Владимир Жельников

КРИПТОГРАФИЯ ОТ ПАПИРУСА ДО КОМПЬЮТРА

Отдел Исследования Программ
http://dore.on.ru

СОДЕРЖАНИЕ

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».

Решительно нет никакой возможности понять пути развития человеческого общества в отрыве от его жгучего стремления к тайнам. Политики и военные, священники и торговцы, писатели и ученые, шарлатаны и аферисты тысячелетиями развивали науку о секретах, доводя их создание до совершенства, служили тайнам, насыщали свои потребности в них. Без тайн не может быть не только государства, но даже малой общности людей - без них нельзя выиграть сражение или выгодно. продать товар, одолеть своих политических противников в жестокой борьбе за власть или сохранить первенство в технологии. Тайны составляют основу науки, техники и политики любой человеческой формации, являясь цементом государственности.

История хранит так много секретов, что просто удивительно, до чего людям они необходимы. Служба безопасности пытается делить их на ряд уровней: от для служебного пользования до совершенно секретно и сугубо доверительно. Американский физик Ричард Фейнман шутил, что при работе над созданием атомной бомбы ему наряду с документами, имеющими пометку ingest after reading, то есть буквально съесть после прочтения, попадались иногда бумаги и со штампом уничтожить до прочтения. Сколь ни высоконаучна теория, лежащая в основе такой классификации, она сводится к заурядной дискриминации групп людей, нарушая их естественные права. Если финансовые хищения юридически можно делить на мелкие и крупные, то степень секретности классифицировать абсурдно. Доклад Хрущева на XX съезде партии о культе личности Сталина представлялся секретным лишь для партаппарата, но не для большинства обывателей, прекрасно знавших положение в обществе.

Секрет для каждого конкретного человека либо есть, либо его нет. Более того, вскрытие тайны аналитически не только не составляет преступления, а являет торжество человеческого разума и должно приветствоваться, если делается открыто, из лучших побуждений. Французы говорят: «Удел богов - создавать тайны, а королей - раскрывать». Действительно, покажите специалистам лишь один узел сложного устройства, и они реконструируют полный его вид, назначение и характеристики. Если биолога спросить, чем питаются черти, то ответ будет однозначным: «Рога и копыта - явные признаки травоядных!»

Эта книга познакомит читателей с одним из величайших видов тайн — наукой о шифрах или криптологией. Изобретенная тысячелетия назад письменность обладает свойством вседоступности, которое, в зависимости от получателя сообщения, можно рассматривать как полезное, или как вредное. Мы обычно рады получить письмо от знакомых, но бываем не в восторге, заметив, что конверт вскрыт и с его содержимым кто-то ознакомился. Потому параллельно письменности, развивается секретное письмо, или по-гречески криптография. Она предназначена спрятать смысл письма от просто грамотных людей и сделать его доступным лишь определенным адресатам. Поскольку компьютер революционно расширил в последние годы сферу письменности, то почти одновременно возникла потребность столь же большого развития криптографии. Насколько актуально ее использование сейчас - судите сами.

От кого же придется защищать свои данные? Пословица гласит: "От своего вора не убережешься". Если верить газетным публикациям, то российская внешняя разведка готова отечественным структурам продавать технологические секреты, выве-

данные за рубежом. На практике это может выглядеть таким образом. Россиянин ведет свое дело в США, а наша разведка, выкрав там его секреты, продаст их в России совместной с американцами фирме. Теория честного жулика, который в своем доме не ворует, в данном случае порочна. Наши разведчики и их шпионы мирно договариваются, какими секретами, похищенными в своих странах, они согласны обменяться и как поделить вырученные от этого деньги. Стремление государственных секретных служб ввести свои правила шифрования частных и коммерческих данных означает ни что иное, как желание Старшего Брата выведать их.

Автору неизвестны случаи, когда служба внешней российской разведки оказала значимую помощь стратегическим разработкам. Люди постарше вспомнят, как во время своего визита в США Хрущев на банкете в Калифорнии целовался с неким режиссером, смущая этим российских телезрителей. Так вот, брат этого режиссера, «секретный» физик Бруно Понтекорво в разгар холодной войны 1950 года бежал в Россию из американского атомного центра Лос-Аламос, прихватив элементы технологии производства ядерного оружия. (Сейчас известно, что технологии создания водородной бомбы тоже были украдены СССР из США и произвели большое впечатление на Сахарова, но не ускорили собственных разработок.) Но большинство разведчиков невысоко оценивают вклад шпионажа России в создание ею атомной и водородной бомб, так как приближенные формулы расчетов из СССР оказались удобнее и точнее американских. Кроме того, наш метод обогащения урана по разности плотностей соединений U235 и U238 был проще и эффективнее метода собачников из Лос-Аламоса, производящего обогащение урана за счет разницы в скоростях диффузии изотопов. В годы холодной войны объем краж технологий дошел до абсурда - американские и «корейские» самолеты, обладая идентичными системами «свой-чужой», не могли отличить друг друга по изображениям на экранах радиолокаторов.

Другого рода случай произошел в начале 60-х, когда хрущевская оттепель упразднила «железный занавес», отделявший соцлагерь от буржуазного мира. Тогда разведки беспокоил вопрос о состоянии разработок жидкого ракетного топлива у врагов. Поэтому КГБ устроило международную «научную» конференцию по ракетному топливу, строго-настрого запретив своим специалистам приводить конкретные факты о достижениях. Однако спецы из ЦРУ подло провели наших, заявив: «Не будем задавать вопросов, но сами ответим на любые». По характеру заданных на радостях вопросов они многое узнали и о направлениях российских исследований, и об их состоянии, сократив тем самым свое отставание в создании мощных баллистических ракет на пару лет. Теперь, если на одну чашу весов положить «подарки» разведки, а на другую сумму секретов, уплывших за кордон из-за двойной игры или промахов, то неизбежно последует грустный вывод, что научный и экономический шпионажи аморальны, принося крупный ущерб даже стране, их применяющей. И пока существуют разведки, будет угроза раскрытия конфиденциальных данных.

Правительства всех стран мира стремятся лишить людей интимной жизни: письма читаются, телефоны прослушиваются, багаж и носильные вещи досматривается, за людьми наблюдают. Вместе с тем все больше наши частные сообщения идут по электронным каналам. Сначала были телефоны, потом появились факсы и наконец вовсю заработала электронная почта. Сообщения электронной почты особенно легко перехватывать или сканировать по ключевым словам, что широко делается как правительственными органами, так хакерами и просто любопытными. Международные отправления все без исключения читаются государственными службами.

Несомненные предвестники апокалипсиса, как взрыв Чернобыля, высыхание Арала, озоновые дыры и братоубийственные войны затмевают в нашем сознании важность сохранности личных тайн, давно грозящую перерасти в проблему, последствия которой могут стать катастрофическими уже в ближайшем будущем. Трогательно

наивные люди, верящие, будто неприкосновенность содержания их писем, телеграмм и телефонных разговоров охраняется Конституцией, должны понять: она лишь дает право на такую защиту, но охранять сама не может. У московского международного почтамта нередко можно найти валяющиеся на тротуаре вскрытые письма, так и не дошедшие до получателя. Известная американская киноактриса, познакомившись со своим досье в ФБР, воскликнула: «Боже, так я всю жизнь купалась в стеклянной ванне на людном перекрестке!» Поэтому когда США в 1994 году пытались принять за стандарт шифрования Clipper, позволяющий правительству читать любые частные шифровки, то более 50000 американцев направили по электронной почте в Вашингтон протесты.

Впрочем, порой некомпетентные сотрудники, отвечающие за безопасность, страшнее шпионов. Примером этого является известное дело Prestel, имевшее место в начале 80-х годов, когда был взломан «электронный почтовый ящик» герцога Эдинбургского. Администратор, отвечающий за работу системы британской электронной почты Prestel, по халатности оставил на экране дисплея свой пароль доступа к системе, и он стал известен злоумышленникам. Другой казус, вполне объяснимый низкой компетентностью служб безопасности произошел, когда бельгийский премьер-министр Вифред Мартене обнаружил, что посторонние через компьютерную сеть имеют доступ к государственным секретам в личных файлах членов кабинета министров. Несколько месяцев электронная почта Мартенса, включая секретную информацию об убийстве британского солдата террористами из Ирландской Республиканской Армии в Остенде, была доступна любопытным. Один из взломщиков для саморекламы показал газетному репортеру, как просто ворваться в компьютер Мартенса, получив доступ к девяти свежим письмам и шифру. Более того, в течение часовой демонстрации, он «столкнулся» с другим вором, грабившим тот же самый компьютер.

Кроме этой проблемы, есть и не менее важная сейчас, пусть не для личности, но для страны — сохранность данных исследований, разработок и стратегической управляющей информации в компьютерных системах. От этого напрямую зависит безопасность общества. Например, злоумышленное нарушение работы программ управления ядерных реакторов Игналинской АЭС в 1992 году по серьезности возможных последствий приравнивается к Чернобыльской катастрофе.

Основная опасность «дьяволов компьютерной преступности» состоит в том, что им, как правило, успешно удается скрыть свое существование и следы деятельности. Можно ли чувствовать опасность, если ЭВМ находится дома, а доступ к ней ограничен паролем? Однако известен случай, когда копирование данных с такого компьютера сделал ребенок, не подозревавший ничего плохого и рассчитывавший, запустив данную ему другом дискету, поиграть в новую очень интересную игру.

Статистика экономических преступлений западного мира демонстрирует их перемещение в область электронной обработки данных. При этом лидирующее положение занимают махинации в банках, которые сводятся к изменению данных с целью получения финансовой выгоды. Новизна компьютерных преступлений состоит в том, что информация, представляющая активы фирм, теперь хранится не на бумаге в видимом и легко доступном человеческому восприятию виде, а в неосязаемой и считываемой только машинами форме на электронных устройствах хранения. Раскрывается лишь малая толика компьютерных преступлений, так как финансовые компании предпочитают о них умалчивать, чтобы не потерять престижа. Удивительно поэтому было заявление Сити банка, что за 1994 год выявлено около ста попыток электронных краж из России и половина из них окончилась удачно, нанеся ущерб на десятки миллионов долларов. В связи с этим из прессы стали известны имена таких петербуржцев, как Владимир Левин и супруги Корольковы (похоже, что это были рядовые исполнители).

Эксперты считают, что около 70% финансовых преступлений в банках совершают свои сотрудники, связанные с обработкой данных на вычислительной технике. Цена каждого подобного проникновения составляет в США от десятков тысяч до миллиона долларов и, по оценке криминалистов, убытки от незаконного проникновения в финансовые автоматизированные системы оцениваются минимум в десятки миллионов долларов ежегодно. Кто знает, чем был вызван «черный понедельник», 10 октября 1987 года, когда компьютеры многих бирж и банков Уолл-стрита внезапно стали распродавать акции, которые в то время следовало бы придержать?

За примерами легкости потрошения закрытых для посторонних компьютеров далеко ходить не надо. Для демонстрации своих возможностей хакеры неоднократно взламывали секретные системы на глазах изумленных экспертов. Термин хакер (по-русски hacker ближе всего к словам трудяга, поденщик, наемный рабочий. Хакерами еще порой называют журналистов, пишущих скандальные статьи по заказу) стал впервые использоваться в Массачусетском технологическом институте в начале семидесятых годов, применительно к молодым программистам и проектировщикам аппаратных средств ЭВМ, которые в гаражах и подвалах мастерили первые персональные компьютеры и даже пытались продавать их. Позднее газетчики стали называть хакерами компьютерных преступников всех родов и мастей.

Чтобы понять истоки нынешнего компьютерного разбоя, нужно осмыслить социальный климат 60-х на Западе. То поколение молодежи вырастало в мирное время, прочувствовав на себе массу социальных несправедливостей. С вовлечением США во Вьетнамскую войну и призывом на нее студенты нашли первую причину для протеста, и университетские городки заполнили демонстранты. Расстрелу манифестантов в Беркли молодежь противопоставила не прямое насилие, а лояльные формы неповиновения, в виде демонстративного сожжения призывных документов и разрушения данных в компьютерах Министерства обороны.

Другой аспект современного мира волновал молодежь не меньше: почему миллионы людей живут в бесконечной бедности. Казалось простым и логичным обвинить в этой бедности государство и тех, кто побогаче. Молодое поколение хотело изменить все и сразу вызвав хаос, переходящий в анархию. В итоге это привело ее к лозунгу «грабь награбленное» и породило сложные нравственные проблемы. Но все хорошее в жизни, утверждают скептики, либо незаконно, либо аморально. Мелкое пакостничество хакеров, хотя занятие совсем не из порядочных, но есть масса куда более порочных и по-человечески менее привлекательных. Стремление политиков к власти, а бизнесменов к деньгам, например.

Число хакеров много больше, чем кажется на первый взгляд, а их незаконные действия имеют очень широкий диапазон от подглядывания чужих секретов из простого любопытства до грабежа и убийств. Представьте себя юнцом, который понял, как можно сделать телефонные звонки по компьютеру бесплатными. Вскоре, благодаря общению с друзьями из других городов и стран в его руки попали подробные инструкции о том, как можно стянуть деньги с чужой кредитной карточки. Искушение надуть знаменитую компанию вроде VISA велико, а действительные последствия ареста, да и сама его возможность из-за недостатка жизненного опыта кажутся расплывчатыми.

Человек, назвавшийся Мануэлем Вайлариалом, заказал по телефону в США компьютер и сообщил продавцу, что Билл Майер придет отобрать для него товар днем позже. Продавец магазина стал подозрительным, заметив чрезмерное волнение юноши, представившегося Майером. Поскольку юноша не смог вполне доказать свои полномочия, то продавец предложил ему, чтобы Вайлариал пришел и засвидетельствовал себя лично. После ухода парня продавец вызвал полицию и Майера, известного также как хакер по кличке Петр 1, арестовали меньше, чем за день. Он был

обвинен в попытке использовать чужую кредитную карточку и полицейские конфисковали у него сотни дискет, пытаясь их «обыскать». «Мы распечатывали содержимое лишь одного файла в течение трех часов подряд» — посетовал полицейский журналистам. Этот файл содержал по крайней мере 10000 фамилий, с номерами кредитных карточек, датами их истечения, адресами, номерами телефонов и водительских удостоверений.

Вскоре стал известен другой инцидент. Парень зарезервировал по телефону в гостинице место, дав номер своей кредитной карточки. Лишь когда он съехал, дежурный администратор гостиницы заметил, что кредит в $500 за номер был сделан по его собственной карточке. Прочтя вскоре в газете о Петре 1, администратор вспомнил, будто в день заказа молодым человеком гостиничного номера был сбой в системе их компьютера и хотел узнать в полиции — не связано ли это с Петром 1. Увы, полиция не знала. Должностные лица гостиницы тем не менее утверждали: их ограбил хакер, потому что нанятый ими антихакер доказал оформление кредита через телефонный модем, а не с терминала в гостинице, как это принято. Полиции точно так же не удалось связать дело Петра 1 с 9 компьютерными кражами в Вашингтонском университете. Полиция нашла невероятным, чтобы хакеры могли взломать систему университета. Они, может, и хотели бы, однако в полиции не представляли себе, как можно было это сделать.

Дело доходило до того, что подростки в США играли — кто больше взломает компьютеров государственных учреждений. Тринадцать юных хакеров были обвинены во взломе компьютера университета штата Вашингтон и причинении дорогостоящего повреждения файловой системе. Один из них, учащийся школы 14 лет из Нью-Йорка, кроме того подозревался в блокировании компьютера ВВС Пентагона. Хакер по кличке Зод подобрал пароль, который давал студентам университета легальный доступ к системе и захватил над ней контроль, загрузив в компьютер собственную программу, через которую и другие могли бы незаконно войти туда. Благодаря ему толпа из полусотни хакеров, ворвалась в систему университета, видоизменяя и удаляя файлы пользователей. Зод был выслежен через телефонную сеть администратором системы. Аресты и обыски были произведены сразу в 17 местах, где полиция конфисковала на $50000 компьютеров и оборудования. Большинство хакеров проникают в системы из чистого любопытства и удовлетворения от отгадывания паролей. Зод из их числа, но последствия его действий оказались плачевными.

Действия хакеров нередко дискредитировали государственные службы безопасности. Образцами беззащитности компьютерных систем от хакеров служат и бесплатное предоставление младшему американскому школьнику свободного доступа к военной вычислительной сети, лишь бы только он перестал блокировать работу ее узлового процессора, и доказательство возможности коррекции орбиты спутника НАСА, сделанное любителями из клуба CCC (CCC (ChaosComputerClub) — клуб европейских хакеров) в 1986 году. Тогда же расследование полиции Амстердама, в сотрудничестве с бригадой разведки и географического отдела науки Свободного университета привело к аресту двух хакеров. Они, вторгаясь в компьютерные системы, нанесли ущерб более чем на сто тысяч голландских гульденов. 25-летний компьютерный инженер по кличке Fidelio и 21-летний студент по кличке Wave, были первыми хакерами, которых арестовали в Нидерландах. Из операционной системы UNIX своего компьютера они были способны получить доступ к другим ЭВМ в США, Скандинавии, Испании и Италии, где крали пароли, программы и закрытые технические данные.

Убытки от компьютерной преступности оценить трудно, но один миллион долларов, украденный с помощью ЭВМ Джерри Шнайдером при выставлении счетов за оплату телефонных разговоров в 60-х годах, давным-давно стократно превзойден и

вычеркнут из книги рекордов Гиннесса. Приведем еще несколько коротких примеров. В 1987 году вскрыта многомиллионная кража из компьютера фирмы Фольксвагенверк. Зафиксирована чуть не закончившаяся успехом попытка выкрасть хакерами 15,2 миллионов долларов государственного лотерейного фонда штата Пенсильвания. Трое больных раком скончались из-за модификации программы радиологической облучающей установки, задавшей им в 100 раз более высокие дозы облучения.

Если события в дальних странах представляются как мягкий ландшафт, прикрытый дымкой, то происходящее на родине ослепляет от близости контрастами ярких красок. Поэтому про Россию очень сложно писать непредвзято. В бывшем СССР обстановка много сложнее, чем на Западе. Хотя наша компьютерная преступность родилась лишь в конце семидесятых годов, но попав на благодатную российскую почву, где нет ограничивающих ее законов, быстро разрослась в лавину, грозящую смести зачатки информационных отраслей экономики. В 1991 году из Внешэкономбанка с помощью компьютера похищено $125000. Лишь в сентябре 1994 года в ОПЕРУ Сбербанка Москвы выявлено больше чем на сто миллиардов рублей фальшивых электронных авизо и арестовано три хакера. Неизвестные хакеры годом ранее пытались похитить по компьютерной сети Центробанка 68 миллиардов рублей. Всего по данным ЦБ России ежеквартально выявляется фиктивных электронных платежей на десятки миллиардов рублей.

Усиление зависимости деловых и научных кругов от ЭВМ наряду с озабоченностью общественности, что обработка информации затрагивает личные интересы граждан, привела к возрастанию внимания к проблемам защиты конфиденциальных данных в компьютерах от незаконного доступа. Нельзя сказать, чтобы такими проблемами раньше никто не занимался. КГБ имел специальную службу, защищающую партийную и дипломатическую связь от ознакомления с ее секретами непричастных (8 управление КГБ занималось шифрами). В армии вопросами секретной связи ведало ГРУ — Главное разведывательное управление, теснейшим образом связанное с КГБ, специализирующееся на разведке и отлично финансируемое. Однако эти учреждения всегда ставили перед собой и противоположную задачу — добиться, чтобы никто из граждан России не смог защитить свои данные от их взора. Общество по сей день не только лишено малейших познаний в криптографии, но и редкие публикации, появлявшиеся в печати до распада СССР, представляли грубую дезинформацию. Из сообщений в прессе и по телевизору можно сделать вывод, что, обладая абсолютной монополией в области засекречивания, государственная криптографическая служба России стремится и впредь ее сохранять.

На Западе у фирм факсы и телефоны оснащены криптографическим оборудованием, а как быть нашим коммерсантам? Отечественные средства засекречивания могут расколоться при первой же атаке, вследствие того что меньшая часть их не имеет теоретической основы, а большая сделана в лабораториях тех же спецслужб. Вспомните — шла иракская война, когда появилось сообщение, будто французы кодовым сигналом отключили бортовые компьютеры самолетов «Мираж» армии Хусейна. Можно ли быть уверенным в том, что спецслужбы не оставили себе «ключ от черного входа» к шифрам? Но кто в России кроме ФАПСИ, Федерального агентства правительственной связи и информации, пришедшего на смену 8 управлению КГБ, способен провести экспертизу средств защиты данных? Может быть, стоит приобретать такие средства за рубежом? Однако почти все правительства проводят политику запрета доступа к секретам криптографических служб и систем защищенной связи. Контроль за экспортом в США ограничивает развитие внутренних и международных криптографических служб. Билль сената S266 от 1991 года требует чтобы американское криптографическое оборудование содержало ловушки, известные лишь АНБ (NSA (National Security Agency) — Агентство национальной безопасности США, за-

нимающееся шифрами. Оно больше и лучше финансируется, чем ЦРУ и ФБР вместе взятые), а чиновники могли прочесть любые шифрованньк сообщения, а это подрывает общественное доверие к технике из США. Там в 1992 году ФБР предложило конгрессу закон, облегчающий подслушивание телефонных сообщений, и это вызвало резкое возмущение общественности. Однако наибольшее вторжение в личные секреты Белый Дом осуществил в 1993 году, пытаясь утвердить в качестве государственного стандарта криптографическую микросхему Clipper для употребления при засекречивании в телефонах, факсах и электронной почте. Компания AT&T ставит микросхему Clipper во все свои изделия, обеспечивающие конфиденциальность. Вместе с тем, что каждый пользователь может установить свой секретный ключ, правительство США будет иметь возможность свободно читать их сообщения, так как имеет ключи от «черного входа» в Clipper.

Далее, лишь квалифицированные пользователи способны качественно эксплуатировать сложную шифровальную технику. Давным-давно ходил анекдот, как неизвестный доброжелатель посоветовал специалистам фирмы Хагелин, производящей криптографическое оборудование, сделать ревизии своих изделий, поставленных одной азиатской стране. Оказалось, что там, в установленном силами местных умельцев шифрующем блоке, телеграфные сигналы шли помимо его и лишь перепутанные соединения создавали видимость шифра. Вызывает серьезную озабоченность качество используемых, но не апробированных научной общественностью методик шифрования. Стандарт США по засекречиванию, именуемый далее DES, выдержал критику, а чего стоит стойкость к взлому неаттестованных шифров, например, применяемых в таких широко распространенных базах данных, как Paradox или Access, никто кроме криптографов не знает.

В настоящее время люди, которым нужна гарантированная защита своих данных от постороннего вмешательства, незнакомы даже с ее основами. Эта книга, написанная на элементарном уровне, задумана азбукой по криптографии и предназначается в первую очередь тем, кто работает на персональных компьютерах и планирует вести там защиту своих данных. Все же автор старался сделать ее занимательной для широкого круга читателей, представив как первую книгу по шифрованию. Хочется верить что все: писатели, журналисты, историки, деловые люди и школьники смогут найти в ней для себя что-нибудь интересное и полезное. Под защитой данных далее понимается ряд организационных и технических мер по их охране с целью предотвратить несанкционированный доступ к содержащемуся в них смыслу или искажение. Большое внимание в книге уделено скучным вопросам административного и организационного характера, без решения которых шифрование бессмысленно. Автор придерживается точки зрения, что криптография состоит из истории, теории и практики, которым посвящены страницы этой книги. Надлежит сделать ряд замечаний. Во-первых, автор не претендует на всеобъемлющий и строгий научный подход, считая, приведенный технический уровень вполне достаточным для начального ознакомления. Во-вторых, он, отнюдь, не считает изложенный материал не только полным, но даже абсолютно точным, когда речь идет о событиях, еще недавно считавшихся государственной, дипломатической или военной тайной. Многие факты так и не удалось перепроверить из-за отсутствия доступных первоисточников, и к их изложению следует отнестись как к анекдотам или вольному пересказу. В-третьих, он не имеет желания вступать в полемику по изложенным вопросам, и предлагает тому, кто может сказать больше, правильнее или лучше, самому написать книгу, а автор будет рад ее прочесть.

Непосредственным поводом к написанию этой книги послужило сообщение о незаконном изъятии московскими властями в 1991 году у фирмы МММ коммерческой документации. Невольно подумалось, что стало бы делать следствие с изъятыми шиф-

ровками? Жизнь не принимает сослагательного наклонения — ее требования конкретно и жестки. Видимо, по этой причине шифровальная техника стала широко внедряться. Сейчас аппаратурой засекречивания оборудованы не только резиденция Патриарха Московского и Всея Руси Алексия II, РТСБ и МЕНАТЕП, но и масса небольших коммерческих контор. Похоже, перехват их корреспонденции не грозит превратиться в сенсации на страницах газет.

Хотя традиционно криптография применялась исключительно вооруженными силами и дипломатическими службами, но сейчас она позволяет выполнять деловые операции путем передачи информации по сетям связи с использованием методов идентификации и аутентификации (идентификация и аутентификация — доказательства авторств и подлинности сообщения), цифровой подписи, выдачи разрешений на транзакции с регистрацией и их нотариальным заверением, отметки даты, времени суток и многое другое. Эти новые приложения превращают криптографию в технику двойного использования — для военных и гражданских целей. Шифрование в гражданском секторе ведется для проведения международных банковских операций, электронного обмена информацией, обмена электронной почтой и коммерческих сделок по сетям связи более чем 1000 коммерческих организаций в России и не менее чем 600 банков уже используют для этого специальные криптографические устройства. В основе такого разграничения применений лежит разделение сфер использования криптографии для сохранения секретности информации и для ее аутентификации. Это разграничение явно выражено в новейших криптографических системах с открытым ключом. Криптография необходима частному коммерческому сектору экономики России для прогрессивного развития и применение ее не должно зависеть лишь от интересов ФАПСИ. Это относится к использованию криптографических алгоритмов, их прикладных применений, общих методов управления ключами и их распределения. Газета «Московский комсомолец» в 1992 году опубликовала статью с утверждением, что шифры, созданные коммерческими специалистами, ФАПСИ расколет за обеденный перерыв. Автор верит: после того, как не знающие шифрования коммерческие специалисты прочтут эту книгу, в ФАПСИ обеды станут гораздо продолжительнее. Ему непонятна гордость засекреченных академиков неведомыми достижениями, когда лишенное элементарных познаний в области шифрования общество беззащитно от растущей компьютерной преступности. В этом смысле Россия, перефразируя Марка Твена, напоминает рыцаря, надевшего на голову мощный шлем, но выступающего по полю битвы голым, без доспехов и щита.

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 сизюмар 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 сисгемы 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 бую 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, о чем будет рассказано ниже. 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 экспеспублики Югославии, где для сербохорватского языка давно используются сразу две основные системы письменности. Одна из них, вуковица, названная по имени Вуко Караджича, 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 набира-

ли 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 мало и в этой книге многие факты даны через художественный анализ. 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, что читателям просто проверить на кухне.) 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-шпиона 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, дос-

тупные 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 СМ-4. 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.

Символ	Число в тексте	Код
А	4	00
М	4	01
пробел	2	100
Ы	2	101
Р	1	110
Л	1	111

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, ис-

пользованы 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 MKKTT(MKKTT — международный консультативный комитет по телеграфии и телефонии) рекомендовал стандарт H.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 RADIX-50. 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 MOCKBA 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 RADIX-64:

Значение	0	1	2-11	12-37	38-63
Символ	+	/	0-9	A-Z	a-z

```
--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 ABC, а 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:

Таблица кодирования		Таблица декодирования	
VANOL	A, an	ABABA	It is hoped
LANEX	Abandon-ing-s	ABACA	Assignment
STUGH	Abandoned	ABBCO	Shipped
TBYNT	Abate-ing-s	ACAYT	As to
RIZLB	Abated	ACDZR	Terminated

В этом коде использованы не все возможные группы, например, нет группы AAAAA. 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)206-DID-DEMA, не надо смущаться — это телефон корпорации Aldus в Сиэтле. Кодовая таблица соответствия букв цифрам показана ниже. Из таблицы определяем, что номер телефона корпорации 343-3362. Хотя, увидев на рекламном щите телефон предварительных заказов ночного клуба GUE-STS-ONLY, не пытайтесь набирать 483-787-6659, а просто переведите с английского: «только для приглашенных». Эта запись в рекламе означает, что заказы принимаются по телефону, указанному в пригласительном или членском билете.

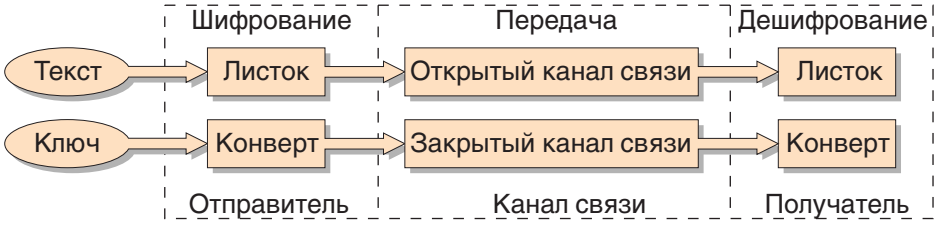
1	2	3	4	5	6	7	8	9
	ABC	DEF	GHI	JKL	MNO	PRS	TUV	WXY

Надеюсь, читатели поймут сообщение «Женя Дмитрий Ульяна Борис Ольга Роберт Игорь Света», 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 не повезло 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.

Наше 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 развивайтся, 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.