму. Побуквенное зашифрование не дает такого преимущества. Шифр Тритемия является также первым нетривиальным примером периодического шифра. Так называется многоалфавитный шифр, правило зашифрования которого состоит в использовании периодически повторяющейся последовательности простых замен.



В 1553 г. Джованни Баттиста Белазо предложил использовать для многоалфавитного шифра буквенный, легко запо­минаемый ключ, который он назвал паролем. Паролем могло служить слово или фраза. Пароль периодически записывался над открытым текстом. Буква пароля, расположенная над буквой текста, указывала на алфавит таблицы, который исполь­зовался для зашифрования этой буквы. Например, это мог быть алфавит из таблицы Тритемия, первой буквой которого являлась буква пароля. Однако Белазо, как и Тритемий, использовал в качестве шифралфавитов обычные алфавиты.

Воскресить смешанные алфавиты, которые применял Альберти, и объединить идеи Альберти с идеями Тритемия и Белазо в современную концепцию многоалфавитной замены выпало на долю итальянца Джованни де ла Порта. Ему было 28 лет, когда он в 1563 г. опубликовал книгу "О тайной переписке". По сути, эта книга являлась учебником по криптогра­фии, содержащим криптографические познания того времени. Порта предложил использовать квадратную таблицу с периодически сдвигаемым смешанным алфавитом и паролем. Он советовал выбирать длинный ключ. Впервые им был предложен шифр простой биграммной замены, в котором пары букв представлялись одним специальным графическим символом. Они заполняли квадратную таблицу размером , строки и столбцы которой занумерованы буквами алфавита



ABCDEFGHILMNOPQRSTUZ

Например, биграмма ЕА заменялась символом биграмма



LF — символом и т. д. В своей книге Порта ввел многоал­фавитный шифр, определяемый табл. 3.

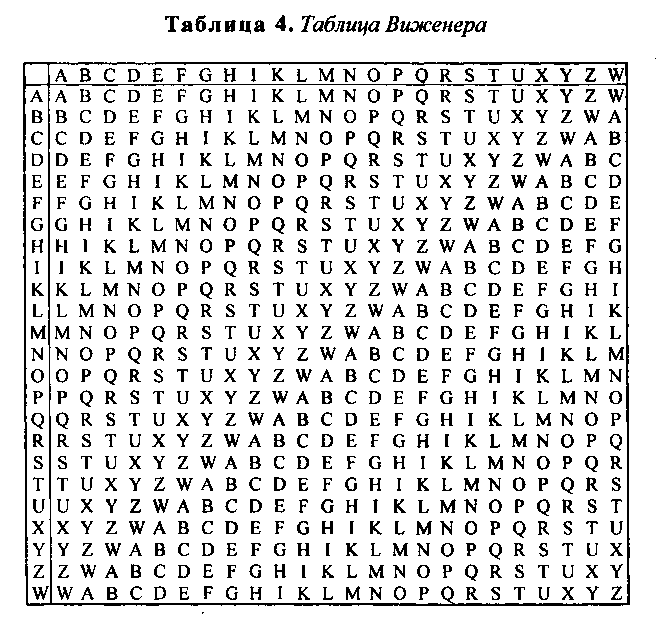


Таблица 3. Таблица Порта

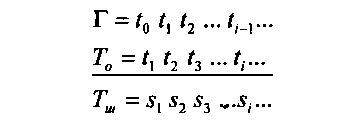
|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A | А | B | С | D | E | F | G | H | I | К | L | M |
| B | N | O | P | Q | R | S | T | U | X | У | Z | W |
| C | А | B | С | D | E | F | G | H | I | К | L | M |
| D | O | Р | Q | R | S | T | U | X | У | Z | W | N |
| Е | А | B | С | D | E | F | G | H | I | К | L | M |
| F | Р | Q | R | S | T | U | X | У | Z | W | N | O |
| G | А | B | С | D | E | F | G | H | I | К | L | M |
| Н | Q | R | S | T | U | X | У | Z | W | N | O | P |
| I | А | B | С | D | E | F | G | H | I | К | L | M |
| К | R | S | T | U | X | У | Z | W | N | O | Р | Q |
| L | А | B | С | D | E | F | G | H | I | К | L | M |
| М | S | T | U | X | У | Z | W | N | O | Р | Q | R |
| N | А | B | С | D | E | F | G | H | I | К | L | M |
| O | T | U | X | У | Z | W | N | O | P | Q | R | S |
| Р | А | B | С | D | E | F | G | H | I | К | L | M |
| Q | U | X | У | Z | W | N | O | P | Q | R | S | T |
| R | А | B | С | D | E | F | G | H | I | К | L | M |
| S | X | У | Z | W | N | O | P | Q | R | S | T | U |
| Т | А | B | С | D | E | F | G | H | I | K | L | M |
| U | У | Z | W | N | O | P | Q | R | S | T | U | X |
| Х | А | B | С | D | E | F | G | H | I | K | L | M |
| Y | Z | W | N | O | P | Q | R | S | T | U | X | У |
| Z | А | B | С | D | E | F | G | H | I | K | L | M |
| W | W | N | O | P | Q | R | S | T | U | X | y | Z |

Шифрование осуществляется при помощи лозунга, который пишется над открытым текстом. Буква лозунга определя­ет алфавит (заглавные буквы первого столбца), расположенная под ней буква открытого текста ищется в верхнем или нижнем полуалфавите и заменяется соответствующей ей буквой второго полуалфавита. Например, фраза, начинающаяся словами HUNC СAVETO VIRUM..., будет зашифрована при помощи лозунга DE LA PORTA в XFHP YTMOGA FQEAS.

Еще одно важное усовершенствование многоалфавитных систем, состоящее в идее использования в качестве ключа текста самого сообщения или же шифрованного текста, при­надлежит Джероламо Кардано и Блезу де Виженеру. Такой шифр был назван самоключом. В книге Виженера 'Трактат о шифрах" самоключ представлен следующим образом. В про­стейшем случае за основу бралась таблица Тритемия с добав­ленными к ней в качестве первой строки и первого столбца алфавитами в их естественном порядке. Позже такая таблица стала называться таблицей Виженера. Подчеркнем, что в общем случае таблица Виженера состоит из циклически сдви­гаемых алфавитов, причем первая строка может быть произ­вольным смешанным алфавитом (см. табл. 4).



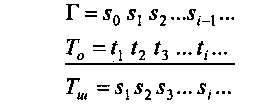
Первая строка служит алфавитом открытого текста, а первый столбец — алфавитом ключа. Для зашифрования открытого сообщения Виженер предлагал в качестве ключевой последовательности (Г) использовать само сообщение (Т0) с добавленной к нему в качестве первой буквы(), известной отправителю и получателю (этим идея Виженера отличалась от идеи Кардано, у которого не было начальной буквы и система которого не обеспечивала однозначности расшифрования). Последовательности букв подписывались друг под другом:



При этом пара букв, стоящих друг под другом в Г и, указывала, соответственно, номера строк и столбцов таблицы, на пресечении которых находится знак шифрованного текста (Тш). Например, фраза HUNC CAVETO VIRUM ..., использованная в предыдущих примерах, и начальная буква Р дают шифртекст YCHP ECUWZHIDAMG.

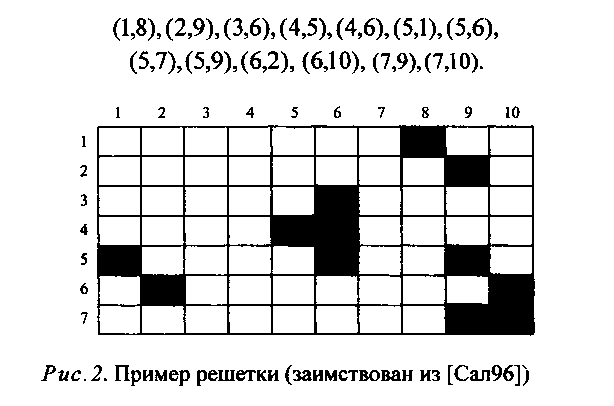


Во втором варианте Виженер предлагал в качестве ключевой последовательности использовать шифрованный текст:

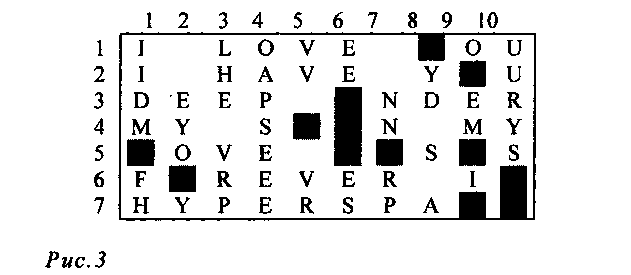


Самоключ Виженера был незаслуженно забыт на долгое время, а под шифром Виженера до сих пор понимают самый простой вариант с коротким ключевым словом и с таблицей, состоящей из обычных алфавитов.

Кардано принадлежит также идея поворотной решетки как средства шифрования. Изначально обычная решетка представляла собой лист из твердого материала, в котором через неправильные интервалы сделаны прямоугольные вы­резы высотой для одной строчки и различной длины. Накла­дывая эту решетку на лист писчей бумаги, можно было запи­сывать в вырезы секретное сообщение. После этого, сняв ре­шетку, нужно было заполнить оставшиеся свободные места на листе бумаги неким текстом, маскирующим секретное сооб­щение. Подобным стеганографическим методом маскировки сообщения пользовались многие известные исторические ли­ца, например кардинал Ришелье во Франции и русский ди­пломат и писатель А. Грибоедов. Так, Ришелье использовал прямоугольник размера 7x10. Для длинных сообщений пря­моугольник использовался несколько раз. Прорези трафарета размещались в позициях:



Следующий текст выглядит как невинное любовное письмо (см. рис. 3).



Однако используя трафарет Ришелье, получим зловещую команду:

YOU KILL ATONES

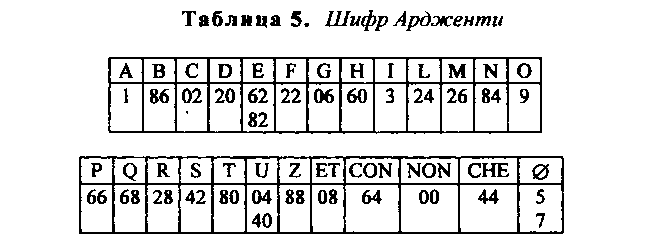
Кардано использовал квадратную решетку, которая своими вырезами однократно покрывает всю площадь квадрата при ее самосовмещениях. На основе такой решетки он построил шифр перестановки.

Нельзя не упомянуть в историческом обзоре имени Матео Ардженти, работавшего в области криптографии в начале XVII в. Он составил руководство по криптографии на 135 листах, изданное в переплете из телячьей кожи. В этой книге впервые предложено использовать некоторое слово в качестве мнемонического ключа для смешанного алфавита. Началом смешанного алфавита служило ключевое слово (как правило, без повторяющихся букв), за которым следовали остальные буквы в их естественном порядке. Например, ключевое слово PIETRO дает смешанный латинский алфавит

PIETROABCDFGHLMNQSUZ

Такие смешанные алфавиты часто использовались в качестве алфавитов шифртекста в шифрах простой замены.

С целью усложнения шифра простой замены Ардженти вводил пустышки, которые добавлялись в шифрованное сообщение, использовал шифробозначения разной значности, для некоторых частых сочетаний букв текста вводил отдельные обозначения, придавал частым буквам несколько обозна­чений. Позже подобные идеи получили широкое распространение. Приведем пример шифра Ардженти (см. табл. 5).



Слово ARGENTI может быть зашифровано многими способами, например так:

5128068285480377 или же так:

172850675628455803

Наибольшим достижением Ардженти считается разработанный им буквенный код — один из шифров замены, в котором буквы, слоги, слова и целые фразы заменялись группами букв. Необходимым количеством словарных величин в коде в то время считалось 1200.

В истории криптографии XVII — XVIII в. называют эрой "черных кабинетов". В этот период во многих государствах Европы, в первую очередь во Франции, получили развитие дешифровальные подразделения, названные "черными кабинетами". Первый из них образован по инициативе кардинала Ришелье при дворе короля Людовика XIII. Его возглавил первый профессиональный криптограф Франции Антуан Россиньоль. Следует отметить, что некоторые оригинальные идеи, возникшие в криптографии в этот период, связаны с именем самого Ришелье, который использовал, например, для секретной переписки с королем оригинальный шифр перестановки с переменным ключом. Его использование становится понятным из следующего примера:

Шифр Ришелье

Ключ: 2741635; 15243; 671852493; 07;28615;943;...

Открытый текст:

LETTER SENT TO THE EMPEROR GIVING FULL DETAIL

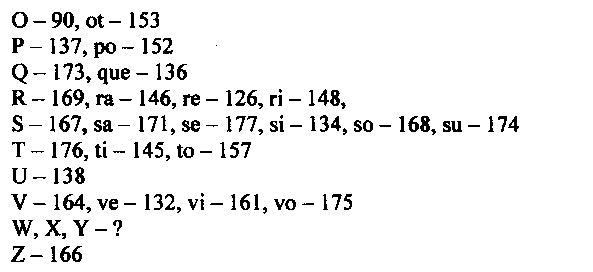
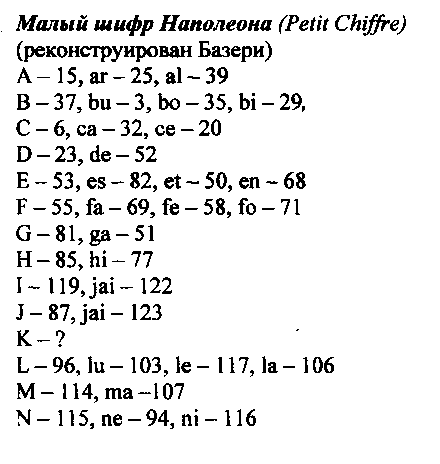
Ключ:

(2741635) (15243) (671852493) (07) (28615)(943)(2741635)

Шифртекст:

TLRTSEE ETOTN EPOEMTHER N1 LUGIG VFR TLIE SAD

Известно, что Ришелье пользовался также кодами. Попутно отметим, что свой несложный код был и у знаменитого Наполеона:



В то время в Европе получили широкое распространение шифры, называемые номенклаторами, объединявшие в себе простую замену и код. В простейших номенклаторах код состоял из нескольких десятков слов или фраз с двухбуквенными кодовыми обозначениями. Со временем списки заменяемых слов в номенклаторах увеличились до двух или трех тысяч эквивалентов слогов и слов. В царской России XVIII в. закодированное открытое сообщение шифровалось далее простой заменой.

Кстати, несколько слов о русской криптографии. Уже с XIV в. в Новгороде существовала техника тайного письма. Использовались в основном шифры простой замены. Благодаря торговым связям Новгорода с Германией в России становятся известными многие западные разработки, в том числе новые системы шифрования. Учреждение постоянной почтовой связи России с Европой дало возможность развитию шифрованной переписки. Благодаря привлечению Петром I для разработки проектов развития образования и государственного устройства России знаменитого Готфрида Вильгельма Лейбница, который известен и как криптограф, в Петербурге появилась цифирная палата, задачами которой было развитие и использование систем шифрования.

Когда Россиньоль начинал свою карьеру, в номенклато­рах как элементы открытого текста, так и элементы кода рас полагались в алфавитном порядке (или в алфавитном и числовом порядке, если код был цифровой). Россиньоль заметил, что такой "параллелизм" открытого текста и кода облегчал восстановление открытого текста. Если, например, он устанавливал, что в английской депеше 137 заменяет FOR, a 168 — IN, то он уже знал, что 21 не может заменять ТО, так как цифровые кодовые обозначения для слов, начинающихся с Т, должны быть больше, нежели для слов, начинающихся с I. Обнаружив такую слабость, Россиньоль перемешивал кодовые элементы по отношению к открытому тексту. На одном листе он располагал элементы открытого текста в алфавитном порядке, а кодовые элементы — вразброс, на другом листе для облегчения, расшифрования кодовые элементы стояли в алфавитном порядке, тогда как их открытые эквиваленты были разбросаны. Это явилось значительным усовершенствованием подобных шифрсистем. Однако составление неалфавитных номенклаторов обходилось очень дорого, и, таким образом, по соображениям экономии и в ущерб надежности многие номенклаторы регрессировали к упрощенному алфавитному типу.

В Англии тоже был свой "черный кабинет". В его работе в XVII в. заметное место занимал Джон Валлис, известный как крупнейший английский математик до Исаака Ньютона. Работы по вскрытию шифров для парламента привели к назначению Валлиса в 1649 г. в Оксфорд профессором геометрии в возрасте 32 лет. В своем труде "Арифметика бесконечного" он сделал выводы, которые послужили Ньютону стартовой площадкой для разработки интегрального исчисления. Валлис ввел знак для бесконечности и первый путем интерполяции вычислил число . Кстати, само это обозначение также принадежит ему.



В Германии начальником первого дешифровального отделения был граф Гронсфельд, создавший один из вариантов усовершенствования шифра Виженера. Он взял числовой, легко запоминаемый лозунг. Вместо таблицы Виженера ис пользовался один несмешанный алфавит. При шифровании знаки открытого текста выписывались под цифрами лозунга. Очередная буква открытого текста заменялась буквой алфавита, отстоящей от нее вправо на количество букв, равное соответствующей цифре лозунга.

Шифр Гронсфелъда

Открытый текст: GERMANY

Лозунг: 13 5 7 9

Алфавит: ABCDEFGHIJKLMNOPQRST UVWXYZ

Для удобства выпишем алфавит с порядковыми номерами букв:

ABCDEFGHI JKLM 1 2 3 4 5 6 7 8 9 10 И 12 13

NOPQR S TUVWXYZ

14 15 16 17 18 19 20 21 22 23 24 25 26

и лозунг над текстом:

13 5 7 9 13 GERMANY

Теперь легко получить шифрованный текст:

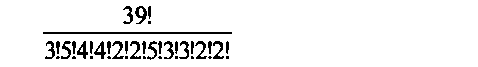
HHWTJOB

Любопытен опыт использования криптографии при составлении астрономических анаграмм. Одно из таких применений связано с открытием колец Сатурна.

В годы жизни Галилео Галилея существовал обычай закреплять за собой право на первенство в каком-либо открытии своеобразным способом. Напав на открытие, которое нуждается в дальнейшем подтверждении, ученый из опасения, чтобы его не опередили другие, прибегал к помощи анаграммы (перестановке букв); он кратко объявлял о сущности своего открытия в форме анаграммы, истинный смысл которой был известен лишь ему одному. Это давало ученому возможность не спеша проверить свое открытие, а в случае появления другого претендента — доказать свое первенство. Когда же он окончательно убеждался в правильности первоначальной догадки, он раскрывал секрет анаграммы. Заметив в свою несовершенную подзорную трубу, что Сатурн имеет по бокам какие-то придатки, Галилей поспешил сделать заявку на это открытие и опубликовал следующий набор букв:

SMAISMRMIELMEPOETALEUMIBUVNEUGTTAVIRAS

Задача восстановления открытого текста (без какой-либо дополнительной информации об использованном преобразовании) требует перебора



возможных перестановок букв криптограммы (это — число перестановок с повторениями). Приведенное число имеет в своей записи примерно 35 цифр.

Современник итальянского ученого Иоганн Кеплер с присущим ему беспримерным терпением затратил немало труда на то, чтобы проникнуть в сокровенный смысл заявки Галилея, и ему казалось, что он добился этого, когда из опубликованных букв (опустив две из них) составил такую латинскую фразу:

SALVE, UMBISTINEUM GEMINAUM MARTIA PROLES (Привет вам, близнецы, Марса порождение)

Кеплер был убежден, что Галилей открыл те два спутника Марса, существование которых подозревал он сам (они в действительности и были открыты, но спустя два с половиной века). Однако остроумие Кеплера на этот раз не привело к цели. Когда Галилей раскрыл, наконец, секрет своей заявки, оказалось, что фраза (если двумя буквами пренебречь) такова:

ALTISSIMUM PLANETAM TERGEMINUM OBSERVAVI

(Высочайшую планету тройною наблюдал)

Из-за слабости своей трубы Галилей не мог понять истинного значения этого "тройного" образа Сатурна, а когда спустя несколько лет боковые придатки планеты совершенно "исчезли", Галилей решил, что ошибся, и никаких придатков у Сатурна нет. Открыть кольца Сатурна удалось только через полвека Гюйгенсу. Подобно Галилею, он не сразу опубликовал свое открытие, а скрыл догадку под тайнописью:

AAAAAAACCCCCDEEEEGHimmLLLLMMNNNNNNNNN OOOOPPQRRSTTTTTUUUUU

Спустя три года, убедившись в правильности своей догадки, Гюйгенс обнародовал смысл заявки:

Annulo cingitur, tenui, piano, nusquam cohaerente,

ad eclipticam inclinato

(Кольцом окружен тонким, плоским, нигде

не прикасающимся, к эклиптике наклоненном)

В целом можно сказать, что XVII и XVIII вв. не дали новых идей в криптографии. Эра "черных кабинетов" закончилась в 40-х годах XIX в. в период революционного подъема.

Много новых идей в криптографии принес XIX в. Изобретение в середине XIX в. телеграфа и других технических видов связи дало новый толчок развитию криптографии. Информация передавалась в виде токовых и бестоковых посылок, то есть представлялась в двоичном виде. Поэтому возникла проблема "рационального" представления информа ции, которая решалась с помощью кодов. Коды позволяли передать длинное слово или целую фразу двумя-тремя знаками. Появилась потребность в высокоскоростных способах шифрования и в корректирующих кодах, необходимых в связи с неизбежными ошибками при передаче сообщений.

Однако еще до изобретения телеграфа появился ряд интересных шифровальных устройств. Приблизительно в 1800 г. была создана одна шифровальная система, занимающая особое место в истории криптографии. Речь идет о "дисковом шифре" Т. Джефферсона — первого государственного секретаря США, ставшего позже третьим президентом.

Дисковый шифратор Т. Джефферсона состоял из 25 - 36 деревянных дисков одинакового размера, насаженных на общую ось

На одном конце оси имелась неподвижная головка, на другом — резьба и гайка, с помощью которой все диски фиксировались в любом нужном угловом положении. Имелась также прямолинейная рейка, способная вращаться на оси и позволяющая выделить строку букв на дисках, параллельную оси. На боковой поверхности каждого диска, разделенной на 26 равных частей, наносились буквы смешанных английских алфавитов. Для зашифрования части сообщения (длина которой равнялась числу дисков на оси) под рейку, находящуюся в фиксированном угловом положении, подводилась первая бук ва сообщения, найденная на первом диске, затем — вторая буква сообщения, найденная на втором диске, и т. д., так, чтобы все подобранные буквы оказались в одной строке. Положение дисков фиксировалось гайкой, после чего рейка подводилась под любую другую строку цилиндра, буквы которой составляли шифрованный текст. При расшифровании буквы шифрованного текста, набранные на последовательных дисках, подводились аналогичным образом под рейку, положение дисков фиксировалось гайкой, после чего с помощью рейки просматривались образовавшиеся строки цилиндра, среди которых несложно было найти открытое сообщение.

Кажущаяся некорректность, связанная с возможностью неоднозначности расшифрования, устраняется достаточно большим числом используемых дисков. Это замечание относится, конечно, лишь к осмысленным текстам. При зашифровании неосмысленных текстов требовалась дополнительная информация о величине сдвига рейки, без чего однозначное расшифрование невозможно.

Такая шифрсистема имеет огромное количество ключевых элементов. К ним относятся: расположение букв алфавита на дисках, расстановка дисков на оси, выбор набора дисков из имеющегося запаса. Дисковый шифр можно отнести по типу к многоалфавитной замене. Его особенностью является поблочный характер зашифрования, при котором каждый участок текста (блок) шифруется независимо от других. Позже такие шифры стали называться блочными шифрами.

Вместо того чтобы (пользуясь служебным положением) внедрить свое замечательное изобретение в практику, Джефферсон, по-видимому, отложил его в архив и предал забвению. Шифр был обнаружен в его бумагах в библиотеке конгресса лишь в 1922 г., по иронии судьбы именно в том году, когда в армии США начали применять почти аналогичную систему, изобретенную независимо от Джефферсона.

В 1817 г. другой американец Десиус Уодсворт сконструировал шифровальное устройство, которое также внесло но вый принцип в криптографию. Его нововведение состояло в том, что он сделал алфавиты открытого и шифрованного текстов различных длин. Устройство, с помощью которого он это осуществил, представляло собой диск, на котором были расположены два подвижных кольца с алфавитами. Внешний алфавит состоял из 26 букв и 7 цифр (от 2 до 8). Внутренний алфавит состоял лишь из 26 букв. Диск имел подобие неподвижной часовой стрелки, в двух прорезях которой появлялись расположенные друг под другом буквы алфавитов. На внутреннем кольце указывалась буква открытого текста, на внешнем кольце — соответствующая буква шифртекста. Оба кольца могли вращаться и были связаны друг с другом с помощью двух шестерен, одна из которых имела 33 зубца, а другая — 26. Буквы и цифры внешнего кольца были съемными и могли быть собраны в любом порядке. Перед зашифро­ванием корреспонденты договаривались относительно взаимного начального положения обоих колец. Для установки дисков в такое положение шестерни можно было разъединить. Проследим на примере слова "введение" процесс за­шифрования.

Сначала внутреннее кольцо поворачивалось до тех пор, пока в прорези стрелки не показывалась буква "в". Стоящая в другой прорези буква внешнего кольца записывалась в качестве первой буквы шифртекста. Затем внутреннее кольцо вращалось до тех пор, пока буква "в" вновь не показывалась в прорези. Это вращение посредством шестерен передавалось на внешнее кольцо, но из-за различия в числе букв алфавитов оно совершало лишь полного оборота, в то время как



внутреннее кольцо совершало полный оборот. Значит, второй знак шифртекста располагался во внешнем алфавите на расстоянии семи мест вперед от первого знака, несмотря на то, что оба знака представляли одну и ту же букву открытого текста. Если этот процесс зашифрования осуществлять дальше, то эквиваленты шифртекста для буквы "в" начнут повторяться лишь после того, как будут использованы все 33 буквы и цифры внешнего алфавита. Это объясняется тем, что числа 26 и 33 не имеют общих делителей, благодаря которым такое повторение могло бы произойти раньше. Следующие буквы открытого текста шифровались аналогично.

Такая шифрсистема реализует периодическую многоалфавитную замену. Различие чисел букв алфавитов открытого и шифрованного текстов приводит к существенным отличиям этой системы от предыдущих многоалфавитных систем. Так, в устройстве Уодсворда используется 33 шифралфавита, а не 24 или 26, как в системах Тритемия или Виженера. Важнее то, что эти алфавиты используются не непосредственно один за другим, а в произвольном порядке, который зависит от букв открытого текста. Этот произвольный порядок служит гораздо более надежной защитой шифра, чем правильная последовательность использования алфавитов, как в системе Тритемия.

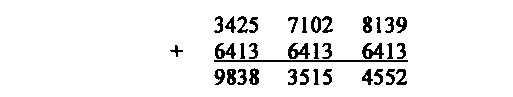
Идея Уодсворда была незаслуженно забыта. Славу открытия приписывают английскому ученому Чарлзу Уитстону, который значительно позже и независимо изобрел свое устройство на том же принципе (см. рис. 5). Основное отличие заключалось в том, что в устройстве Уитстона алфавиты были неподвижными, но зато имелась пара подвижных стрелок, соединенных шестеренками.

Уитстон более известен как ученый, предложивший идею электрического телеграфа, изобретатель концертино, автор первых стереоскопических рисунков. Он высказал гипотезу о создании говорящих машин, разработал метод точного измерения электрического сопротивления, который называется "мостик Уитстона".

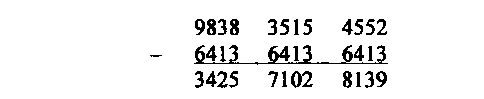
Впервые свое устройство Уитстон продемонстрировал на Всемирной выставке в Париже в 1876 г. На внешнем кольце находился алфавит открытого текста, состоящий из 27 элементов: 26 букв, расположенных в обычном порядке, и знака пробела между словами. Внутренний алфавит состоял из 26 букв, расположенных в произвольном порядке.

Уитстон изобрел шифр, который позже стали называть шифром Плейфера. Дело в том, что Лион Плейфер, замести­тель председателя Палаты общин, министр почт, председатель Британской ассоциации развития науки, был другом Уитстона, был похож на него, так что их часто путали. В 1854 г. Плейфер продемонстрировал систему шифрования, которую он назвал "недавно открытый симметричный шифр Уитстона". Это был первый из известных биграммных буквенных шифров (напомним, что биграммный шифр Порта был значковым). То обстоятельство, что Плейфер популяризировал изобретение Уитстона, сохранило его имя в названии шифра. Этот шифр использовался англичанами в период первой мировой войны.

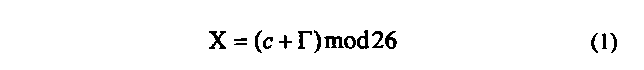
Во второй половине XIX в. появился весьма устойчивый способ усложнения числовых кодов — гаммирование. Он заключался в перешифровании закодированного сообщения с помощью некоторого ключевого числа, которое и называлось гаммой. Шифрование с помощью гаммы состояло в сложении всех кодированных групп сообщения с одним и тем же ключевым числом. Эту операцию стали называть "наложением гаммы". Например, результатом наложения гаммы 6413 на кодированный текст 3425 7102 8139 являлась числовая последовательность 9838 3515 4552:



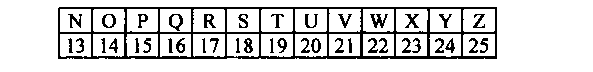
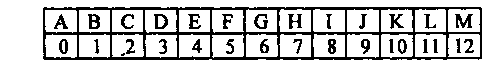
Единицы переноса, появляющиеся при сложении между кодовыми группами, опускались. "Снятие гаммы" являлось обратной операцией:



В 1888 г. француз маркиз де Виари в одной из своих научных статей, посвященных криптографии, обозначил греческой буквой X любую букву шифрованного текста, греческой буквой Г любую букву гаммы и строчной буквой С любую букву открытого текста. Он, по сути, доказал, что алгебраическая формула



воспроизводит зашифрование по Виженеру при замене букв алфавита числами согласно следующей таблице:



Тем самым была заложена алгебраическая основа для исследования шифров замены типа шифра Виженера. Используя уравнение шифрования, можно было отказаться от громоздкой таблицы Виженера.

Позже лозунговая гамма стала произвольной последовательностью, а шифр с уравнением шифрования (1) стал называться шифром гаммирования.

Еще одним известным криптографом того времени был голландец Керкгоффс. Его полным именем было Жан-Вильгельм-Губерт-Виктор-Франсуа-Александр-Огюст Керкгоффс Ван Ньювенгоф. Разносторонний ученый, преподававший 6 иностранных языков, историю и математику, он в возрасте 47 лет написал книгу "Военная криптография". В ней сформулированы 6 конкретных требований к шифрам, два из которых относятся к стойкости шифрования, а остальные — к эксплуатационным качествам. Одно из них ("компрометация системы не должна причинять неудобств корреспондентам") стало называться "правилом Керкгоффса". Суть этого правила состоит в том, что стойкость (или надежность) шифра определяется лишь секретностью ключа. Другими словами, оценка качества шифра (на основе некоторого шифрованного текста) должна проводиться при условии, что о данном шифре известно все, кроме использованного ключа.

XX в. "прославился" двумя мировыми войнами. Эти войны оставили свой отпечаток на всех процессах, происходивших в человеческом обществе. Они не могли не сказаться и на развитии криптографии.

В период первой мировой войны в качестве полевых шифров широко использовались ручные шифры, в первую очередь шифры перестановки с различными усложнениями. Это были вертикальные перестановки, усложненные перекодировкой исходного алфавита, а также двойные вертикальные перестановки.

Первая мировая война явилась поворотным пунктом в истории криптографии: если до войны криптография представляла собой достаточно узкую область, то после войны она стала широким полем деятельности. Причина этого состояла в необычайном росте объема шифрпереписки, передаваемой по различным каналам связи. Криптоанализ стал важнейшим элементом разведки.

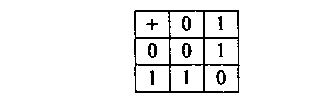
Прогресс этой области криптографии характеризовался и изменениями в самом криптоанализе. Эта наука переросла методы индивидуальной работы криптоаналитика над криптограммой. Системы секретной связи перестали быть настолько малочисленными и однородными, что один специалист мог овладеть всеми специализациями. Характер используемых шифров потребовал для их вскрытия скрупулезного анализа переписки, поиска ситуаций, благоприятствующих успешному криптоанализу, знания соответствующей обстановки. Кроме того, криптоанализ обогатился большим опытом использования в годы войны ошибок неопытных или ленивых шифровальщиков. Еще Ф. Бэкон писал, что "в результате неловкости и неискусности тех рук, через которые проходят величайшие секреты, эти секреты во многих случаях оказывались обеспеченными слабейшими шифрами". Этот печальный опыт привел к необходимости введения строгой дисциплины среди шифровальщиков.

Несмотря на указанные последствия, первая мировая война не породила никаких новых научных идей в криптографии. Наоборот, полностью исчерпали свои возможности ручное шифрование, с одной стороны, и техническая сторона криптоанализа, состоявшая в подсчете частот встречаемости знаков, с другой.

В тот период проявились таланты целого ряда ставших впоследствии известными криптографов. В их числе был Г. О. Ярдли, который вскоре после вступления США в войну в 1917 г. убедил военное министерство в необходимости создания криптографической службы. В 27 лет он был назначен начальником криптографического отдела (MI-8) разведки военного министерства. При отделе было создано учебное отделение по подготовке криптоаналитиков для американской армии. Отдел MI-8 добился больших успехов в дешифровании дипломатической переписки многих развитых стран. В 1919 г. отдел был преобразован в "черный кабинет" с совместным финансированием от военного министерства и госдепартамента в объеме 100 тыс. долларов в год. Одной из главных задач "черного кабинета" было раскрытие японских кодов, некоторые из которых содержали до 25 тысяч кодовых величин. В период с 1917 по 1929 г. специалистам "черного кабинета" удалось дешифровать более 45 тысяч криптограмм различных стран, в том числе и Японии.

Ярдли, желая упрочить успехи, подготовил докладную записку Президенту США о мерах по укреплению своей службы. Однако ставший в то время Государственным секретарем Г. Стимсон был шокирован, узнав о существовании "черного кабинета", и полностью осудил его деятельность. Ему принадлежит знаменитая фраза: "Джентльмены не читают писем друг друга". Финансирование "черного кабинета" было прекращено, и Ярдли лишился работы. Он написал книгу "Американский черный кабинет", в которой рассказал о многих успехах по дешифрованию. Книга была издана большими тиражами в ряде стран и произвела эффект разорвавшейся бомбы. Позже он написал книгу "Японские дипломатические секреты", в которой приводились многие японские телеграммы. Рукопись этой книги была конфискована по решению суда. Последние годы жизни Ярдли не занимался криптографией. Он умер в 1958 г. и был похоронен с воинскими почестями на Арлингтонском национальном кладбище. В некрологе он был назван "отцом американской криптографии". Значительный успех в криптографии связан с еще одним  
американцем — Г. Вернамом. В 1917 г. он, будучи сотрудником телеграфной компании, предложил идею автоматического  
шифрования телеграфных сообщений. Речь шла о своеобразном наложении гаммы на знаки алфавита, представленные в  
соответствии с телетайпным кодом Бодо пятизначными "импульсными комбинациями". Например, буква а представлялась комбинацией ( + + – –), а комбинация ( + + – + + ) представляла символ перехода от букв к цифрам. На бумажной ленте, используемой при работе телетайпа, знаку " + " отвечало наличие отверстия, а знаку "-" — его отсутствие. При считывании с ленты металлические щупы проходили через отверстия, замыкали электрическую цепь и тем самым посылали в линию импульс тока.

Вернам предложил электромеханически покоординатно складывать "импульсы" знаков открытого текста с "импульсами" гаммы, предварительно нанесенными на ленту. Сложение проводилось "по модулю 2". Имеется в виду, что если "+" отождествить с 1, а "-" с 0, то сложение определяется двоичной арифметикой:



Например, наложение на знак открытого текста (11001) знака гаммы (01111) давало знак шифртекста (10110). При расшифровании нужно было произвести ту же операцию со знаком шифртекста: (10110)(01111) = (11001).



Вернам сконструировал и устройство для такого сложения. Замечательно то, что процесс шифрования оказывался полностью автоматизированным, в предложенной схеме исключался шифровальщик. Кроме того, оказывались слитыми воедино процессы шифрования-расшифрования и передачи по каналу связи. Тем самым наряду с традиционной схемой предварительного шифрования, когда по каналу передается предварительно зашифрованное сообщение, положено начало линейному шифрованию.

В 1918 г. два комплекта соответствующей аппаратуры были изготовлены и испытаны. Испытания дали положительные результаты. Единственное неудовлетворение специалистов-криптографов было связано с гаммой. Дело в том, что первоначально гамма была нанесена на ленту, склеенную в кольцо. Несмотря на то, что знаки гаммы на ленте выбирались случайно, при зашифровании длинных сообщений гамма регулярно повторялась. Этот недостаток так же отчетливо осознавался, как и для шифра Виженера. Уже тогда хорошо понимали, что повторное использование гаммы недопустимо даже в пределах одного сообщения. Хотя сам Вернам не был математиком, он, может и неосознанно, предлагал однократное использование гаммы. Попытки удлинить гамму приводили к неудобствам в работе с длинным кольцом. Тогда был предложен вариант с двумя лентами, одна из которых шифровала другую, в результате чего получалась гамма, имеющая длину периода, равную произведению длин исходных периодов.

Несмотря на то, что шифр Вернама обладал целым рядом достоинств, он не получил широкого распространения. Трудности, связанные с изготовлением, рассылкой и учетом использованной гаммы, особенно в условиях военной связи, при передаче больших объемов сообщений, стали непреодолимыми. Вспомнили о шифре Вернама лишь накануне второй мировой войны.

Почти половина XX в. была связана с использованием колесных шифраторов. Различные их конструкции были запатентованы примерно в одно и то же время (в период 1917 — 1919 гг.) в разных странах: американцем Э. X. Хеберном, голландцем Х.Ф.Кохом, немцем А. Шербиусом и шведом А. Г. Даммом.

Чертежи своей схемы на основе шифрующего диска Хеберн представил в 1917 г., и уже в следующем году был по строен первый дисковый аппарат, получивший одобрение ВМС США. В 1921 г. Хеберн основал первую в США компанию по производству шифрмашин, которую через десять лет ждал бесславный конец, связанный с финансовыми трудно­стями.

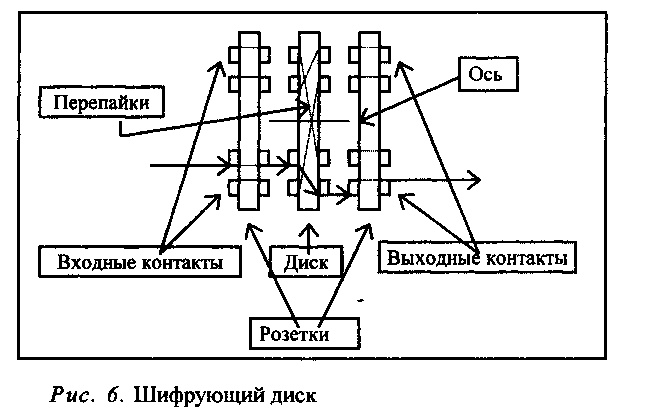
Что представлял собой шифрующий диск? Корпус диска (имевшего размеры хоккейной шайбы) состоял из изоляционного материала, например твердой резины. По окружностям каждой из его сторон были вмонтированы на равном расстоя­нии друг от друга 26 электрических контактов (см. рис. 6). Каждый контакт был соединен внутри корпуса с некоторым контактом на другой стороне. Контакты на входной стороне представляли буквы открытого текста, контакты на выходной стороне — буквы шифртекста.

Диск устанавливался на оси между двумя неподвижными пластинами (розетками), каждая из которых также была изготовлена из изолятора и имела 26 контактов, соответствующих расположению контактов на диске. Контакты входной розетки соединялись с клавиатурой пишущей машинки, печатающей буквы открытого текста. Контакты выходной розетки соеди­нялись с выходным устройством, указывающим буквы шифр-текста, например, с помощью лампочек. При фиксированном угловом положении диска электрические цепи, соединяющие входные и выходные контакты, реализовывали одноалфавит-ную замену. При повороте же диска (на углы ) схема реализовывала многоалфавитную замену (с 26 простыми за­менами).



Рядом с одним диском можно было установить и другие диски. Тем самым схема токопрохождения удлинялась и чис­ло возможных простых замен, реализуемых многодисковой схемой значительно возрастало. При движении к дисков по

простейшей схеме одометра получался период, равный 26 , который можно было сделать астрономическим числом. Подобные шифрмашины обслуживали значительную часть линий связи высшего командования ВМС США, начиная с 20-х годов.



X. Ф. Кох предлагал конструкцию шифрующего диска, в котором роль электричества выполняла пневматика. Речь идет о каналах, соединяющих входные и выходные контакты, по которым может проходить поток воздуха, водная или масляная струя и т. п. Любопытно, что подобные дисковые сис­темы на основе пневматики были реально изготовлены и ис­пользовались на практике.

Принцип шифрующего диска использовали и шифрмашины, разработанные А. Шербиусом. Самой знаменитой из них была "Энигма", которая в двух отношениях отличалась от других дисковых машин. Во-первых, после блока дисков была расположена неподвижная обратимая розетка, контакты которой были попарно соединены друг с другом. Импульс тока, приходивший на этот контакт, заворачивался и вновь проходил через блок дисков в противоположном направлении. Это давало двойное шифрование каждой буквы. Другая особенность "Энигмы" заключалась в неравномерном движении дисков, которое управлялось зубчатыми колесами.

В 1923 г. "Энигма" выставлялась на конгрессе международного почтового союза, однако это не способствовало ее коммерческому успеху: она не раскупалась. За десять лет фирма Шербиуса, производившая "Энигму", не получила прибыли и в 1934 г. была ликвидирована и передала свои ак­тивы другой фирме. После прихода к власти в Германии Гит­лера началось серьезное перевооружение армии, и немецкие специалисты сочли "Энигму" достаточно удобной и надежной шифрмашиной. В довоенный период и во время второй миро­вой войны "Энигма" широко использовалась в германской армии, ВМС и ВВС. Она была портативной (размером с пи­шущую машинку), работала от батареи, имела деревянный футляр. Ее серьезный недостаток состоял в том, что она не печатала шифртекст (а имела лишь загорающиеся лампочки, отвечающие буквам), и для быстрой работы требовались три или даже четыре человека — для чтения и набора на клавиа­туре текста сообщения, диктовки высвечивающихся букв шифртекста и их записи.

С "Энигмой" теснейшим образом связан ход многих событий периода второй мировой войны. Дело в том, что она являлась источником ценнейших сведений для английских спецслужб, читавших переписку "Энигмы" (в рамках операции "Ультра"). Эта информация стоила так дорого, что У. Черчилль пожертвовал городом Ковентри, когда ему стал известен план германской бомбардировки этого английского города. С "Энигмой" связано также появление первой в исто­рии вычислительной машины, сконструированной в 1942 г. для перебора ключевых элементов группой специалистов-криптографов под руководством известного математика А. Тьюринга.

Еще один патент на дисковую машину был выдан А. Г. Дамму в 1919 г. Устройство этой машины было настоль ко сложным, что никогда не было реализовано. Но его автор основал компанию по производству шифрмашин, которая впоследствии стала прибыльной. Среди вкладчиков капитала были Э. Нобель, племянник знаменитого А. Нобеля, и Ц. Хагелин, управляющий нефтедобывающей компанией братьев Нобелей в России и некоторое время бывший гене­ральным консулом Швеции в Санкт-Петербурге. До 1927 г. эта компания не имела больших успехов. Их появление было связано с именем сына Ц. Хагелина — Б. Хагелина, родивше­гося на Кавказе, проучившегося несколько лет в Петербургском университете и получившего позже диплом инженера-механика в Швеции.

В 1925 г. Б. Хагелину удалось модернизировать одну из машин Дамма, снабдив ее клавиатурой и индикаторными лампочками, как у "Энигмы". Это была также колесная машина, работающая, однако, по иному, чем дисковые машины, принципу. Она получила название В-21. Ее работа была осно­вана на матричном коммутаторе, в котором электрически изменялось соединение строк и столбцов для преобразования буквы открытого текста в букву шифртекста. Эти изменения определялись группой ключевых колес, каждое из которых имело по ободу выдвинутые или вдвинутые штифты. Колеса имели различные числа штифтов, так что период многоалфа­витного шифра, реализуемого машиной, был равен произве­дению чисел штифтов на всех колесах. В 1926 г. Б. Хагелин предложил В 21 шведской армии, которая сделала на нее большой заказ.

В 1927 г. Б. Хагелин возглавил фирму, выкупленную семьей Хагелин. Свою следующую машину В-211 он снабдил печатающим устройством, работавшим со скоростью около 200 знаков в минуту. Она была самой портативной печатающей шифрмашиной в 1934 г.

В том же году французский генштаб заказал Б. Хагелину карманную печатающую машину, которая могла бы обслуживаться одним человеком. Через некоторое время такая машина была изготовлена. Она реализовывала шифр гаммирования, причем для выработки гаммы была использована идея сумми­рующего устройства, состоящего из комбинационных линеек, расположенных в цилиндрическом барабане. На линейках рядами были расположены так называемые рейтеры. При повороте барабана на 360° рейтеры, вступая во взаимодейст­вие с другими элементами схемы, могли выдвигать некоторые линейки влево, причем число выдвинутых линеек и определя­ло значение знака гаммы (от 0 до 25) в данный такт шифрова­ния. Во взаимодействие с рейтерами вступали штифты, рас­положенные на колесах блока дисков, составляющего вторую основную часть машины. Размеры и схема движения дисков

обеспечивали период, приблизительно равный. Как расположение рейтеров, так и расположение штифтов могло легко меняться, они являлись ключевыми элементами. Это была машина С-36, ставшая впоследствии знаменитой. По размерам она была меньше телефонного аппарата, весила вместе с футляром около двух с половиной килограммов. Французы сразу же сделали заказ на 5000 машин. Позднее машина была существенно усовершенствована, ею заинтере­совались в США. В 1939 г. она была взята на вооружение ар­мии США. Под военным наименованием М-209 она использо­валась в качестве полевого шифра на протяжении всей вто­рой мировой войны. Всего было произведено около 140 000 таких машин. Позже фирма Хагелин стала производить широ­ко известные машины С-48, С-52, Т-55 и многие другие.



Среди заметных фигур в криптографии первой половины XX в. выделяется У. Фридман, получивший серьезные теоре­тические результаты в криптоанализе и ставший известным благодаря своим заслугам по вскрытию военных шифров Японии и Германии.

У.Фридман родился в 1891 г. в Кишиневе, в семье пере­водчика, работавшего в русском почтовом ведомстве. В 1892 г. его семья эмигрировала в США, где отец стал зани­маться швейными машинами. У.Фридман в 1914 г. Окончил Корнельский университет по специальности генетика. В городе Итака, где проживала семья Фридмана, крупный бизнесмен Д. Фабиан имел собственные лаборатории по акустике, гене­тике и криптографии. Любопытно, что криптографией Д. Фабиан увлекся, пытаясь доказать, что автором пьес У. Шекспира являлся Ф. Бэкон.

В 1915 г. Д. Фабиан нанял на работу в свое поместье Ривербэнк специалиста по генетике. Им стал У. Фридман. Вско­ре он увлекся криптографией и проявил себя в этом деле. Че­рез некоторое время У. Фридман уже возглавлял в Ривербэнкских лабораториях два отдела — генетики и шифров.

Помимо криптоаналитической работы У.Фридман занимался преподаванием в классе, состоявшем из армейских офицеров, присланных в Ривербэнк для изучения криптографии. До 1918 г. им был подготовлен цикл из семи лекций, восьмую он написал после возвращения со службы в качестве дешифровалыцика в американских экспедиционных силах (шла первая мировая война). Известные все вместе как Ривербэнкские публикации, эти работы являются серьезным вкла­дом в теоретическую криптографию.

Наибольший интерес с точки зрения современной криптографии представляют лекции "Методы раскрытия шифров с длинной связной гаммой" и "Индекс совпадения и его приме­нения в криптографии". В первой из них предлагается бесключевой метод чтения при использовании неравноверо­ятной гаммы. Во второй излагается так называемый к-тест, позволяющий выяснить, можно ли подписать друг под другом две (или более) криптограммы (или отрезки криптограмм) так, чтобы буквы в каждой колонке оказались бы зашифрованы одинаковыми знаками гаммы.

Поступив в 1921 г. на службу в войска связи, У. Фридман успешно применял свои методы для вскрытия машинных шифров. Когда была создана служба радиоразведки, У.Фридман стал ее главой и продолжил свои разработки, самой значимой из которых было вскрытие японской пурпурной шифрмашины. В 1929 г. он стал широко известен как один из ведущих криптографов мира, когда "Британская энциклопедия" поместила его статью "О кодах и шифрах". С основными результатами У. Фридмана можно познакомиться в четырехтомнике "Военная криптогра­фия".

Выдающиеся результаты в применении математических методов в криптографии принадлежат Клоду Шеннону. К. Шеннон получил образование по электронике и математике в Мичиганском университете, где и начал проявлять интерес к теории связи и теории шифров. В 1940 г. он получил степень доктора по математике, в течение года обучался в Принстонском институте усовершенствования, после чего был принят на службу в лабораторию компании "Bell Telephone".

К 1944 г. К. Шеннон завершил разработку теории секретной связи. В 1945 г. им был подготовлен секретный доклад "Матема­тическая теория криптографии", который был рассекречен в 1949 г. и издан.

В данной работе излагается теория так называемых секрет­ных систем, служащих фактически математической моделью шифров. Помимо основных алгебраических (или функциональ­ных) свойств шифров, постулируемых в модели, множества со­общений и ключей наделяются соответствующими априорными вероятностными свойствами, что позволяет формализовать мно­гие постановки задач синтеза и анализа шифров. Так, и сегодня при разработке новых классов шифров широко используется принцип Шеннона рассеивания и перемешивания, состоящий в использовании при шифровании многих итераций "рассеиваю­щих" и "перемешивающих" преобразований.

Разработанные К. Шенноном концепции теоретической и практической секретности (или стойкости) позволяют количе­ственно оценивать криптографические качества шифров и пы­таться строить в некотором смысле идеальные или совершенные шифры. Моделируется также и язык открытых сообщений. А именно, предлагается рассматривать язык как вероятностный процесс, который создает дискретную последовательность сим­волов в соответствии с некоторой вероятностной схемой.

Центральной в работах К. Шеннона является концепция из­быточной информации, содержащейся в текстовых сообщениях. Избыточность означает, что в сообщении содержится больше символов, чем в действительности требуется для передачи со­держащейся в нем информации. Например, всего лишь десять английских слов — the, of, and, to, a, in, that, it, is, i — состав­ляют более 25% любого (английского) текста. Легко понять, что их можно изъять из текста без потери информации, так как их легко восстановить по смыслу (или по контексту). Фактически К.Шеннон показал, что успех криптоанализа определяется тем, насколько избыточность, имеющаяся в сообщении, "переносит­ся" в шифрованный текст. Если шифрование "стирает" избыточ­ность, то восстановить текст сообщения по криптограмме стано­вится принципиально невозможно.

Задачу дешифрования К. Шеннон рассматривает как задачу вычисления апостериорных знаний противника о шифре после перехвата криптограммы. Дело в том, что вероятности сообще­ний и ключей составляют априорные знания противника, кото­рыми он располагает в соответствии с правилом Керкгоффса. После перехвата криптограммы он может (по крайней мере, в принципе, поскольку множества сообщений и ключей конечны) вычислить апостериорные вероятности возможных ключей и сообщений, которые могли быть использованы при составлении данной криптограммы. Вот эти вероятности и составляют апо­стериорные знания противника. С этой точки зрения показателен следующий пример.

Пусть для зашифрования нормативного английского языка применяется шифр простой замены, в котором каждый из 26! ключей может быть выбран с равной вероятностью. Пусть про­тивник знает об источнике сообщений лишь то, что он создает английский текст. Тогда априорными вероятностями различных сообщений из N букв являются их относительные частоты в нормативном тексте. Если же противник перехватил крипто грамму из N букв, то он может вычислить условные вероятно­сти открытых текстов и ключей, которые могут создать такую криптограмму. Если N достаточно велико, скажем N = 50, то обычно имеется единственное сообщение (и единственный ключ) с условной вероятностью, близкой к единице (это — само сообщение, подвергнутое шифрованию), в то время как все дру­гие сообщения имеют суммарную вероятность, близкую к нулю. Таким образом, имеется, по существу, единственное "решение" такой криптограммы. Для меньших значений N, скажем N = 10, обычно найдется несколько пар сообщений и ключей, вероятности которых сравнимы друг с другом, то есть, нет ни одного сообщения (и ключа) с вероятностью, близкой к единице. В этом случае "решение" криптограммы неоднозначно.

Понятие совершенной секретности К. Шеннон определяет требованием, чтобы апостериорные знания противника в точно­сти совпадали бы с априорными знаниями. Он приводит пример совершенного шифра, которым является шифр Вернама (со слу­чайной равновероятной гаммой). Следует подчеркнуть, что все рассуждения о стойкости шифров К. Шеннон проводит лишь для одной постановки задачи криптоанализа: когда противник располагает лишь одной криптограммой и требуется найти текст сообщения. Для других постановок задач требуются отдельные исследования.

Теоретической мерой секретности (или стойкости) по К.Шеннону является энтропийная характеристика — неопреде­ленность шифра по открытому сообщению, которая измеряет (в статистическом смысле), насколько "близка" средняя крип­тограмма из N букв к единственному "решению". Он выводит формулу для приближенного вычисления минимального N,при котором находится единственное "решение". Такая вели­чина получила название расстояния единственности. Форму­ла для расстояния единственности связывает между собой не­определенность шифра по открытому тексту и избыточность текста. Чем большим оказывается расстояние единственности, тем более шифр приближается к совершенному шифру, для которого формально расстояние единственности равно .



Наконец, К. Шеннон вводит понятие рабочей характери­стики шифра, подходя к практической оценке стойкости. Он формулирует также основные критерии оценки качества секрет­ных систем с позиций практики их использования.

Как видим, К. Шеннону удалось решить фундаментальные проблемы в теоретической криптографии. Его работы стимули­ровали бурный рост научных исследований по теории информа­ции и криптографии.

В работах К. Шеннона по исследованию свойств языка важ­ную роль играет величина удельной энтропии Н на букву тек­ста, другими словами, среднее количество информации, переда­ваемой буквой открытого текста. Предложенный им метод экс­периментов с угадыванием очередной буквы английского текста по предыдущим буквам оказался неэффективным при получе­нии оценок величины Н для других языков. Метод "отгадыва­ния" развил в своих работах А. Н. Колмогоров. Достаточно точ­ные приближения параметра Н для русского и французского языков получил Б. Б. Пиотровский. Он указал на существенную разницу между значениями Н для текстов различного характе­ра (литературных, деловых, разговорной речи).

Понятие "количества информации", содержащейся в тексте, базировалось, по К. Шеннону, лишь на частотных характеристи­ках. В своих фундаментальных работах 60-х годов А. Н. Колмо­горов подошел к определению количества информации с учетом смыслового содержания текста, что позволило уточнить при­ближение величины Н для литературных текстов. Необходимо также отметить, что еще задолго до К. Шеннона частотные ха­рактеристики языка изучал выдающийся русский ученый А. А. Марков. Сегодня часто используются так называемые марковские модели открытых текстов, учитывающие зависимости букв текста от предыдущих букв.

Следующая страница в истории криптографии XX в. посвя­щена телефонным шифраторам, которые были разработаны в 30-х годах и стали широко использоваться во время второй мировой войны. В России разработка телефонного шифратора велась под руководством В.А.Котельникова, ставшего впоследствии акаде­миком, ученым с мировым именем. Ему принадлежит знамени­тая теорема дискретизации (или теорема отсчетов), лежащая в основе теории цифровой обработки сигналов.

Согласно, идея телефонного шифратора была запа­тентована Д. Х. Роджерсом еще в 1881 г., спустя пять лет после изобретения Беллом телефона. Идея состояла в передаче теле­фонного сообщения по нескольким (в простейшем случае — по двум) цепям поочередными импульсами в некоторой быстро изменяющейся последовательности. Предлагалось разнести та­кие линии на значительное расстояние друг от друга с тем, что­бы устранить возможность подключения сразу ко всем одновре­менно. Подключение же к одной из них позволяло бы слышать лишь отдельные неразборчивые сигналы.

В более поздних разработках предлагались различные пре­образования непосредственно самой речи. Звуки речи преобра­зуются телефоном в непрерывный электрический сигнал, кото­рый с помощью соответствующих устройств изменяется шифра­тором по законам электричества. К числу возможных изменений относятся: инверсия, смещение, или деление диапазона частот, шумовые маскировки, временные перестановки частей сигнала, а также различные комбинации перечисленных преобразований. Естественно, каждое из указанных преобразований производит­ся под управлением ключа, который имеется у отправителя и получателя. Наиболее просто реализуемым являлось преобразо­вание инверсии. Сложнее реализовались временные перестанов­ки. Для их осуществления речевой сигнал в некоторый проме­жуток времени предварительно записывался на магнитофонной ленте. Запись делилась на отрезки длительностью в доли секунд. Отрезки с помощью нескольких магнитных головок разносились и перемешивались, в результате чего в канале слышалась хаоти­ческая последовательность звуков. Использовалась также дви­жущаяся магнитная головка, которая в зависимости от направления движения считывала сигналы быстрее или медленнее, чем они были записаны на ленте. В результате тон сигналов становился выше или ниже обычного, в канале быстро чередовались высокие и низкие звуки, не воспринимаемые ухом. Следует от­метить, что одной из самых сложных проблем, которые возника­ли при разработке телефонных шифраторов, была проблема узнавания восстановленной после расшифрования речи.

В США первый телефонный шифратор, под названием A3, был принят в эксплуатацию в 1937 г. Именно он доставил президенту Рузвельту известие о начале второй мировой войны утром 1 сентября 1939 г. по вызову американского посла в Па­риже. A3 осуществлял инверсию и перестановку 5 поддиапазонов частот. Из 3840 возможных комбинаций () фактически использовались лишь 6, которые менялись 36 раз за каждые 20 секунд. Слабость используемой криптографии компенсирова­лась регулярным изменением частот передачи.



В настоящее время аналоговая телефония уступает место цифровой телефонии. Тем самым и многие технические проблемы, связанные с криптографическими преобразованиями анало­говых сигналов, отпадают за ненадобностью. Дело в том, что оцифрованный сигнал является дискретным и, следовательно, к нему можно применить хорошо разработанную надежную "дис­кретную криптографию".

Во второй половине XX в., вслед за развитием элементной базы вычислительной техники, появились электронные шифраторы, разработка которых потребовала серьезных теоретиче­ских исследований во многих областях прикладной и фундамен­тальной математики, в первую очередь алгебре, теории вероят­ностей и математической статистике. Сегодня именно электрон­ные шифраторы составляют подавляющую долю средств шиф­рования. Они удовлетворяют все возрастающим требованиям по надежности и скорости шифрования. Прогресс в развитии вы­числительной техники сделал возможными программные реали­зации криптографических алгоритмов, которые все увереннее вытесняют во многих сферах традиционные аппаратные средства.

В семидесятых годах произошло два события, серьезно повлиявших на дальнейшее развитие криптографии. Во-первых, был принят (и опубликован!) первый стандарт шифрования данных (DES), "легализовавший" принцип Керкгоффса в криптографии. Во-вторых, после работы американ­ских математиков У. Диффи и М. Хеллмана родилась "новая криптография"— криптография с открытым клю­чом. Оба этих события были рождены потребностями бурно развивающихся средств коммуникаций, в том числе локаль­ных и глобальных компьютерных сетей, для защиты которых потребовались легко доступные и достаточно надежные крип­тографические средства. Криптография стала широко востребоваться не только в военной, дипломатической, государст­венной сферах, но также в коммерческой, банковской и дру­гих сферах.

Вслед за идеей Диффи и Хеллмана, связанной с гипотетическим понятием однонаправленной (или односторонней) функции с секретом, появились "кандидат" на такую функ­цию и реально осуществленная шифрсистема RSA с откры­тым ключом. Такая система была предложена в 1978 г. Райвестом, Шамиром и Адлеманом. Парадоксальным казалось то, что в RSA для зашифрования и расшифрования используются разные ключи, причем ключ зашифрования может быть от­крытым, то есть всем известным. Вслед за RSA появился целый ряд других систем. В связи с несимметричным исполь­зованием ключей стал использоваться термин асимметричная шифрсистема, в то время как традиционные шифрсистемы стали называться симметричными.

Наряду с идеей открытого шифрования Диффи и Хеллман предложили идею открытого распределения ключей, позво­ляющую избавиться от защищенного канала связи при рас­сылке криптографических ключей. Их идея основывалась на сложности решения задачи дискретного логарифмировании, то есть задачи, являющейся обратной для задачи возведения в степень в конечном поле большого порядка.

**Заключение.**

Появление в середине двадцатого столетия первых электронно-вычислительных машин кардинально изменило ситуацию в области шифрования (криптографии). С проникновением компьютеров в различные сферы жизни возникла принципиально новая отрасль - информационная индустрия.

В 60-х и частично в 70-х годах проблема защиты информации решалась достаточно эффективно применением в основном организационных мер. К ним относились прежде всего режимные мероприятия, охрана, сигнализация и простейшие программные средства защиты информации. Эффективность использования указанных средств достигалась за счет концентрации информации на вычислительных центрах, как правило автономных, что способствовало обеспечению защиты относительно малыми средствами. "Рассосредоточение" информации по местам ее хранения и обработки, чему в немалой степени способствовало появление в огромных количествах дешевых персональных компьютеров и построенных на их основе локальных и глобальных национальных и транснациональных сетей ЭВМ, использующих спутниковые каналы связи, создание высокоэффективных систем разведки и добычи информации, обострило ситуацию с защитой информации.

Проблема обеспечения необходимого уровня защиты информации оказалась (и это предметно подтверждено как теоретическими исследованиями, так и опытом практического решения) весьма сложной, требующей для своего решения не просто осуществления некоторой совокупности научных, научно-технических и организационных мероприятий и применения специфических средств и методов, а создания целостной системы организационных мероприятий и применения специфических средств и методов по защите информации.

Объем циркулирующей в обществе информации стабильно возрастает. Популярность всемирной сети Интренет в последние годы способствует удваиванию информации каждый год. Фактически, на пороге нового тысячелетия человечество создало информационную цивилизацию, в которой от успешной работы средств обработки информации зависит благополучие и даже выживание человечества в его нынешнем качестве. Произошедшие за этот период изменения можно охарактеризовать следующим образом: объемы обрабатываемой информации возросли за полвека на несколько порядков; доступ к определенным данным позволяет контролировать значительные материальные и финансовые ценности; информация приобрела стоимость, которую даже можно подсчитать; характер обрабатываемых данных стал чрезвычайно многообразным и более не сводится к исключительно текстовым данным; информация полностью "обезличилась", т.е. особенности ее материального

представления потеряли свое значение - сравните письмо прошлого века и современное послание по электронной почте; характер информационных взаимодействий чрезвычайно усложнился, и наряду с классической задачей защиты передаваемых текстовых сообщений от несанкционированного прочтения и искажения возникли новые задачи сферы защиты информации, ранее стоявшие и решавшиеся в рамках используемых "бумажных" технологий - например, подпись под электронным документом и вручение электронного документа "под расписку"; субъектами информационных процессов теперь являются не только люди, но и созданные ими автоматические системы, действующие по заложенной в них программе; вычислительные "способности" современных компьютеров подняли на совершенно новый уровень как возможности по реализации шифров, ранее немыслимых из-за своей высокой сложности, так и возможности аналитиков по их взлому.

Перечисленные выше изменения привели к тому, что очень быстро после распространения компьютеров в деловой сфере практическая криптография сделала в своем развитии огромный скачок, причем сразу по нескольким направлениям: во-первых, были разработаны стойкие блочные с секретным ключом, предназначенные для решения классической задачи - обеспечения секретности и целостности, передаваемых или хранимых данных, они до сих пор остаются "рабочей лошадкой" криптографии, наиболее часто используемыми средствами

**Примечания.**

1. Во многих приложениях задача идентификации и аутентификации доступа человека или программы к некоторому ресурсу является даже более важной, чем задача обеспечения конфиденциальности. Практически все многопользовательские и сетевые операционные системы требуют аутентификации пользователя. Равно как банкоматы и кассовые терминалы. С развитием интернета и безбумажных технологий число приложений, которые требуют аутентификации пользователей, будет только возрастать.

Итак, сначала – определения. В дальнейшем под субъектом будем понимать пользователя или пользовательского агента(программу), осуществляющего доступ к некоторому ресурсу. Под информационной системой будем понимать отдельный компьютер или компьютерную сеть, или иное электронное устройство, доступ к которому регламентируется определенной системой полномочий и/или прав. Задачей систем идентификации и аутентификации является определение и верификация набора полномочий субъекта при доступе к информационной системе. Идентификацией субъекта при доступе к информационной системе называется процесс сопоставления его с некоторой хранимой системой характеристикой субъекта – идентификатором. В дальнейшем идентификатор субъекта используется для предоставления субъекту определенного уровня прав и полномочий при использовании информационной системой. Аутентификацией субъекта называется процедура верификации принадлежности идентификатора субъекту. Аутентификация производится на основании того или иного секретного элемента (аутентификатора), которым располагают как субъект, так и информационная система. Обычно информационная система располагает не самим секретным элементом, но некоторой информацией о нем, на основании которой принимается решение об адекватности субъекта идентификатору.

Для того, чтобы эта сухая теория стала более понятной, рассмотрим конкретный пример. Перед началом интерактивного сеанса работы большинство операционных систем запрашивают у пользователя его имя и пароль. Введенное имя является идентификатором пользователя, а его пароль – аутентификатором. Операционная система обычно хранит не сам пароль, а его хэш сумму, обеспечивая тем самым практическую невозможность восстановления пароля. Использование пары «имя пользователя пароль» для аутентификации субъектов является наиболее распространенным, но не единственным. Принципиально разных методов аутентификации на самом деле немного. Один класс методов аутентификации основывается на том, что аутентифицируемый субъект должен иметь некоторый секретный элемент(пароль, секретный ключ или специальный аутентификационный токен). Другой класс методов аутентификации применим, в основном, для аутентификации людей. Он основывается на наличии уникальных физических свойств самого человека (отпечатки пальцев, форма кисти руки, голос, радужная оболочка глаза). У каждого класса методов есть как достоинства,так и недостатки. Сравнением обоих классов методов мы займемся чуть позже, а пока рассмотрим подробнее разные методы аутентификации.

Алгоритмически процедура аутентификации представляется как последовательная передача одной или нескольких информационных посылок между субъектом и информационной системой и промежуточная их обработка обеими сторонами. В результате этих действий обе стороны обмена должны удостоверить, что они являются теми, за кого себя выдают. Про аутентификацию секретным элементом мы уже говорили. Другим распространенным методом аутентификации является аутентификация с использованием сертификатов открытого ключа. Разработано и применяется несколько таких алгоритмов. Обычно аутентификацию с использованием ключей совмещают с процедурой генерации парного симметричного ключа с целью его дальнейшего использования для обмена сообщениями. Наиболее известной процедурой взаимной аутентификации пары абонентов является метод Диффи Хеллмана. Он широко описан как в статьях самих авторов, так и в независимых работах. Суть метода состоит в том, что каждый из участников обмена путем математических преобразований своего секретного ключа и открытого ключа своего корреспондента и обмена несекретными посылками получают независимо друг от друга секретное число. Поскольку секретный и открытый ключи абонентов связаны некоторым соотношением, то есть возможность подбора преобразований ключей так, что полученные обоими абонентами числа совпадают. Полученное секретное число можно использовать в качестве разделяемого секрета.

Другим интересным методом аутентификации является использование аутентификационного токена. Аутентификационный токен представляет собой физическое устройство, обычно небольших размеров для удобства его ношения с собой. Это может быть смарт карта или недавно появившиеся устройства, подключаемые к порту USB и выполненные в виде брелока. Обычно аутентификационный токен содержит «на борту» энергонезависимую память и специализированный процессор. Некоторые устройства дополнительно имеют встроенный аппаратный генератор случайных чисел или таймер(часы реального времени). Процессор токена в зависимости от мощности способен выполнять самые различные операции. Есть процессоры, способные выполнять шифрование данных алгоритмом DES или вычислять хэш суммы c использованием ключа (HMACMD5). Специализированный токен позволяет производить криптографические преобразования без извлечения ключа из памяти токена и передавать между токеном, компьютером и информационной системой только несекретные или зашифрованные данные, что дополнительно защищает протокол аутентификации от перехвата ключей. Обычно программный доступ к токену возможен только после ввода PIN кода, известного только владельцу аутентификационного токена. Дополнительные возможности токенов позволяют реализовать более надежные протоколы аутентификации. Интересную технологию аутентификации, основанную на «одноразовых паролях», предложила компания Security Dynamics. Технология носит название SecureID. Одноразовыми паролями являются псевдослучайные числа. Генератором последовательности псевдослучайных чисел является аутентификационный токен. RSA Security предлагает несколько вариантов токена – смарт-карту, калькулятор с возможностью ввода PIN кода, брелоки. Каждый токен имеет уникальный серийный номер. Токен генерирует новое псевдослучайное число по одному в минуту. Период генератора псевдослучайных чисел таков, что время использования одного токена составляет два года. Для аутентификации по технологии SecureID информационная система должна содержать в себе аутентификационный сервер SecureID и базу данных, сопоставляющую имена аутентифицируемых пользователей и серийные номера токенов. Запрос на аутентификацию от пользователя состоит из его имени и случайного числа, считываемого пользователем с токена. Сервер, на основании полученного от пользователя числа и серийного номера токена, решает принадлежит ли данное число последовательности, генерируемой именно этим токеном, или нет.

Указанные и многие другие методы аутентификации страдают одним недостатком – они, на самом деле, аутентифицируют не конкретного субъекта, а фиксируют тот факт, что аутентификатор субъекта соответствует его идентификатору. То есть, все перечисленные методы незащищены от компрометации аутентификатора. Биометрические методы идентификации или аутентификации свободны от этого недостатка. Как уже отмечалось, биометрические методы основываются на анализе уникальных характеристик самого человека. Биометрическая характеристика может являться как идентификатором (как, собственно, дактилоскопия рассматривает отпечаток пальца, как идентификатор личности), так и аутентификатором (пользователь вводит свое имя и подтверждает его, посмотрев в окуляр анализатора радужной оболочки глаза). Для некоторых приложений(например, для контроля доступа в помещения) идентификации оказывается достаточно. Для некоторых(«параноидальных») случаев требуется ввести имя пользователя, его отпечаток пальца да еще и произнести кодовую фразу.  
Наиболее распространенным методом (и дешевым) биометрической идентификации или аутентификации является анализ отпечатка пальца. При регистрации пользователя в базу данных аутентификационного сервера помещается свертка – некоторая хэш сумма отсканированного отпечатка пальца. В зависимости от реализации, длина свертки составляет 200–400 байт. Но у биометрических методов аутентификации личности есть один серьезный недостаток (кроме относительно высокой стоимости). В случае компрометации аутентификационного токена, ключа или пароля субъект может отказаться от его использования и получить новый аутентификатор. В случае компрометации электронного представления биометрического аутентификатора, человек может просто «выпасть» из процесса аутентификации. В случае использования биометрической характеристики как идентификатора личности, угрозы компрометации нет.

2 Можно ли, используя криптографические технологии, обеспечить подлинность бумажного документа (завещания, доверенности или иного юридического документа)? Традиционным подходом является составление юридического документа на бумаге с водяными знаками или иными защитными элементами. Такой подход требует наличия специального бланка на момент составления документа или наличия типографии со специальным оборудованием. А что делать когда уже есть бумажный документ и есть желание защитить его от подделки? Известно, что каждый лист бумаги уникален по структуре образующих его волокон. С появлением недорогих сканеров, имеющих высокое разрешение, и надежных технологий распознавания образов, появилась возможность анализировать микроструктуру бумаги и использовать полученную информацию для обеспечения уникальности документа.

На сегодняшний день уже имеется проработанная технология, доведенная до программно-аппаратного решения, обеспечивающая уникальность бумажных документов, использующая вышеизложенную идею. Выбранный документ сканируется с высоким разрешением, и в отсканированном образе выделяются несколько особенностей (микро вкрапления, характерные изгибы образующих волокон, и т.д.). В общем, тут напрашивается некоторая аналогия с технологией анализа отпечатков пальцев... И, кстати, не случайно. Полученные данные преобразуются в двоичный массив, для которого вычисляется хэш функция. Полученное значение хэш функции и является аналогом «водяного знака» и обеспечивает уникальность документа. Легко заметить, что предложенную технологию легко расширить и значение хэш функции печатать прямо на бланке документа вместе с печатью нотариуса при нотариальном заверении документа. Но такой подход требует соответствующего законодательства. Попытки использовать «электронные водяные знаки» для небумажных носителей пока, к сожалению, не имели успеха. Самым известным примером может служить попытка защиты DVD дисков от нелегального распространения. Идея разработчиков состояла в том, чтобы помимо шифрования информации на диске помещать на него некоторую информацию, которая терялась или переставала быть актуальной на копии. Практика показала, что попытки внедрить подобную технологию оказались неудачными.   
  
Приведенный пример, кстати, отражает глубокое и, к сожалению, часто не замечаемое различие традиционных документов и электронных. Суть этой разницы хорошо видна на примере применения электронной подписи. Программа проверки подписи, вообще говоря, может установить лишь то, что проверяемый документ был подписан с использованием ключа, имеющего указанный идентификатор и подпись верна (либо – не верна). Но по подписи нельзя определить кто же именно воспользовался данным ключом. Пусть, например, для вычисления «контрольной суммы» легального DVD диска использовались такие его характеристики, как материал покрытия, данные, нанесенные штрих кодом, код завода изготовителя и серийный номер диска. Обладание алгоритмом вычисления такой «контрольной суммы» позволит потенциальным «пиратам» изготовить неограниченное число копий просто перевычисляя «контрольную сумму» в процессе изготовления для тех «болванок», которые имеются в их распоряжении. Любой DVD проигрыватель воспримет так изготовленный диск как легальный!

1. Криптографическими методами можно обеспечить не только конфиденциальность, но и проконтролировать целостность передаваемых или хранимых данных. Контроль целостности в основном производится путем расчета некоторой «контрольной суммы» данных. Математиками и инженерами, работающими в области передачи данных и теории кодирования, разработано множество алгоритмов, рассчитывающих контрольные суммы передаваемых данных. Для многих приложений простой контрольной суммы (например, известного алгоритма crc32 или последовательного побайтного или пословного сложения исходного текста с известной константой) оказывается достаточно, особенно тогда, когда важна скорость обработки данных и не известен заранее объем данных (типичный случай – передача данных по каналам связи).   
   Проблема простых алгоритмов вычисления контрольной суммы в том, что достаточно легко подобрать несколько массивов данных, имеющих одинаковую контрольную сумму. Криптографически стойкие контрольные суммы вычисляются как результат применения к исходному тексту так называемой хэш функции.   
    Одним из результатов теории сложности и теории функций является гипотеза о существовании односторонних функций. Под односторонней функцией понимается функция, определенная (например) на множестве натуральных чисел и не требующая для вычисления своего значения больших вычислительных ресурсов. Но вычисление обратной функции(то есть, по известному значению функции восстановить значение аргумента) оказывается невозможно теоретически или (в крайнем случае) невозможно вычислительно. Строгое существование односторонних функций пока не доказано. Поэтому все используемые в настоящее время хэш функции являются лишь «кандидатами» в односторонние функции, хотя и имеют достаточно хорошие свойства. Основными свойствами криптографически «хорошей» хэш функции является свойство рассеивания, свойство стойкости к коллизиям и свойство необратимости. О необратимости мы уже говорили. Коллизией хэш функции H называется ситуация, при которой существуют два различных текста T1 и T2, но H(T1) = H(T2). Значение хэш функции всегда имеет фиксированную длину, а на длину исходного текста не накладывается никаких ограничений. Из этого следует, что коллизии существуют. Требование стойкости к коллизиям обозначает, что для криптографически «хорошей» хэш функции для заданного текста T1 вычислительно невозможно найти текст T2, вызывающий коллизию. Свойство рассеивания требует, чтобы минимальные изменения текста, подлежащего хэшированию, вызывали максимальные изменения в значении хэш функции.   
    Основные применяемые на сегодняшний день алгоритмы, реализующие хэш функции, являются MD2, MD4, MD5, SHA и его вариант SHA1, российский алгоритм, описываемый стандартом ГОСТ Р 34.11 94. Наиболее часто используются MD5, SHA1 и в России 34.11. Длина значения хэш функции различна. Типичной длиной является 16–32 байта. В свете последних криптоаналитических результатов, вероятно, придется в недалеком будущем отказаться от MD5, так как было заявлено: «его стойкость к коллизиям опустилась и, вероятно, подошла близко к той отметке, после которой о стойкости вообще говорить не приходится». В заголовок раздела вынесены слова «электронная подпись». Но не сказать об электронной подписи совсем было бы неправильно. Дело в том, что без несимметричной криптографии электронной подписи не было бы вообще! Идея электронной подписи проста. Когда описывался процесс шифрования с использованием несимметричного алгоритма, то отмечалось, что для зашифрования сообщения использовался открытый ключ, а для расшифрования – секретный. Но в применении к шифрованию ключи взаимозаменяемы. Можно зашифровать сообщение на своем секретном ключе, и тогда любой желающий сможет его расшифровать, используя открытый ключ. Это свойство несимметричных алгоритмов и используетсяпри формировании и проверке электронно-цифровой подписи. Собственно ЭЦП документа – это его хэш сумма, зашифрованная секретным ключом. Проверка ЭЦП документа сводится к вычислению хэш суммы документа, расшифрованию хэш суммы, содержащейся в подписи, и сравнению двух величин. Если значения вычисленной и сохраненной в подписи хэш сумм совпали, то считается, что подпись под документом верна.
2. Гай Юлий Цезарь.

5. Полибий; Polybios, из Мегалополя в Аркадии, ок. 200-ок. 118 гг. до н. э., греческий историк. Сын Ликорта, влиятельного политика и главы Ахейского союза, с юности принимал участие в военной и политической жизни. В 169 г. во время III Македонской войны стал гиппархом (предводителем конницы). Ездил с посольством к консулу Манлию. После победы под Пидной (168 г. до н. э.) римляне захватили 1000 заложников из самых знатных ахейских семей, в числе которых был и Полибий. В Риме он подружился с сыновьями Эмилия Паула, победителя под Пидной, а в особенности со Сципионом Младшим. Освобожденный вместе с другими заложниками, в 151 г. возвратился на родину, совершал многочисленные путешествия, часто приезжал в Рим по приглашению Сципиона, который использовал его познания в военном деле. В 146 г. до н. э. стал свидетелем взятия Карфагена. В том же году после взятия римлянами Коринфа и его разрушения Полибий. принял на себя посредническую роль в урегулировании отношений в покоренной Греции. По-видимому, Полибий. участвовал и в осаде Нуманция Сципионом в 133 г. до н. э. Последние годы жизни Полибий. провел на родине, умер в возрасте 82 лет, вероятно, вследствие падения с лошади. - Главное произведение Полибия. - История в 40 книгах - является всемирной историей, в которой автиор показал, как в течение 50 лет, от начала II Пунической войны до конца III Македонской, Рим объединил под своей властью почти весь населенный мир того времени.

Полибий, грек, был первым историком, открывшим величие Рима как грекам, так и самим римлянам. Причины побед римлян Полибий видел в тактическом совершенстве легиона, а также в смешанном государственном устройстве Рима, соединившим в себе элементы монархии, аристократии и демократии. Чтобы прояснить картину, Полибий описал во вступлении события I Пунической войны, а в процессе написания последующих частей произведения расширил первоначальный план описания взятия и разрушения Карфагена и Коринфа. Таким образом, произведение охватывало период 264-144 гг. до н. э. От Истории Полибия сохранилось 5 начальных книг, остальные мы имеем в выдержках, известнейшей из которых представляется выдержка из книги VI (отступление о государстве, формах правления, сравнение общественного строя Рима с политической структурой греческих государств и Карфагена). Полибий описывал события хронологически, по олимпиадам, подражая в этом Тимею. В отношении современных ему фактов Полибий (в соответствии с традициями греческой историографии) полагался прежде всего на собственную память и на сообщения очевидцев, зато для реконструкции событий прошлого использовал работы своих предшественников, интерпретируя их в свете собственного знания. Порой он обращался и к оригинальным документам, как, например, постановления римского сената, торговые договоры, документы из греческих архивов. Своих предшественников, а особенно Тимея, Полибий резко критиковал, при случае излагая собственный исторический метод. С одной стороны, он выступал против чрезмерной драматизации описываемых событий, которая обычно приводила к искажению истины ради эффекта. Историков этого направления, представителем которого был Филарх, П. обвиняет в том, что они выступают в большей степени трагическими поэтами, чем историками. А с другой стороны, полемизируя с Тимеем, доказывает, что историку недостаточно знакомиться с описываемыми событиями лишь по книгам. Он должен знать по личным впечатлениям страну, о которой пишет, и прежде всего - места важнейших сражений. Также он сам должен быть военным и политиком, чтобы его произведение могли с пользой для себя читать вожди и государственные деятели. В этой концепции, исходящей от Фукидида, Полибий провозглашал принцип беспристрастности историка, однако, сам ему не следовал ни в отношении современников, ни в отношении предшественников. Порой он исполнен гнева, ненависти, разочарования, в другом же месте - восхищения. Он идеализирует свою родину и Ахейский Союз. Полибий не стремился к красочности повествования. Его стиль шероховатый и жесткий. Но иногда он становится очень живым, а некоторые сцены, как, например, объявление Птолемея V царем и связанные с этим события в Александрии, написаны ярко и интересно. Другие произведения Полибия: Филопомен в 3 книгах - хвала предводителю Ахейского Союза, написанная после 183 г., а также не сохранившееся произведения, посвященное тактике, и монография о Нумантинской войне. К Истории Полибий неоднократно обращался Ливий, местами просто переводя ее. Из греческих историков дело Полибия продолжили Посидоний и Страбон, его использовали Диодор и Плутарх. В византийскую эпоху вышел пересказ произведения

6. Альберти Леон Батиста - итальянский архитектор и литератор, один из наиболее ярких представителей культуры Возрождения. Обладал обширными познаниями в самых разных областях: был философом и музыкантом, скульптором и математиком, физиком и лингвистом. На протяжении ряда лет он - итальянский ученый, архитектор, теоретик искусства эпохи Раннего Возрождения. Теоретические трактаты («О статуе», 1435, «О живописи», 1435-36, «О зодчестве»; опубликован в 1485) обобщили опыт современного ему искусства и гуманистической науки в области изучения античного наследия. В архитектуре использовал античную ордерную систему (церковь Сант-Андреа в Мантуе, 1472-94, дворец Ручеллаи во Флоренции, 1446-51). В молодости написал на латыни комедию "Любитель славы" (около 1424). Исследованию природы власти посвящен его сатирический роман (тоже на латыни) "Мом" (между 1443 и 1450). Он выступал горячим защитником литературного "народного" языка и основные его сочинения написаны по-итальянски. Это сонеты, элегии и эклоги. Наиболее известная работа - трактат в 4-х книгах "О семье" (1433-1441). Огромное значение имел знаменитый латинский трактат в 10-ти книгах "О зодчестве" (1450). Один из основополжников проективной геометрии.

1. **Чарлз Уитстон** (Wheatstone) (6.2.1802, Глостер, Англия, - 19.10.1875, Париж), английский физик и изобретатель, член Лондонского королевского общества (1836). Занимаясь изготовлением музыкальных инструментов, поставил ряд остроумных акустических опытов. В 1833 году объяснил возникновение фигур Хладни. С 1834 года профессор Королевского колледжа (Лондон). Предложил метод измерения продолжительности разрядной искры (1834); показал, что искровые спектры металлов однозначно характеризуют эти металлы (1835). В 1837 году вместе с У. Ф. Куком получил патент на изобретение электромагнитного телеграфа; в 1858 году создал первый практически пригодный автоматический телеграфный аппарат (телеграфный аппарат Уитстона). В 1867 году независимо от Э. В. Сименса открыл принцип самовозбуждения электрических машин. Сконструировал зеркальный стереоскоп, фотометр, шифровальный аппарат - криптограф, самопишущие метеорологические приборы и др. Предложил мостовой метод измерения сопротивлений.
2. Томас Джефферсон.

9. Клод Элвуд Шеннон (Shannon)(1916 — 2001) — американский инженер и математик. Человек, которого называют отцом современных теорий информации и связи. Осенним днем 1989 года корреспондент журнала "Scientific American" вошел в старинный дом свидом на озеро к северу от Бостона. Но встретивший его хозяин, 73-летнийстройный старик с пышной седой гривой и озорной улыбкой, совсем не желалвспоминать "дела давно минувших дней" и обсуждать свои научные открытия 30-50-летней давности. Быть может, гость лучше посмотрит его игрушки? Не дожидаясь ответа и неслушая увещеваний жены Бетти, хозяин увлек изумленного журналиста в соседнюю юкомнату, где с гордостью 10-летнего мальчишки продемонстрировал свои сокровища: семь шахматных машин, цирковой шест с пружиной и бензиновым двигателем, складной нож с сотней лезвий, двухместный одноколесный велосипед, жонглирующий манекен, а также компьютер, вычисляющий в римской системе счисления. И не беда, что многие из этих творений хозяина давно сломаны и порядком запылены, — он счастлив. Кто этот старик? Неужели это он, будучи еще молодым инженером Bell Laboratories, написал в 1948 году"Великую хартию" информационной эры — "Математическую теорию связи"? Его ли труд назвали "величайшей работой в анналах технической мысли"? Его ли интуицию первооткрывателя сравнивали с гением Эйнштейна? Да, это все о нем. И он же в тех же 40-х годах конструировал летающий диск на ракетном двигателе и катался, одновременно жонглируя, на одноколесном велосипеде по коридорам Bell Labs. Это Клод Элвуд Шеннон, отец кибернетики и теории информации, гордо заявивший: "Я всегда следовал своим интересам, недумая ни о том, во что они мне обойдутся, ни об их ценности для мира. Я по тратил уйму времени на совершенно бесполезные вещи."Клод Шеннон родился в 1916году и вырос в городе Гэйлорде штата Мичиган. Еще в детские годы Клод познакомился как с детальностью технических конструкций, так и с общностью математических принципов. Он постоянно возился с детекторными приемниками и радио-конструкторами, которые приносил ему отец, помощник судьи, и решал математические задачки и головоломки, которыми снабжала его старшая сестра Кэтрин, ставшая впоследствии профессором математики. Клод полюбил эти два мира, столь несхожие между собой, — технику и математику. Будучи студентом Мичиганского университета, который он окончил в 1936 году, Клод специализировался одновременно и в математике, и в электротехнике. Эта двусторонность интересов и образования определила первый крупный успех, которого Клод Шеннон достиг в свои аспирантские годы в Массачусетском технологическом институте. В своей диссертации, защищенной в 1940 году, он доказал, что работу переключателей и реле в электрических схемах можно представить посредством алгебры, изобретенной в середине XIX века английским математиком Джорджем Булем. "Просто случилось так, что никто другой не был знаком с этими обеими областями одновременно!" — так скромно Шеннон объяснил причину своего открытия. В наши дни совершенно излишне объяснять читателям компьютерного издания, что значит булева алгебра для современной схемотехники. В 1941 году 25-летний Клод Шеннон поступил на работу в Bell Laboratories. В годы войны он занимался разработкой криптографических систем, и позже это помогло ему открыть методы кодирования с коррекцией ошибок. А в свободное время он начал развивать идеи, которые потом вылились в теорию информации. Исходная цель Шеннона заключалась в улучшении передачи информации по телеграфному или телефонному каналу, находящемуся под воздействием электрических шумов. Он быстро пришел к выводу, что наилучшее решение проблемы заключается в более эффективной упаковке информации. Но что же такое информация? Чем измерять ее количество? Шеннону пришлось ответить на эти вопросы еще до того, как он приступил к исследованиям пропускной способности каналов связи. В своих работах 1948-49 годов он определил количество информации через энтропию —величину, известную в термодинамике и статистической физике как мера разупорядоченности системы, а за единицу информации принял то, что впоследствии окрестили"битом", то есть выбор одного из двух равновероятных вариантов. Позже Шеннон любил рассказывать, что использовать энтропию ему посоветовал знаменитый математик Джон фон Нейман, который мотивировал свой совет тем, что мало кто из математиков и инженеров знает об энтропии, и это обеспечит Шеннону большое преимущество в неизбежных спорах. Шутка это или нет, но как трудно нам теперь представить, что всего полвека назад понятие "количество информации"еще нуждалось в строгом определении и что это определение могло вызвать какие-то споры. На прочном фундаменте своего определения количества информации Клод Шеннон доказал удивительную теорему о пропускной способности зашумленных каналов связи. Во всей полноте эта теорема была опубликована в его работах 1957-61 годов и теперь носит его имя. В чем суть теоремы Шеннона? Всякий зашумленный канал связи характеризуется своей предельной скоростью передачи информации, называемой пределом Шеннона. При скоростях передачи выше этого предела неизбежны ошибки в передаваемой информации. Зато снизу к этому пределу можно подойти сколь угодно близко, обеспечивая соответствующим кодированием информации сколь угодно малую вероятность ошибки при любой зашумленности канала. Эти идеи Шеннона оказались слишком провидческими и не смогли найти себе применения в годы медленной ламповой электроники. Но в наше время высокоскоростных микросхем они работают повсюду, где хранится, обрабатывается и передается информация: в компьютере и лазерном диске, в факсимильном аппарате и межпланетной станции. Мы не замечаем теорему Шеннона, как не замечаем воздух. Кроме теории информации, неуемный Шеннон приложился во многих областях. Одним из первых он высказал мысль о том, что машины могут играть в игры и самообучаться. В 1950 году он сделал механическую мышку Тесей, дистанционно управляемую сложной электронной схемой. Эта мышка училась находить выход из лабиринта. В честь его изобретения IEEE учредил международный конкурс "микромышь", в котором до сих пор принимают участие тысячи студентов технических вузов. В те же 50-е годы Шеннон создал машину, которая "читала мысли" при игре в "монетку":человек загадывал "орел" или "решку", а машина отгадывала с вероятностью выше 50%, потому что человек никак не может избежать каких-либо закономерностей, которые машина может использовать. В 1956 году Шеннон покинул Bell Labs и со следующего года стал профессором Массачусетского технологического института, откуда ушел на пенсию в 1978 году. В числе его студентов был, в частности, Марвин Мински и другие известные ученые, работавшие в области искусственного интеллекта. Труды Шеннона, к которым с благоговением относятся деятели науки, столь же интересны и для специалистов, решающих сугубо прикладные задачи. Шеннон заложил основание и для современного кодирования с коррекцией ошибок, без которого не обходится сейчас ни один дисковод для жестких дисков или система потокового видео, и, возможно, многие продукты, которым еще только предстоит увидеть свет. В МТИ и на пенсии им полностью завладело его давнее увлечение жонглированием. Шеннон построил несколько жонглирующих машин и даже создал общую теорию жонглирования, которая, впрочем, не помогла ему побить личный рекорд — жонглирование четырьмя мячиками. Еще он испытал свои силы в поэзии, а также разработал разнообразные модели биржи акций и опробовал их (по его словам — успешно) на собственных акциях. Но с начала 60-х годов Шеннон не сделал в теории информации практически больше ничего. Это выглядело так, как будто ему всего за 20 лет надоела созданная им же теория. Такое явление — не редкость в мире науки, и в этом случае об ученом говорят одно слово: перегорел. Как лампочка, что ли? Мне кажется, более точным было бы сравнение ученых со звездами. Самые мощные звезды светят не долго, около ста миллионов лет, и кончают свою творческую жизнь вспышкой сверхновой, в процессе которой происходит нуклеосинтез: из водорода и гелия рождается вся таблица Менделеева. Мы с вами состоим из пепла этих звезд, и так же наша цивилизация состоит из продуктов быстрого сгорания самых мощных умов. Есть звезды второго типа: они горят ровно и долго и миллиарды лет дарят свет и тепло населенным планетам (по крайней мере, одной). Исследователи такого типа тоже очень нужны науке и человечеству: они сообщают цивилизации энергию развития. А звезды третьего сорта — красные и коричневые карлики — светят и греют чуть-чуть, лишь себе под нос. Таких ученых хватает, но в статье о Шенноне говорить о них просто неприлично. В 1985 году Клод Шеннон и его жена Бетти неожиданно посетили Международный симпозиум по теории информации в английском городе Брайтоне. Почти целое поколение Шеннон не появлялся на конференциях, и поначалу его никто не узнал. Затем участники симпозиума начали перешептываться: вон тот скромный седой джентльмен — это Клод Элвуд Шеннон, тот самый! На банкете Шеннон сказал несколько слов, немного пожонглировал тремя (увы, только тремя) мячиками, а затем подписал сотни автографов ошеломленным инженерам и ученым, выстроившимся в длиннейшую очередь. Стоящие в очередиговорили, что испытывают такие же чувства, какие испытали бы физики, явись на их конференцию сам сэр Исаак Ньютон. Клод Шеннон скончался в2001 году в массачусетском доме для престарелых от болезни Альцгеймера на 84году жизни.

10 Эней.

Список литературы.

1. А. П. Алфёров, А. Ю. Зубов, А. С. Кузьмин, А. В. Черёмушкин «Основы

криптографии».

2. С. Г. Баричев, Р. Е. Серов «Основы современной криптографии».

3. Владимир Жельников «Криптография от папируса до компьютера».

4. http://acoder.org/

5. http://www.uran.donetsk.ua/~masters/2005/feht/chernenkaya/ind/history.html

6. http://borlpasc.narod.ru/inzik/glava6/kratkay.htm

7. www.ssl.stu.neva.ru/psw/

8. http://persona.rin.ru/cgi-bin/rus/view.pl?id=31397&a=f&idr=3

9. http://www.tonnel.ru/?l=kniga&273

10. http://www.c-cafe.ru/days/bio/5/085.php

11. http://www.eduref.ru/f68a9-79c5e.html