Министерство образования и науки Украины
Донецкий национальный технический университет
Кафедра прикладной математики и информатики

РЕФЕРАТ

«Криптография. Обзор криптографических алгоритмов»

Д0403.52.02.034Р

Руководитель:_____ Н. Е. Губенко
(подпись) (дата)
_____ А. В. Чернышова
(подпись) (дата)

Составил :_____ Д. П. Пауков
ст. гр. ПО-98в (подпись) (дата)

ДОНЕЦК
2002

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

…Я не люблю холодного цинизма,
В восторженность не верю, и ещё –
Когда чужой мои читает письма,
Заглядывая мне через плечо…

В. Высоцкий,
«Я не люблю», 1969.

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 высоконаучная 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.

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.

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, выведанные за рубежом. На практике это может выглядеть таким образом.

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 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.

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 доля 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 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.

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.

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 (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

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, занимающееся шифрами. Оно больше и лучше финансируется, чем ЦРУ и ФБР вместе взятые), а чиновники могли прочесть любые шифрованные 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.

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. 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.

Существует два основных типа алгоритмов, основанных на ключах: симметричные и с открытым ключом. Симметричные алгоритмы, иногда называемые условными, представляют собой алгоритмы, в которых ключ шифрования может быть рассчитан по ключу дешифрования и наоборот. В большинстве симметричных алгоритмов ключи шифрования и дешифрования одни и те же. Эти алгоритмы требуют согласованности ключей между отправителем и получателем перед безопасной передаче сообщения. Симметричные алгоритмы делятся на две категории: одни алгоритмы обрабатывают открытый текст побитно (иногда побайтно), они называются потоковыми алгоритмами, другие работают с группами битов открытого текста – блочные алгоритмы.

Алгоритмы с открытым ключом (называемые ассиметричными) разработаны таким образом, что ключ, используемый для шифрования, отличается от ключа дешифрования. Более того, ключ дешифрования не может быть (по крайней мере в течении разумного интервала времени) рассчитан по ключу шифрования. Таким образом, ключ шифрования открыт для всех, а ключ дешифрования известен только конкретному человеку.

1 СИММЕТРИЧНЫЕ АЛГОРИТМЫ ШИФРОВАНИЯ

1.1 Шифры замены основанные на XOR

Самый простой и эффективный способ сделать текст нечитаемым - спрятать его, смешав с последовательностью случайных чисел, заданной ключом, с помощью операции XOR (операция XOR выполняет следующие действия:

(0 XOR 0)=0, (0 XOR 1)=1, (1 XOR 0)=1, (1 XOR 1)=0.

При этом информация сообщения прячется в шуме - самом информативном, по определению Шеннона, сигнале. Все правильно, песчинку лучше прятать на пляже, рыбу в море, а информацию в шуме.

Есть и другие обоснования выбора случайных чисел для шифрования заменой. Можно исходить из того, что криптоаналитик попытается снизить неопределенность чтения шифровки, зная статистические свойства нашей последовательности. А как только человеку становится известным чье-то намерение, то его поведение соответственно меняется. Поэтому если криптоаналитик знает наше намерение использовать последовательность, где 1 встречается с вероятностью p, а 0 с вероятностью 1-p, то, зная теорию игр, он тоже с вероятностью p будет предполагать наличие 1. Вероятность его успехов будет равна:

P(P)=P-P+(1-P)-(1-P)

Эта функция достигает минимума при p=0.5, что выпадает при случайном выборе из 0 и 1 с равновероятными исходами. Далее, если биты в случайной последовательности с одинаковой вероятностью принимают значения 0 и 1, то биты в шифровке будут обладать тем же свойством. Докажем это. Пусть вероятность нулевого бита в тексте равна p, а единичного соответственно 1-p. Нулевой бит в шифровке появляется, когда соответствующие биты последовательности и текста оба равны либо 0, либо 1. Значит, вероятность появления нулевого бита в шифре равна:

P=0.5-p+0.5-(1-p)=0.5

Более того, если биты в используемой для шифрования случайной последовательности статистически независимы друг от друга, то и в шифровке они становятся такими же. Текст превращается во что угодно, то есть в шум. Из-за специфики операции XOR процедура шифрования совпадает с процедурой расшифрования. Например, обозначив через t вектор бит сообщения, y вектор случайной последовательности и s шифровки, получаем t=s XOR y и s=t XOR y.

У машинного многоалфавитного шифра замены с помощью операции XOR есть ряд очень слабых мест, которые нужно знать и учитывать при использовании этого шифра. Серьезную неприятность может доставить обратимость этого шифра, так как для расшифровки применяется то же самое преобразование, что и для зашифровки. В том случае, если одно и то же сообщение должно быть послано нескольким адресатам и шифруется одним и тем же шифром может произойти так, что длина сообщения изменится из-за сбоя или ошибки. В этом случае будет получено 2 сообщения разной длины.

Другая неприятность с машинным многоалфавитным шифром замены может возникнуть, если в сообщении встречаются большие участки пробелов или

нулевых символов. Допустим, например, что линия связи недозагружена, но в то время, когда нет сообщений, аппаратура шифрования не выключается. Поэтому когда сообщений нет и t=0, шифровка будет представлять собой "чистую" последовательность ключа. Если в это время с помощью специальной аппаратуры перехватить шифровку, представляющую собой ключ s=y, то можно наложить на нее текст своего сообщения s'=s+t=t+y и передать искаженную шифровку по каналу связи. Получатель, расшифровав ее: s'+y=s+t+y=t+y+y=t получит переданный ему перехватчиком текст сообщения. А так как этот текст поступит в шифрованном виде, то его содержимому могут поверить, а это уже никак не допустимо. Так как перехватчик не знает, свободна ли линия, то будет накладывать свой текст на непрерывный шифрованный сигнал наугад несколько раз. Даже если в это время по линии шла передача - не беда, скорее всего возникшие искажения будут интерпретированы как помехи в канале связи.

1.2 Шифры перестановки

Из-за отмеченных особенностей шифр замены в чистом его виде никогда не применяется, а всегда употребляется вместе с перестановкой, например, бит внутри байта. Если после замены символы сообщения превращались во что угодно, но сохраняли в шифровке свое исходное местоположение, то после перестановки они там и расположены еще и где угодно, что надежно защищает шифровку от атак криптологов. Потому что перестановку можно рассматривать как умножение вектора сообщения на матрицу перестановки бит P с элементами 0 и 1 и размером в длину сообщения в битах. Рассмотрим два случая.

1) Перестановка может делаться до наложения на сообщение случайной последовательности, то есть s'=Pt+y. В случае, если текст в сообщении отсутствует t=0 и идут нули или пробелы, то s'=y, а в канал связи попадает чистый ключ.

2) Перестановка может делаться и после наложения на сообщение случайной последовательности, то есть s"=P(t+y). В случае, если текст в сообщении отсутствует t=0 и идут нули или пробелы, как s"=Py, а в канал связи попадает ключ, шифрованный перестановкой.

Поэтому обычно предпочтение отдается второй схеме, когда в отсутствие текста шифровка представляет собой не чистый ключ, а осложненный перестановкой. Хотя и в том, и в другом случае наложение на шифровку своего текста для введения получателя в заблуждение ничего не дает. Однако перестановки необходимы и для того, чтобы атака на ключ стала неэффективной. Если передача идет побайтно, то достаточно лишь переставлять биты внутри байта, чтобы с вероятностью 0.97 исказить его и сделать перехват ключа описанным способом невозможным.

Шифр замены, осложненный перестановкой, представлял собой раннее поколение машинных криптографических преобразований. Он окончательно испортил надежду на вскрытие шифра хитроумными методами отгадывания текста сообщения, оставив взломщикам лишь возможность прямого подбора ключа. Вскрытие случайной перестановки без знания ключа неоднозначно, что не позволяет сколько-нибудь уверенно расшифровать сообщение. Однако по

сохранившейся статистике использованных в сообщении символов можно делать более или, скорее, менее уверенные прогнозы о его общем содержании.

1.3 Шифры взбивания и стандарт DES

Казалось бы, что предел возможностей сокрытия сообщения уже достигнут. Результат можно ощутимо улучшить, если вместо перестановки использовать линейное преобразование: s=L*t, где L - невырожденная матрица случайного линейного преобразования бит, или, что то же самое, детерминант L не равен нулю. И хотя расшифровывание в этом случае придется осуществлять решением систем линейных уравнений, но каждый бит шифровки начинает уже зависеть от каждого бита текста. Шифры на основе этого преобразования называют скрамблерами или взбивалками за то, что они взбивают текст сообщения, как повара омлет. К сожалению, доля невырожденных матриц с увеличением их размера стремительно убывает. Детерминант матрицы L, как и ее элементы, может быть равен либо 0, либо 1. Если det(L)=0, то матрица вырождена.

Для того, чтобы матрица L была невырожденной, случайной и при расшифровании не нужно было производить много вычислений, американскими криптографами был предложен алгоритм, легший в основу стандартного криптографического преобразования DES. Суть его одного шага можно описать следующей схемой.

Входной блок данных делится пополам на левую L' и правую R' части. После этого формируется выходной массив так, что его левая часть L" представлена правой частью R' входного, а правая R" формируется как сумма L' и R' операцией XOR. Далее, выходной массив шифруется перестановкой с заменой. Можно убедиться, что все проведенные операции могут быть обращены и расшифровывание осуществляется за число операций, линейно зависящее от размера блока. В то же самое время, после нескольких таких взбиваний можно считать, что каждый бит выходного блока шифровки может зависеть от каждого бита сообщения.

Система шифрования DES была разработана IBM под именем Lucifer и предложена со своими корректировками Национальным Бюро Стандартов США в 1976 году как стандарт шифрования. В нейпримене ключ из 56 бит. Следует отметить, что в стандарте DES применены перестановки лишь специального типа, что наводило критиков этого стандарта на мысль, что АНБ хорошо знало их теорию и могло для взлома воспользоваться заранее известными слабыми местами. Однако принцип этого шифрования прошел самую широкую апробацию и ему посвящено множество публикаций. Нарекания вызывали лишь выбранные короткими длины блока в 64 бита и ключа в 56 бит, что недостаточно для таких задач, как национальная безопасность. Свое развитие DES получил в ГОСТ 28147-89, который увеличил длину ключа до 256 бит и допустил произвольные перестановки.

Шифр DES принят федеральным стандартом США, и хорош в использовании для многих коммерческих приложений. Однако правительства

сами никогда не используют шифры, предлагаемые коммерсантам, чтобы закрыть свои данные, так как они недостаточно стойки от атак аналитиков. Например, 16-кратный DES был взломан Шамиром, применявшим дифференциальный криптоанализ, и Матсуи, использовавшим линейный криптоанализ. Наиболее серьезную практическую атаку на DES осуществил Мишель Винер, который разработал и опробовал микросхему, проверяющую в секунду 50 миллионов ключей DES. ЭВМ, стоящая миллион долларов и содержащая несколько десятков тысяч таких микросхем, способна перебрать все ключи DES за 7 часов. АБН тратят на вычислительную технику такие деньги, что могут построить ЭВМ, взламывающую шифровку DES за секунду. Это означает, что DES нельзя пользоваться для серьезных приложений. Для того, чтобы испортить правительственным криптоаналитикам сон, коммерсанты применяют так называемый "тройной DES", шифруя сообщение трижды двумя разными ключами, что увеличивает реальную длину ключа до 112 бит. Однако такой метод медленнее обычного DES метода в три раза.

1. 4 Шифр Энигмы

Энигма - шифр того типа, который вырабатывала известная уже машина Энигма инженера Кирха. При его моделировании на ЭВМ можно достичь хорошей устойчивости при сравнительной простоте программы. Напомним, что эта машина представляла собой ряд вращающихся на одной оси барабанов с электрическими контактами, обеспечивающих множество вариантов простой замены, определяемой текущим положением барабанов. В ранних моделях было 5 барабанов, которые перед началом работы устанавливались по кодовому слову, а в ходе шифрования они поворачивались при кодировании очередного символа как в счетчике электроэнергии. Таким образом, получался ключ заведомо более длинный, чем текст сообщения. В чем же была слабость шифра?

1) Пять барабанов могли обеспечить лишь около ста миллионов ключей, что позволяло их за день перебрать на ЭВМ. Если использовать не 25 латинских символов, а 256 кодов ASCII и увеличить число барабанов, то сложность раскалывания шифра существенно возрастет.

2) Набор барабанов был ограничен и менялся редко, что вызвало охоту англичан за их экземплярами в подводных лодках. ЭВМ может для каждой шифровки использовать индивидуальные барабаны, генерируемые по ключу, а это опять таки резко усложняет вскрытие шифра.

3) Наконец, можно сделать движение барабанов хаотичным по случайной последовательности, тоже вырабатываемой по ключу.

Подсчитаем число ключей такого шифра, реализованного программно. Пусть длина периода программного генератора случайных чисел равна 2**24. Восемь барабанов, генерируемые с помощью этого генератора, дадут вместе 2**192 вариантов ключа, а если учесть еще варианты псевдослучайной последовательности, управляющей движением барабанов, то получится внушительная цифра в 2**216 вариантов ключа. Таким образом, довольно просто получить устойчивый шифр даже при использовании программного генератора случайных чисел с периодом малой для криптографии длины. И хотя

несомненно, что криптоаналитики наработали массу "домашних заготовок" для атак на такой шифр, но еще князь Владимирко Галицкий знал о том, что "в наше время чудес не бывает", и вскрытие шифра Энигмы будет дорого стоить.

1. 5 Другие шифры

На самом деле систем шифрования побольше, чем описано. Но практически употребляется лишь похожий на DES алгоритм IDEA (IDEA - Improved Proposed Encryption Standard - улучшенный стандарт шифрования.) , отличающийся применением ключа длиной 128 бит и смещением операций разных алгебраических групп для блоков длиной 64 бита. Алгоритм IDEA разработан в Цюрихе Джеймсом Мэсси и опубликован в 1990 году. Он считается более стойким, чем традиционный DES, и представляет основу программы шифрования PGP, применяемой пользователями Интернет. Разработчик PGP, Фил Циммерман, сейчас подвергнут в США уголовному преследованию за экспорт криптостойких шифров. Примечательно, что алгоритмы, входящие в PGP, как IDEA и RSA, АНБ ранее объявляло не стойкими криптографически, но, тем не менее, завело дело "Правительство США против Филиппа Циммермана". Приравняв Фила к торговцам оружием и наркотикам, АНБ фактически созналось в очередной лжи - похоже, что PGP с IDEA и RSA оказалась слишком "крепким орешком" для правительственных чиновников.

Перечислим и другие блочные шифры [2]: MADRIGA, NewDES, FEAL, REDOC, LOKI, KNUFU, KHAFRE, RC2, MMB, CA-1.1, SKIPJACK, ГОСТ-28147-89, CAST, SAFER, 3-WAY, CRAB, SXAL8/MBAL и др.

2 ШИФРЫ С ОТКРЫТЫМ КЛЮЧОМ

2.1 Исторические данные

Развитие криптографии в XX веке было стремительным, но неравномерным. Анализ истории ее развития как специфической области человеческой деятельности выделяет три основных периода.

1) Начальный, имевший дело лишь с ручными шифрами, начавшийся в седой древности, за кончился лишь в конце тридцатых годов XX века. Криптография за это время прошла длинный путь от магического искусства древних жрецов до будничной прикладной профессии чиновников секретных ведомств.

2) Следующий период отмечен созданием и широким внедрением в практику сначала механических, потом электромеханических и, наконец, электронных устройств шифрования, созданием сетей засекреченной связи. Его началом можно считать применение телеграфных шифровальных машин, использующих длинный одноразовый ключ. Длится он по наши дни. Однако к середине семидесятых годов было достигнуто положения, когда повышение стойкости шифров отошло на второй план. С развитием разветвленных коммерческих сетей связи, электронной почты и глобальных информационных систем самыми главными стали проблемы распределения секретных ключей и подтверждения авторства. К ним теперь привлечено внимание широкого круга криптологов.

3) Началом третьего периода развития криптологии обычно считают 1976 год, когда американские математики Диффи и Хеллман предложили принципиально новый вид организации засекреченной связи без предварительного снабжения абонентов секретными ключами, так называемое шифрование с открытым ключом. В результате стали появляться криптографические системы, основанные на подходе, сформулированном еще в сороковых годах Шенноном. Он предложил строить шифр таким способом, чтобы его раскрытие было эквивалентно решению математической задачи, требующей выполнения объемов вычислений, превосходящих возможности современных ЭВМ. Новый период развития криптографии характеризуется появлением полностью автоматизированных систем шифрованной связи, в которых каждый пользователь имеет свой индивидуальный пароль для подтверждения подлинности, хранит его, к примеру, на магнитной карте, и предъявляет при входе в систему, а весь остальной процесс проведения секретной связи происходит автоматически.

В традиционных криптосистемах одним и тем же секретным ключом осуществляется как шифрование, так и дешифрование сообщения. Это предполагает, что отправитель и получатель сообщения получили идентичные копии ключа курьером. Этот прием почти неприменим для коммерческих фирм и абсолютно недоступен частным лицам из-за своей дороговизны.

При шифровании с открытым ключом для шифрования и расшифровывания используются разные ключи, и знание одного из них не дает практической возможности определить второй. Поэтому ключ для шифрования может быть сделан общедоступным без потери стойкости шифра, если ключ для расшифровывания сохраняется в секрете, например, генерируется и хранится

только получателем информации. Несмотря на подозрительность (кому верят криптоаналитики?) и консерватизм (лучшее - для криптографов - враг хорошего!) новые идеи стали быстро реализовываться на практике. Шифруют и сейчас традиционными методами, но рассылка ключей и цифровая подпись стали выполняться уже по-новому. Сейчас два метода шифрования с открытым ключом получили признание и закреплены в стандартах. Национальный институт стандартов и технологий США NIST (бывший ANSI) принял стандарт MD 20899, основанный на алгоритме ЭльГамаля, а на основе алгоритма RSA приняты стандарты ISO/IEC/DIS 9594-8 международной организацией по стандартизации и X.509 международным комитетом по связи.

2.2 Шифр Ривеста-Шамира-Алдемана (RSA)

Первой и наиболее известной криптографической системой с открытым ключом была предложенная в 1978 году так называемая система RSA. Ее название происходит от первых букв фамилий авторов Rivest, Shamir и Aldeman, которые придумали ее во время совместных исследований в Массачусетском технологическом институте в 1977 году. Она основана на трудности разложения очень больших целых чисел на простые сомножители. Алгоритм ее работает так:

1) Отправитель выбирает два очень больших простых числа P и Q и вычисляет два произведения N=PQ и M=(P-1)(Q-1).

2) Затем он выбирает случайное целое число D, взаимно простое с M, и вычисляет E, удовлетворяющее условию DE = 1 MOD M.

3) После этого он публикует D и N как свой открытый ключ шифрования, сохраняя E как закрытый ключ.

4) Если S - сообщение, длина которого, определяемая по значению выражаемого им целого числа, должна быть в интервале (1, N), то оно превращается в шифровку возведением в степень D по модулю N и отправляется получателю S'=(S**D) MOD N.

5) Получатель сообщения расшифровывает его, возводя в степень E по модулю N, так как S=(S'**E) MOD N = (S**(D*E)) MOD N.

Таким образом, открытым ключом служит пара чисел N и D, а секретным ключом число E. Смысл этой системы шифрования становится прозрачным, если упомянуть про малую теорему Ферма, которая утверждает, что при простом числе P и любом целом числе K, которое меньше P, справедливо тождество

K**(P-1)=1 MOD P.

Эта теорема позволяет определять, является ли какое-либо число простым или же составным.

Приведем простой пример на малых простых числах P=211 и Q=223. В этом случае N=47053 и M=46620. Выберем открытый ключ шифрования D=16813 и вычислим секретный ключ расшифровывания E=19837. Теперь, взяв за сообщение название метода RSA, переведем его в число. Для этого будем считать букву R равной 18, S равной 19, A равной 1 по порядковому номеру их положения в английском алфавите. На представление каждой буквы отведем по 5 бит числа, представляющего открытый текст. В этом случае слову RSA соответствует следующее число: S=((1*32)+19)*32+18=1650

С помощью открытого ключа получаем шифровку:

S'=(S**D) MOD N=1650**16813 MOD 47053=3071

Получатель расшифровывает ее с помощью секретного ключа:

S = (S'**E) MOD N=3071**19837 MOD 47053=1650

Авторы RSA в примере из своей первой публикации использовали D=9007 и N=1143816257578888676692357799761466120102182967212423625625618429357069352457338978305971235639587050589890751475992900268795435 41. Приняв за исходный открытый текст фразу из "Юлия Цезаря" Шекспира:

ITS ALL GREEK TO ME,

представленную целым числом

S=9201900011212000718050511002015013 05,

они получили такую шифровку

S'=1999351314978051004523171227402606474232040170583914631037037174062597160894892750439920962672582675012893554461353823769748026.

Криптостойкость системы RSA основана на том, что M не может быть просто вычислена без знания простых сомножителей P и Q, а нахождение этих сомножителей из N считалась трудно разрешимой задачей. Однако недавние работы по разложению больших чисел на сомножители показали, что для этого могут быть использованы разные и даже совершенно неожиданные средства. Сначала авторы RSA предлагали выбрать простые числа P и Q случайно, по 50 десятичных знаков каждое. Считалось, что такие большие числа очень трудно разложить на простые сомножители при криптоанализе. Райвест полагал, что разложение на простые множители числа из почти что 130 десятичных цифр, приведенного в их публикации, потребует более 40 квадриллионов лет машинного времени. Но математики Ленстра из фирмы Bellcore и Манасси из фирмы DEC разложили число из 155 десятичных цифр на простые сомножители всего за 6 недель, соединив для этого 1000 ЭВМ, находящихся в разных странах мира. Выбранное число, называемое девятым числом Ферма, с 1983 года находилось в списке чисел, разложение которых считалось наиболее желательным. Это число взято потому, что оно считалось неразложимым при существующей вычислительной технике и достаточно большим для того, чтобы его можно считать безопасным для формирования N в RSA. Как заявил Ленстра, ведущий в Bellcore исследования по электронной защите информации и разложению больших чисел, их целью было показать разработчикам и пользователям криптографических систем, с какими угрозами они могут встретиться и насколько осторожны должны быть при выборе алгоритмов шифрования. По мнению Ленстра и Манасси, их работа компрометирует и создает большую угрозу применениям криптографических систем RSA.

Следует учесть, что работа по совершенствованию методов и техники разложения больших чисел только началась и будет продолжена. Те же Ленстра и Манасси в 1991 году нашли делитель тринадцатого числа Ферма, которое состоит примерно из 2500 десятичных разрядов. Теперь разработчикам криптографических алгоритмов с открытым ключом на базе RSA приходится как чумы избегать применения разложимых чисел длиной менее 200 десятичных разрядов. Самые последние публикации предлагают для этого применять числа в 250 и даже 300 десятичных разрядов. А так как для щифрования каждого

блока информации приходится соответствующее число возводить в колоссально большую степень по модулю N, то для современных компьютеров это задача на грани возможного. Поэтому для практической реализации шифрования RSA радиоэлектроники начали разрабатывать специальные процессоры, которые позволили бы выполнять операции RSA достаточно быстро. Лучшими из серийно выпускаемых кристаллов являются процессоры фирмы CYLINK, которые позволяют выполнять возведение в степень целого числа из 307 десятичных знаков за доли секунды. Отметим, что чрезвычайно слабое быстродействие криптографических систем на основе RSA лишь ограничивает область их применения, но вовсе не перечеркивает их ценность.

2.3 Шифр ЭльГамаля

Криптографы постоянно вели поиски более эффективных систем открытого шифрования, и в 1985 году ЭльГамаль предложил следующую схему на основе возведения в степень по модулю большого простого числа. Для этого задается большое простое число P. Сообщения представляются целыми числами S из интервала (1, P). Оригинальный протокол передачи сообщения S выглядит в варианте Шамира, одного из авторов RSA, так:

1) Отправитель A и получатель B знают лишь P. A генерирует случайное число X из интервала (1,P) и B тоже генерирует случайное число Y из того же интервала.

2) A шифрует сообщение S1=S**X MOD P и посылает B.

3) B шифрует его своим ключом S2=S1**Y MOD P и посылает S2 к A.

4) A "снимает" свой ключ S3=S2**(-X) MOD P и возвращает S3 к B.

5) Получатель B расшифровывает сообщение: S=S3**(-Y) MOD P.

В системе ЭльГамаля большая степень защиты, чем у алгоритма RSA достигается с тем же по размеру N, что позволяет почти на порядок увеличить скорость шифрования и расшифрования. Криптостойкость системы ЭльГамаля основана на том, что можно легко вычислить степень целого числа, то есть произвести умножение его самого на себя любое число раз так же, как и при операциях с обычными числами. Однако трудно найти показатель степени, в которую нужно возвести заданное число, чтобы получить другое, тоже заданное. В общем случае эта задача дискретного логарифмирования кажется более трудной, чем разложение больших чисел на простые сомножители, на основании чего можно предположить, что сложности вскрытия систем RSA и ЭльГамаля будут сходными. С точки зрения практической реализации, как программным, так и аппаратным способом ощутимой разницы между этими двумя стандартами нет. Однако в криптостойкости они заметно различаются. Если рассматривать задачу разложения произвольного целого числа длиной в 512 бит на простые множители и задачу логарифмирования целых чисел по 512 бит, вторая задача, по оценкам математиков, несравненно сложнее первой. Однако есть одна особенность. Если в системе, построенной с помощью алгоритма RSA, криптоаналитику удалось разложить открытый ключ N одного из абонентов на два простых числа, то возможность злоупотреблений ограничивается только этим конкретным

пользователем. В случае же системы, построенной с помощью алгоритма ЭльГамаля, угрозе раскрытия подвергнутся все абоненты криптографической сети. Кроме того, упомянутые выше Ленстра и Манасси не только поколебали стойкость RSA, разложив девятое число Ферма на простые множители за неприлично короткое время, но и, как было замечено некоторыми экспертами, указали "брешь" в способе ЭльГамаля. Дело в том, что подход, применявшийся при разложении на множители девятого числа Ферма, позволяет существенно усовершенствовать методы дискретного логарифмирования для отдельных специальных простых чисел. То есть тот, кто предлагает простое P для алгоритма ЭльГамаля, имеет возможность выбрать специальное простое, для которого задача дискретного логарифмирования будет вполне по силам обычным ЭВМ.

Следует заметить, что этот недостаток алгоритма ЭльГамаля нефатален. Достаточно предусмотреть процедуру, гарантирующую случайность выбора простого P в этой системе, и тогда только что высказанное возражение теряет силу. Стоит отметить, что чисел специального вида, ослабляющих метод ЭльГамаля, очень мало и случайным их выбором можно пренебречь.

2.4 Открытое распределение ключей

Пока преимущества методов шифрования с открытым ключом не были очевидны. Однако на их основе легко решать задачу выработки общего секретного ключа для сеанса связи любой пары пользователей информационной системы. Еще в 1976 году Диффи и Хеллман предложили для этого протокол открытого распределения ключей. Он подразумевает независимое генерирование каждым из пары связывающихся пользователей своего случайного числа, преобразование его посредством некоторой процедуры, обмен преобразованными числами по открытому каналу связи и вычисление общего секретного ключа на основе информации, полученной в процессе связи от партнера. Каждый такой ключ существует только в течение одного сеанса связи или даже части его.

Таким образом, открытое распределение ключей позволяет каждой паре пользователей системы самим выработать свой общий секретный ключ, упрощая тем процедуру распределения секретных ключей. Хотя все не так просто - отсутствие у абонентов перед сеансом связи заблаговременно распределенного общего секретного ключа в принципе не дает им возможности удостовериться в подлинности друг друга при помощи обмена сообщениями по открытому каналу. Например, пересылать ключи можно и по описанному выше алгоритму ЭльГамаля в модификации Шамира, но как убедиться в том, что имеешь дело с партнером, а не перехватчиком? Для подтверждения подлинности каждый из участников секретной сети все же должен иметь собственный секретный ключ, известный только ему и отличающий его от всех других абонентов. В этом случае алгоритмом Диффи-Хеллмана будет обеспечена такая процедура предъявления пароля, что его многократное использование не снижало надежности доказательства подлинности владельца. В результате две функции общего секретного ключа, обычно доставляемого по секретному каналу, как защита

информации в канале связи от третьей стороны и подтверждение подлинности каждого из абонентов партнеру, разделяются. Алгоритм открытого распределения ключей Диффи-Хеллмана выглядит так:

1) Пусть имеются два абонента открытой сети A и B, знающие пару открытых ключей P и D. Кроме того, у A есть секретный ключ X из интервала (1, N), а у B есть секретный ключ Y из того же интервала.

2) Абонент A посылает B шифровку своего ключа Z'=D**X MOD P, а абонент B посылает A шифровку своего ключа Z''=D**Y MOD P.

3) После этого общий ключ Z они вычисляют как Z=Z'**Y =Z''**X.

При помощи специальных приемов время формирования общего ключа в системе Диффи-Хеллмана может быть сокращено в 5 раз по сравнению с системой ЭльГамаля в модификации Шамира, и в 30 раз по сравнению с RSA при том же уровне стойкости. Это, с точки зрения большинства практических приложений, оказывается заметным преимуществом, так как шифрование и расшифровывание по алгоритму RSA примерно в тысячу раз медленнее классических алгоритмов типа DES. Отметим, что для многих применений криптографических систем с открытым ключом время вычислений при криптографических преобразованиях не имеет большого значения. Например, при идентификации пользователей по кредитным карточкам не будет разницы, потребует ли она одну микросекунду или одну секунду. То же относится и к выбору общего ключа шифрования для другой, более быстродействующей, но не обладающей способностью обмена ключами криптографической системы.

Необходимость в системах открытого распределения ключей иметь заранее распространенные из центра индивидуальные секретные пароли для подтверждения подлинности пользователей не выглядит столь уж обременительной задачей, как изготовление и распределение из центра пар секретных ключей для связи абонентов меж собой. Срок действия такого пароля может быть существенно больше, чем срок действия ключа для связи, скажем год, а их общее число в сети связи равно числу абонентов. Кроме того, при некоторый видах связи, подтверждение подлинности партнера может достигаться за счет узнавания его по физическим признакам.

К началу восьмидесятых годов криптологи пришли к пониманию преимущества так называемых гибридных систем, в которых процедуры шифрования с открытым ключом используются лишь для передачи ключей и цифровой подписи, а информация, которую нужно передать, защищается классическим алгоритмом типа DES, ключ для которого передан с помощью шифрования с открытым ключом. Первым серийным устройством данного типа был Datacryptor фирмы RacalMilgo, выпущенный в 1979 году. Аппарат управления ключами шифрования Datacryptor предназначен в основном для правительственных сетей связи и аттестован на соответствие английскому стандарту защиты не секретной, но важной информации.

В нем предусмотрены сигнализация о нарушениях криптографических требований и извещения об ошибках. В этом аппарате используется алгоритм установления шифрованной связи при помощи выработки и передачи общего секретного ключа по алгоритму RSA. В дальнейшем аппаратов подобного типа для защиты информации было выпущено очень много.

3 КВАНТОВАЯ КРИПТОГРАФИЯ

Базовой задачей криптографии является шифрование данных и аутентификация отправителя. Это легко выполнить, если как отправитель, так и получатель имеют псевдослучайные последовательности бит, называемые ключами. Перед началом обмена каждый из участников должен получить ключ, причем эту процедуру следует выполнить с наивысшим уровнем конфиденциальности, так чтобы никакая третья сторона не могла получить доступ даже к части этой информации. Задача безопасной пересылки ключей может быть решена с помощью квантовой рассылки ключей QKD (Quantum Key Distribution). Надежность метода зиждется на нерушимости законов квантовой механики. Злоумышленник не может отвести часть сигнала с передающей линии, так как нельзя поделить электромагнитный квант на части. Любая попытка злоумышленника вмешаться в процесс передачи вызовет непомерно высокий уровень ошибок. Степень надежности в данной методике выше, чем в случае применения алгоритмов с парными ключами (например, RSA). Здесь ключ может генерироваться во время передачи по совершенно открытому оптическому каналу. Скорость передачи данных при этой технике не высока, но для передачи ключа она и не нужна. По существу квантовая криптография может заменить алгоритм Диффи-Хелмана, который в настоящее время часто используется для пересылки секретных ключей шифрования по каналам связи.

Первый протокол квантовой криптографии (BB84) был предложен и опубликован в 1984 году Беннетом и Брассардом. Позднее идея была развита Экертом в 1991 году. В основе метода квантовой криптографии лежит наблюдение квантовых состояний фотонов. Отправитель задает эти состояния, а получатель их регистрирует. Здесь используется квантовый принцип неопределенности, когда две квантовые величины не могут быть измерены одновременно с требуемой точностью. Так поляризация фотонов может быть ортогональной, диагональной или циркулярной. Измерение одного вида поляризации рэндомизует другую составляющую. Таким образом, если отправитель и получатель не договорились между собой, какой вид поляризации брать за основу, получатель может разрушить посланный отправителем сигнал, не получив никакой полезной информации.

Отправитель кодирует отправляемые данные, задавая определенные квантовые состояния, получатель регистрирует эти состояния. Затем получатель и отправитель совместно обсуждают результаты наблюдений. В конечном итоге со сколь угодно высокой достоверностью можно быть уверенным, что переданная и принятая кодовые последовательности тождественны. Обсуждение результатов касается ошибок, внесенных шумами или злоумышленником, и ни в малейшей мере не раскрывает содержимого переданного сообщения. Может обсуждаться четность сообщения, но не отдельные биты. При передаче данных контролируется поляризация фотонов. Поляризация может быть ортогональной (горизонтальной или вертикальной), циркулярной (левой или правой) и диагональной (45 или 135^0).

В качестве источника света может использоваться светоизлучающий диод или лазер. Свет фильтруется, поляризуется и формируется в виде коротких импульсов малой интенсивности. Поляризация каждого импульса модулируется

отправителем произвольным образом в соответствии с одним из четырех перечисленных состояний (горизонтальная, вертикальная, лево- или право-циркулярная).

Получатель измеряет поляризацию фотонов, используя произвольную последовательность базовых состояний (ортогональная или циркулярная). Получатель открыто сообщает отправителю, какую последовательность базовых состояний он использовал. Отправитель открыто уведомляет получателя о том, какие базовые состояния использованы корректно. Все измерения, выполненные при неверных базовых состояниях, отбрасываются. Измерения интерпретируются согласно двоичной схеме: лево-циркулярная поляризация или горизонтальная - 0, право-циркулярная или вертикальная - 1. Реализация протокола осложняется присутствием шума, который может вызвать ошибки. Вносимые ошибки могут быть обнаружены и устранены с помощью подсчета четности, при этом один бит из каждого блока отбрасывается. Беннет в 1991 году предложил следующий протокол.

1. Отправитель и получатель договариваются о произвольной перестановке битов в строках, чтобы сделать положения ошибок случайными.
2. Строки делятся на блоки размера k (k выбирается так, чтобы вероятность ошибки в блоке была мала).
3. Для каждого блока отправитель и получатель вычисляют и открыто оповещают друг друга о полученных результатах. Последний бит каждого блока удаляется.
4. Для каждого блока, где четность оказалась разной, получатель и отправитель производят итерационный поиск и исправление неверных битов.
5. Чтобы исключить кратные ошибки, которые могут быть не замечены, операции пунктов 1-4 повторяются для большего значения k.
6. Для того чтобы определить, остались или нет необнаруженные ошибки, получатель и отправитель повторяют псевдослучайные проверки:
    - Получатель и отправитель открыто объявляют о случайном перемешивании позиций половины бит в их строках.
    - Получатель и отправитель открыто сравнивают четности. Если строки отличаются, четности должны не совпадать с вероятностью 1/2.
    - Если имеет место отличие, получатель и отправитель, использует двоичный поиск и удаление неверных битов.
    - Если отличий нет, после m итераций получатель и отправитель получают идентичные строки с вероятностью ошибки 2^{-m}.

Схема реализация однонаправленного канала с квантовым шифрованием показана на рис. 3.1. Передающая сторона находится слева, а принимающая - справа. Ячейки Покеля служат для импульсной вариации поляризации потока квантов передатчиком и для анализа импульсов поляризации приемником. Передатчик может формировать одно из четырех состояний поляризации (0, 45, 90 и 135 градусов). Собственно передаваемые данные поступают в виде управляющих сигналов на эти ячейки. В качестве канала передачи данных может использоваться

оптическое волокно. В качестве первичного источника света можно использовать и лазер.

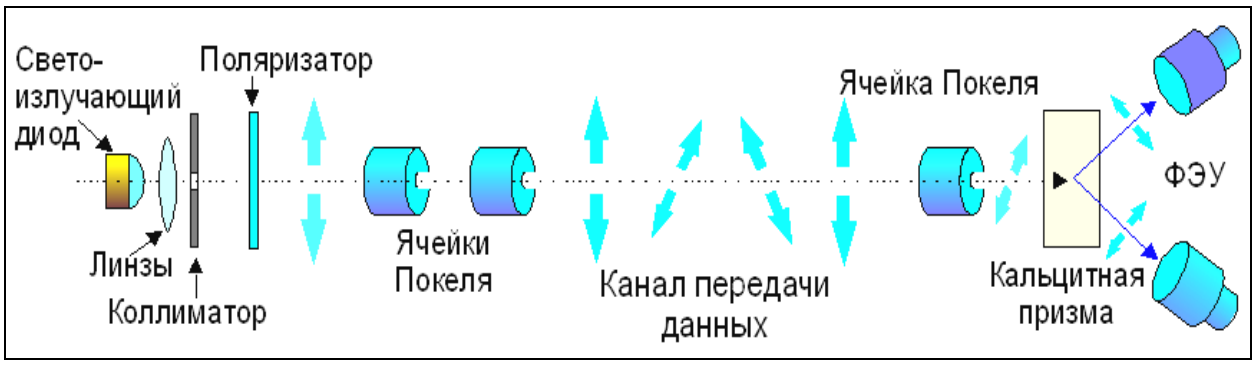

Рисунок. 3.1 - Практическая схема реализации идеи квантовой криптографии

На принимающей стороне после ячейки Покеля ставится кальцитовая призма, которая расщепляет пучок на два фотодетектора (ФЭУ), измеряющие две ортогональные составляющие поляризации. При формировании передаваемых импульсов квантов приходится решать проблему их интенсивности. Если квантов в импульсе 1000, есть вероятность того, что 100 квантов по пути будет отведено злоумышленником на свой приемник. Анализируя позднее открытые переговоры между передающей и принимающей стороной, он может получить нужную ему информацию. В идеале число квантов в импульсе должно быть около одного. Здесь любая попытка отвода части квантов злоумышленником приведет к существенному росту числа ошибок у принимающей стороны. В этом случае принятые данные должны быть отброшены и попытка передачи повторена. Но, делая канал более устойчивым к перехвату, мы в этом случае сталкиваемся с проблемой "темнового" шума (выдача сигнала в отсутствии фотонов на входе) приемника (ведь мы вынуждены повышать его чувствительность). Для того чтобы обеспечить надежную транспортировку данных логическому нулю и единице могут соответствовать определенные последовательности состояний, допускающие коррекцию одинарных и даже кратных ошибок.

Дальнейшего улучшения надежности криптосистемы можно достичь, используя эффект EPR (Binstein-Podolsky-Rosen). Эффект EPR возникает, когда сферически симметричный атом излучает два фотона в противоположных направлениях в сторону двух наблюдателей. Фотоны излучаются с неопределенной поляризацией, но в силу симметрии их поляризации всегда противоположны. Важной особенностью этого эффекта является то, что поляризация фотонов становится известной только после измерения. На основе EPR Экерт предложил крипто-схему, которая гарантирует безопасность пересылки и хранения ключа. Отправитель генерирует некоторое количество EPR фотонных пар. Один фотон из каждой пары он оставляет для себя, второй посылает своему партнеру. При этом, если эффективность регистрации близка к единице, при получении отправителем значения поляризации 1, его партнер зарегистрирует значение 0 и наоборот. Ясно, что таким образом партнеры всякий раз, когда требуется, могут получить идентичные псевдослучайные кодовые последовательности. Практически реализация данной схемы проблематична из-за низкой эффективности регистрации и измерения поляризации одиночного фотона.

Неэффективность регистрации является платой за секретность. Следует учитывать, что при работе в однофотонном режиме возникают чисто квантовые эффекты. При горизонтальной поляризации (H) и использовании вертикального поляризатора (V) результат очевиден - фотон не будет зарегистрирован. При 45^0 поляризации фотона и вертикальном поляризаторе (V) вероятность регистрации 50%. Именно это обстоятельство и используется в квантовой криптографии. Результаты анализа при передаче двоичных разрядов представлены в таблице 3.1. Здесь предполагается, что для передатчика логическому нулю соответствует поляризация V, а единице - $+45^0$, для принимающей стороны логическому нулю соответствует поляризация -45^0, а единице - H.

Таблица 3.1

Передаваемый бит	1	0	1	0
Поляризация передачи	$+45^0$	V	$+45^0$	V
Поляризация приема	-45^0	-45^0	H	H
Биты кода на приеме	0	0	1	1
Результат приема	-	-	+	-

Понятно, что в первой и четвертой колонке поляризации передачи и приеме ортогональны и результат детектирования будет отсутствовать. В колонках 2 и 3 коды двоичных разрядов совпадают и поляризации не ортогональны. По этой причине с вероятностью 50% может быть позитивный результат в любом из этих случаев (и даже в обоих). В таблице предполагается, что успешное детектирование фотона происходит для случая колонки 3. Именно этот бит становится первым битом общего секретного ключа передатчика и приемника.

Однофотонные состояния поляризации более удобны для передачи данных на большие расстояния по оптическим кабелям. Такого рода схема показана на рисунке 3.2 (алгоритм B92; R. J. Hughes, G. G. Luther, G. L. Morgan, C. G. Peterson and C. Simmons, "Quantum cryptography over optical fibers", Uni. of California, Physics Division, LANL, Los Alamos, NM 87545, USA).

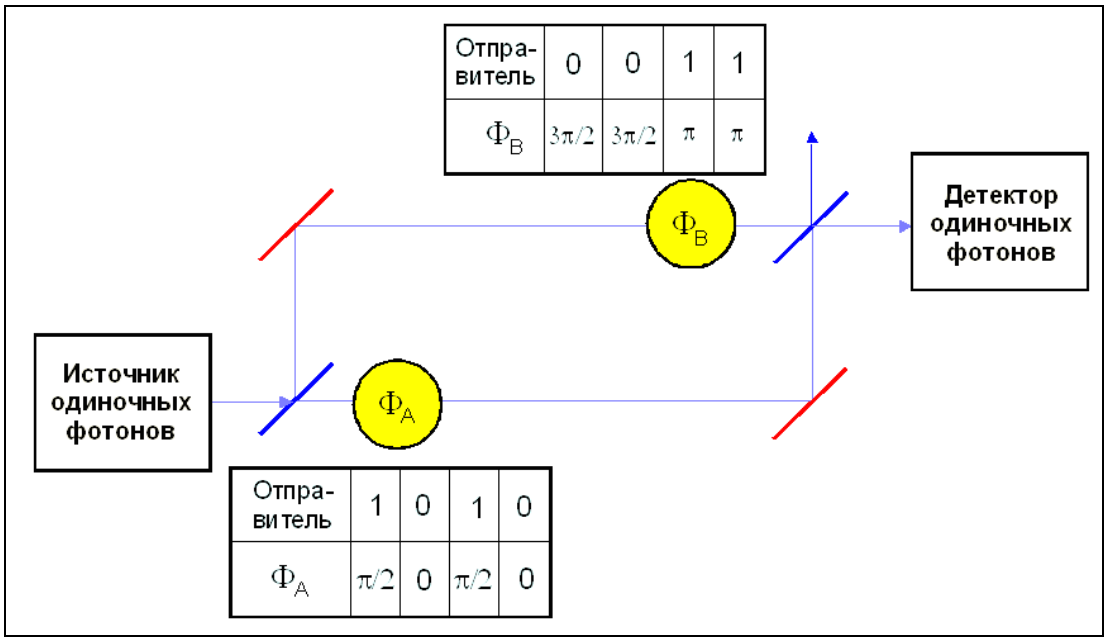

Рисунок 3.2- Реализация алгоритма B92

В алгоритме B92 приемник и передатчик создают систему, базирующуюся на интерферометрах Маха-Цендера. Отправитель определяет углы фазового сдвига, соответствующие логическому нулю и единице ($\Phi_A=\pi/2$), а приемник задает свои фазовые сдвиги для логического нуля ($\Phi_B=3\pi/2$) и единицы ($\Phi_B=\pi$). В данном контексте изменение фазы 2π соответствует изменению длины пути на одну длину волны используемого излучения.

Хотя фотоны ведут себя при детектировании как частицы, они распространяются как волны. Вероятность того, что фотон, посланный отправителем, будет детектирован получателем равна

$$P_D = \cos^2\{(\Phi_A - \Phi_B)/2\}$$

и характеризует интерференцию амплитуд волн, распространяющихся по верхнему и нижнему путям (см. рис. 3.2). Вероятность регистрации будет варьироваться от 1 (при нулевой разности фаз) до нуля. Здесь предполагается, что отправитель и получатель используют фазовые сдвиги (Φ_A, Φ_B) = (0, $3\pi/2$) для нулевых бит и (Φ_A, Φ_B) = ($\pi/2$, π) для единичных битов (для алгоритма BB84 используются другие предположения).

Для регистрации одиночных фотонов, помимо ФЭУ, могут использоваться твердотельные лавинные фотодиоды (германиевые и InGaAs). Для понижения уровня шума их следует охлаждать. Эффективность регистрации одиночных фотонов лежит в диапазоне 10-40%. При этом следует учитывать также довольно высокое поглощение света оптическим волокном (~0,3-3ДБ/км). Схема интерферометра с двумя волокнами достаточно нестабильна из-за разных свойств транспортных волокон и может успешно работать только при малых расстояниях. Лучших характеристик можно достичь, мультиплексируя оба пути фотонов в одно волокно [3, 4] (см. рис. 3.3).

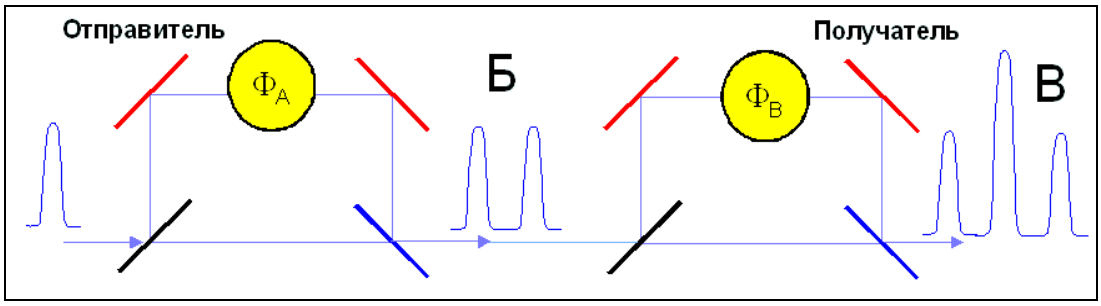

Рисунок 3.3 - Интерферометр с одним транспортным волокном

В этом варианте отправитель и получатель имеют идентичные неравноплечие интерферометры Маха-Цендера (красным цветом отмечены зеркала). Разность фаз длинного и короткого путей ΔT много больше времени когерентности светового источника. По этой причине интерференции в пределах малых интерферометров не происходит (Б). Но на выходе интерферометра получателя она возможна (В). Вероятность того, что фотонные амплитуды сложатся (центральный пик выходного сигнала интерферометра В) равна

$$P = (1/8)[1 + \cos(\Phi_A - \Phi_B)]$$

Следует заметить, что эта амплитуда сигнала в четыре раза меньше чем в случае, показанном на рис 3.2. Разветвители пучка (полупрозрачные зеркала) могут быть заменены на оптоволоконные объединители (coupler). Практические измерения для транспортного кабеля длиной 14 км показали эффективность генерации бита ключа на уровне 2,2 10^{-3} при частоте ошибок (BER) около 1,2%.

ВЫВОДЫ

Одним из самых опасных моментов криптологии является то, что почти удается измерить ее. Знание длины ключей, способов разложения на множители и криптоаналитических методов позволяет оценить (в отсутствии настоящей теории проектирования шифров) «коэффициент работы», необходимый для вскрытия конкретного шифра. В реальном мире у взломщика есть куда больше возможностей, чем использование одного криптоанализа. Часто успех достигается с помощью вскрытий протоколов, троянских коней, вирусов, электромагнитного контроля, шантажа и запугивания владельцев ключа, ошибок операционной системы и прикладных программ, аппаратных ошибок, ошибок пользователей, подслушивания, прикладной социологии, анализа содержимого свалок, и это далеко не все.

Высококачественные шифры и протоколы являются важными средствами, но сами по себе они не заменяют реалистичных, критических размышлений о том, что действительно нужно защитить, и как могут быть взломаны различные уровни обороны (взломщики, в конце концов, редко ограничиваются чистыми, хорошо определенными моделями научного мира).

С резким скачком производительности вычислительной техники сначала столкнулся алгоритм RSA, для вскрытия которого необходимо решать задачу факторизации. В марте 1994 была закончена длившаяся в течение 8 месяцев факторизация числа из 129 цифр (428 бит). Для этого было задействовано 600 добровольцев и 1600 машин, связанных посредством электронной почты. Затраченное машинное время было эквивалентно примерно 5000 MIPS-лет.

Прогресс в решении проблемы факторизации во многом связан не только с ростом вычислительных мощностей, но и с появлением в последнее время новых эффективных алгоритмов. (На факторизацию следующего числа из 130 цифр ушло всего 500 MIPS-лет). На сегодняшний день в принципе реально факторизовать 512-битные числа. Если вспомнить, что такие числа еще недавно использовались в программе PGP, то можно утверждать, что это самая быстро развивающаяся область криптографии и теории чисел.

29 января 1997 фирмой RSA Labs был объявлен конкурс на вскрытие симметричного алгоритма RC5. 40-битный ключ был вскрыт через 3.5 часа после начала конкурса! (Для этого даже не потребовалась связывать компьютеры через Интернет - хватило локальной сети из 250 машин в Берклевском университете). Через 313 часов был вскрыт и 48-битный ключ. Таким образом, всем стало очевидно, что длина ключа, удовлетворяющая экспортным ограничениям, не может обеспечить даже минимальной надежности.

Параллельно со вскрытием RC5 был дан вызов и столпу американской криптографии - алгоритму DES, имеющему ключ в 56 бит. И он пал 17 июня 1997 года, через 140 дней после начала конкурса (при этом было протестировано около 25% всех возможных ключей и затрачено примерно 450 MIPS-лет). Это - безусловно, выдающееся достижение, которое, очевидно, означает фактическую смерть DES как стандарта шифрования.

Совместные усилия организации EFF (Electronic Frontier Foundation) и фирмы Distributed.Net позволили установить новый рекорд по вскрытию шифров с 56-

разрядным ключом (алгоритм DES). Для этого потребовалось всего лишь 23 часа. Предыдущий рекорд, 56 часов, был установлен EFF с помощью специального компьютера "Deep Crack", сконструированного для вскрытия кода. Компания RSA Data Security, спонсировавшая третью попытку вскрытия зашифрованной по алгоритму DES информации, предложила 10 000 дол. каждому, кому удастся сделать это менее чем за 24 часа. Теперь указанную сумму получат EFF и Distributed.Net - коалиция энтузиастов-компьютерщиков. Deep Crack и сеть Distributed.Net, включающая в себя почти 100 000 ПК, решили задачу DES Challenge III за 22 часа 15 минут.

ПЕРЕЧЕНЬ ССЫЛОК

1. В. Жельников Криптография от папируса до компьютера – М.:ABF,1996

2. Брюс Шнайдер Прикладная криптография

3. C.H.Bennet, Quantum Cryptography Using Any Two Non-Orthogonal States, Phys. Rev. lett. 68, 3121 (1992).

4. http://www.cyberbeach.net/~jdwyer/quantum_crypto/quantum2.htm

5. Саломаа А. Криптография с открытым ключом: Пер. с англ. – М.:Мир, 1995. – 318 с., ил.

6. Клод Шеннон Теория связи в секретных системах

7. http://www.algolist.manual.ru

8. А. Винокуров Журнал «Монитор» №1,5 1995 /Алгоритм шифрования ГОСТ 28147-89, его использование и реализация для компьютеров платформы Intel x86.