Муниципальное бюджетное общеобразовательное учреждение «Лицей №6»

**Исследовательский проект**

Криптография и её применение

Работу выполнил:

Кривошеев Петр Андреевич,

ученик 11 «Б» класса

Руководитель:

Рябова Елена Викторовна,

учитель информатики

Рубцовск, 2022

Введение3

1. История криптографии4
   1. Первое применение преобразования иероглифов до нашей эры4
   2. Криптография на Ближнем Востоке в Золотой век ислама6
   3. Эпоха возрождения9
   4. Криптография в Новейшее время12
2. Современная криптография15
   1. Положение и основные принципы15
   2. Криптографические примитивы17
   3. Примеры современных криптографических систем19
3. Практическое применение алгоритма RSA для защиты переписки в Интернете21
   1. Начало работы21
   2. Описание связи «клиент-сервер»23
   3. Внедрение алгоритма шифрования25
   4. Результат работы28

Заключение29

Список использованной литературы30

**Введение**

Криптография — наука о математических методах обеспечения конфиденциальности (невозможности прочтения информации посторонним) и аутентичности информации (целостности, подлинности и невозможности отказа от авторства). Современная компьютерная безопасность решает широкий спектр задач — от защиты специальных государственных сетей до шифрования электронной почты на домашнем компьютере.

Применение методов криптографической защиты характерно для решения подавляющего большинства проблем безопасности. Аутентификация, шифрование данных, контроль целостности, электронная цифровая подпись — понятия, хорошо знакомые сегодня разработчикам программного обеспечения и специалистам в области кибербезопасности, но совершенно неизвестные для большинства пользователей.

Актуальность темы — в современном мире данные имеют огромную ценность как для разных организаций, так и для мошеннической сферы деятельности, потому каждый человек заинтересован в защите собственной конфиденциальности.

Объект исследования — наука криптография.

Предмет исследования — практическое применение криптографических методов обеспечения конфиденциальности.

Цель — узнать, чем занимается такая наука, как криптография, а также изучить методы шифрования данных.

Задачи исследования:

1. Узнать историю появления науки криптографии.
2. Проанализировать основные задачи, поставленные перед современной криптографией.
3. Выяснить методы обеспечения конфиденциальности.
4. **История криптографии**
   1. **Первое применение преобразования иероглифов до нашей эры**

Разные методы шифрования информации существуют столько же, сколько и методы её передачи в виде текста. Первыми случаями использования криптографии считаются преобразования текстов на камнях гробниц в Древнем Египте. Хоть они и не несли цели зашифровать в себе какую-то информацию, случаи преобразования иероглифов на усыпальницах почитаемых людей стали происходить всё чаще. Дело было не в желании скрыть что-то от других, а в желании привлечь внимание читателя, восхитить его, заставить задуматься о написанном или же придать важность тексту. Дэвид Кан в своём труде о криптографии обобщил цель первого из авторов подобного текста: «Таким образом, хотя писец применил не тайнопись, он, бесспорно, воспользовался одним из существенных элементов шифрования – умышленным преобразованием письменных символов. Это самый древний известный нам текст, который претерпел такие изменения». Дальнейшее намеренное изменение иероглифов стало иметь вполне конкретную цель: сокрытие смысла написанного послания от постороннего. Именно отсюда и начинается история криптографии как науки об обеспечении конфиденциальности. От шифрования поминальных текстов эта область научных знаний перешла в литературу и даже политику. Дэвид Кан также пишет об этом: «В классическом древнеиндийском трактате об искусстве управлять государством, написанном между 321-м и 300 гг. до нашей эры, рекомендуется, чтобы глава шпионской спецслужбы давал своим агентам задания с помощью тайнописи». Также имеются упоминания криптоанализа в Библии, когда пророк Даниил открыл тайну таинственных надписей вавилонскому царю Валтасару о скором захвате и разделе его царства. Даже в самой Библии применяются особые преобразования текста без цели сокрытия смысла написанного. Дэвид Кан заключает: «Главной причиной, очевидно, было стремление переписчика обессмертить себя путем изменения текста, который позднее будет снова тщательно переписан и позволит пронести частицу его личности через века».

* 1. **Криптография на Ближнем Востоке в Золотой век ислама**

Дальнейшее развитие криптографии нельзя назвать непрерывным. Искусство тайнописи не получало какого-либо значимого развития вплоть до VIII века нашей эры. Настоящий прорыв случился во время Исламского Ренессанса. Арабский халифат во время правления Аббасидов стал более развитым экономически, что позволило людям больше погрузиться в чтение и изучение различных наук. Люди стремились получить образование, что поощрялось. Книжный труд был достаточно тяжёлым, поскольку каждая отдельная копия любого произведения требовала ручного переписывания, дабы появиться в отдельном экземпляре. Несмотря на это, переведённые работы персидских, греческих и других учёных были доступны в каждом доме, что говорило о высоком уровне образованности населения. Учение ислама обязывало мусульман в равной степени интересоваться и получать знания во всех областях науки, что и привело к развитию многих из них. Криптография начала применяться не только в политике, но и в торговле, а также вошла в жизнь простых граждан. Именно в этот момент и в этих условиях своё зарождение получил криптоанализ – наука о дешифровке сообщений и, главным образом, выяснении ключа к зашифрованному сообщению. Лидером в данной области закрепился математик и философ Абу Юсуф Якуб ибн Исхак аль-Кинди (известен просто как Аль-Кинди). Этот учёный – создатель первого в истории метода дешифровки.

В IX веке единственными методами шифрования сообщений были перестановка и подстановка. В обоих случаях проводилась манипуляция с буквами сообщения. Перестановка – симметричный метод шифрования, т.е. требует для работы только один ключ. Данный метод шифрования создавал из сообщения анаграмму (чаще всего не имеющую смысл), чего было недостаточно для короткого сообщения из одного или двух слов вроде «Привет» или «Высокая гора» (подобрать вариант среди пары десятков или даже сотен вариантов перестановок не представляло большой сложности), но вполне подходило для более длинных сообщений, например «Войска уже подошли к городу, атаковать будем во время восхода Луны». Безопасность сообщения гарантируется тем, что вариантов перестановок его букв – бессчётное количество (в случае приведённого сообщения – 66 факториалов вариантов сообщений. Перебрать все варианты невозможно, поскольку таковых будет больше, чем атомов в видимой вселенной), но проблема этого метода – сложность расшифровки даже для получателя. Одним из самых первых приспособлений для данного шифрования является скитала, также известная как шифр Древней Спарты. Сообщение писалось на пергаменте, обмотанном вокруг цилиндра. Сообщение было читаемо лишь при наматывании данного пергамента на цилиндрический предмет такого же диаметра, как и тот, на котором сообщение писалось изначально. Без цилиндра сообщение представляло из себя лишь полоску с буквами, идущими друг за другом.



Рисунок 1 – Пример скиталы.

Альтернативой служил подстановочный метод шифрования, при котором зашифрованное сообщение может выглядеть совершенно иначе и даже не иметь тех же символов, что его расшифрованный вариант. Этот способ также является симметричным, поскольку для него применяется один и тот же алфавит подстановки, как для шифрования, так и для расшифровывания сообщений. Шифры подстановки гарантировали свою безопасность за счёт более простого способа шифрования, требующего только знание ключа. Под угрозу этот и многие другие методы попали благодаря Аль-Кинди, хорошо знавшему языки, статистику, математику, а также многие другие области науки. Он разработал способ, который описал в своём крупнейшем трактате «Манускрипт по дешифровке зашифрованных сообщений»: «Один из способов решить зашифрованное сообщение, если мы знаем язык, на котором оно написано, заключается в том, чтобы на основе другого открытого (незашифрованного) текста размером приблизительно в один лист высчитать частотность появления каждой буквы. Мы называем наиболее часто встречающуюся букву "первой", следующую за ней по своей частотности в тексте "второй", далее - "третьей", и так до тех пор, пока не будут учтены все буквы данного образца открытого текста. Затем мы смотрим зашифрованный текст, который нужно расшифровать, и также классифицируем его символы. Мы находим наиболее часто встречающийся символ и меняем его на "первую" букву из образца открытого текста. Следующий наиболее частотный символ меняется на "вторую" букву и так далее, пока мы не найдем соответствия всем символам криптограммы (шифрованного сообщения), которую мы хотим дешифровать». Этот метод был назван частотным. Данный способ дешифровки нельзя назвать идеальным, поскольку частотность символов в зашифрованном сообщении не всегда может соответствовать статистике открытого текста, как и, напротив, открытый текст может не соответствовать реальной статистике языка, но открытие Аль-Кинди сделало даже самые сложные криптографические системы того времени крайне уязвимыми и подтолкнуло учёных на поиск новых методов шифрования.

* 1. **Эпоха Возрождения**

Эпоха Возрождения ознаменовала расцвет наук и ремёсел в Италии, а шифры перешли из политики и торговли ещё и в защиту интеллектуальной собственности, вроде защиты научных открытий Галилея, например. Книга Чикко Симонетти, сотрудника тайной канцелярии папской курии, вышла в XIV веке и стала знаковым событием. В этой книге описаны шифры замены, в которых гласные буквы заменяются не одним, а несколькими знаками, что выравнивало частоту букв в тексте и затрудняло расшифровку сообщений с помощью частотного анализа. Также в книге дано описание «лозунгового» шифра: ключевая фраза, после которой пишутся остальные, «неиспользованные» буквы алфавита, на котором написана фраза. Спустя век выходит книга секретаря папы Клементия XII Габриэля де Лавинда «Трактат о шифрах», в которой впервые приводится описание гибридной системы защиты конфиденциальности, использующая одновременно кодирование и шифрование. Предложенный папским секретарем метод предполагал замену одной буквы на несколько знаков, количество которых было прямо пропорционально частоте буквы в открытом тексте. Все значимые имена, титулы и географические места было предложено шифровать отдельными специальными знаками. Так впервые был описан номенклатор.

«В 1466 году опять-таки в папскую канцелярию представляется трактат о шифрах архитектора и философа Леона Альберти, где предлагается способ маскировки сообщения в некотором безобидном вспомогательном тексте. Здесь же Альберти предлагает свой собственный шифр с нескромным названием «шифр королей». По сути, Альберти придумал многоалфавитную замену – новый вид шифрования, используемый в большинстве современных шифрсистем» – из статьи радиочастотного центра Московской Области. Многоалфавитные шифры были прорывом в области криптографии, но незначительная ошибка при написании зашифрованного сообщения могла привести к невозможности расшифровки сообщения даже для получателя, к тому же слишком большие затраты времени для работы с таким методом привели к тому, что способ не снискал популярности, поскольку уступал в скорости работы и более щадящем отношении к ошибкам номенклатору, хоть и был надёжнее. Изобретённый этим же философом позднее код с перешифровкой стал значительным опережением своего времени, поскольку начал применяться только спустя четыреста лет.

Ещё одним важным моментом криптографии Европейского Ренессанса является изобретение биграммного шифра – способа шифрования, позволяющего подставлять на место двух символов всего один. Изобретатель метода – Иоганн Трисемус, аббат из Германии. Этот способ значительно сложнее поддавался криптоанализу, чем какой-либо другой.

Дальнейшее развитие криптографии в XVII веке связано с созданием в странах Европы «чёрных кабинетов», занимавшихся копированием, чтением и, при необходимости, дешифровкой писем иностранным посольствам в разведывательных целях. Особенно стоит выделить работу «чёрного кабинета» в Вене, где процесс работы с иностранными письмами считался наиболее отлаженным в мире: в семь утра все присланные письма привозились в «чёрный кабинет», где копировались, переводились и изучались, а оригинал с поддельной печатью возвращался на почту уже через два с половиной часа.

«В XVII—XVIII веках становится все более понятно, что защита информации — не столько искусство сочинения и отгадывания изощренных шифров, сколько точная наука. Все заметнее переход криптографии из области черной магии в область чистой математики. Мы почти ничего не знаем о том, занимались ли ведущие математики того времени проблемами шифрования и дешифрования, но есть данные, что некоторые из них владели криптографией. Среди них Блез Паскаль, сделавший ряд открытий в области комбинаторики и создавший метод индуктивного доказательства; Исаак Ньютон и Готфрид Лейбниц, разработавшие дифференциальное и интегральное исчисление. Знаменитый английский философ Ф. Бекон предложил идею двоичного кодирования. Леонард Эйлер вел обширные исследования по перечислению и построению латинских квадратов, т. е. шифров многоалфавитной замены».

Все события, произошедшие с момента окончания средних веков до начала XVIII века преобразуют криптографию и окончательно помогают ей уложиться как научной дисциплине. Переход от древних изменений иероглифов и перестановок букв к решёткам, цифровым обозначениям и другим новым методам шифрования приблизили криптографию к её современному виду.

* 1. **Криптография в Новейшее время**

XVIII и первую половину XIX века считают временем застоя для криптографии. Все раннее изобретённые методы шифрования и дешифрования были достаточно эффективны для ручного письма и вполне удовлетворяли нужды того времени. Всё изменилось в конце первой половины XIX века, когда в 1844 году Сэмюэл Морзе представил миру своё творение: телеграф. Конечно же, высокая скорость передачи информации требовала и быстрой шифровки данных, чего шифровальщики, вручную делающие свою работу, дать не смогли.

Повсеместное изучение криптографии начинается в военных училищах всех стран в 80-е годы того же века, когда математик и преподаватель иностранных языков Огюст Кергоффс выпускает труд под названием «Военная криптография». Сам автор не является военным или специалистом в этой области, но его идеи о практической важности стойкого шифра и используемого ключа актуальны и сейчас. Именно в этот момент начинают применять коды с перешифровкой Леона Альберти, созданные им 400 лет назад. Также появляются и поступают в распоряжение первые механические шифровальные устройства.

XX век стал олицетворением технического прогресса, поскольку именно в эту пору происходит переход от механики к электромеханике и электронике, в том числе и связь: помимо уже известного телеграфа появилось ещё и радио. Вместе с тем, конечно же, развивается и криптография, переходя от шифров на бумаге к шифрам в передаче информации по проводам и воздуху. Именно здесь встаёт вопрос о важности обезопасить информацию не методом шифрования, а ключом. Методы стали более стандартизированными, но ключи для расшифровки сообщений отныне требуют большей сложности и бережного сохранения.

Первая Мировая война показала, как важно сохранять конфиденциальность тактической информации, даже если она доставляется быстро, по проводу. Несмотря на постоянно разрабатываемые коды каждой из воюющих сторон, противник мог знать абсолютно всю информацию о своём враге ввиду плохой сохранности ключа, поэтому поражения в битвах из-за ошибок шифровальщиков или плохой организации связи в целом были не редкостью.

1917 год считается революционным в области криптографии. Немецкий изобретатель Эдвард Хеберн разработал шифровальную машину «Enigma», ставшую эталоном. Принцип работы этого устройства перенимают до сих пор все разрабатываемые машины данного типа. Внешне похожая на печатную машинку, данное приспособление было способно создавать сообщения, расшифровка которых была непосильной задачей для многих ученых. Сама машина разрабатывалась и собиралась под строжайшим секретом, что делало невозможным изучение её работы.

Начало 1930-х предопределило области изучения криптографии: алгебра, статистика, теория вероятностей и теория чисел. Такая база для науки, конечно же, даёт понять, что криптография более не является искусством, как раньше, а отныне формируется как точная наука.

К моменту начала Второй Мировой войны многие страны имели свои аналоги шифровальных машин. Код «Энигмы» был расшифрован польским Бюро шифров, но новая версия кода для этой машины стала ещё сложнее, поэтому потягаться с немецким уровнем обеспечения конфиденциальности могли немногие. Главным конкурентом «Энигмы» стал американский М-209, которым пользовались союзники.

В послевоенные 1940-е годы во многих странах криптография стала полностью закрытой наукой. Её изучение продолжилось, а работы отныне стали передаваться и храниться в секретности. Но развитие продолжалось, новые счётные машины были созданы с основой алгоритмизации и кибернетики, а также позволяли себя программировать. Ещё большее развитие получила военная криптография.

Вновь открытой эта наука стала в 1968 году с выходом книги Дэвида Кана «Взломщики шифров». Криптография стала интересовать всё больше умов, но Агентство национальной безопасности США оказывало большое противодействие развитию такой популярности, поскольку попадание систем шифрования в руки террористов было недопустимо.

Первым примером защиты данных пользователей в интернете можно считать электронную почту PGP, созданную Филом Циммерманом в 1991 году. Название программы переводится как «неплохая приватность», что прямо показывает её главную суть: на тот момент не существовало абсолютно безопасного способа обмена информацией, но PGP позволяла шифровать данные так, чтобы никто и никогда не был способен их дешифровать без секретного ключа.

1. **Современная криптография**
   1. **Положение и основные принципы**

Всё время существования науки криптографии её специализация заходила не далее политики и военного дела, иногда проникая в торговлю и право. Тем не менее, время шло, в XX веке ручная работа шифровальщиков перешла к шифровальным машинам, что значительно ускорило время работы с данными, но всё ещё было недостаточно для шифрования «на лету», поскольку за машинами работали люди, неспособные в любое время дня и ночи за максимально короткий срок зашифровать сотни сообщений. «Так продолжалось вплоть до компьютерной революции, ознаменовавшей переход человечества в информационную эпоху. Тогда шифры стали прерогативой компьютеров, а не людей. Сегодня информация — главный ресурс и ее нужно охранять. Криптография проникла во все сферы нашей жизни: она защищает почтовые ящики, мессенджеры, мобильные приложения, финансы, даже штрих-коды в магазинах и более современные QR-коды криптозащищены». Сегодня сложно представить себе крупную Интернет-платформу или компанию, чью безопасность не курируют десятки, а то и сотни, людей.

Современная криптография больше не опирается на изменение символов. Отныне данные преобразуются в двоичные последовательности или проходят другие изменения перед шифрованием. Также отброшена основная идея метода «Неизвестный – безопасный». Алгоритмы стали общедоступными, а секретность данных отныне достигается сохранностью ключа. Каким бы набором инструментов не обладал злоумышленник, сложность вычислений и неимение секретного ключа не дадут ему получить ни крупицы исходной информации. Помимо критериев конфиденциальности и аутентичности, большую роль получила целостность данных, поскольку многие алгоритмы шифрования сегодня не способны передать частичное сообщение, поскольку работают не с исходным текстом, а его преобразованной версией. Также большую важность приобрела неотрекаемость от авторства, поскольку спекуляция информацией в интернете – частая практика среди мошенников.

Как было процитировано выше, криптография не так давно стала не только инструментом засекречивания политической и военной информации, но и методом обеспечения конфиденциальности для всех людей в мире. Связано это с работой сотен и сотен разнообразных сервисов и платформ, чьи данные на серверах могут иметь огромную ценность для злоумышленников и желающих заработать денег. Для хранения данных всё больше начало применяться шифрование, которое, впоследствии, понадобилось и для передачи данных, поскольку перехватить какую-либо важную информацию не составляло труда, но сейчас прочитать зашифрованные строки попросту невозможно ввиду высокого уровня безопасности, организованного со стороны разработчиков как аппаратного, так и программного обеспечения.

Сейчас используются криптографические системы двух типов: с симметричным ключом (обе стороны используют один ключ для работы с данными, что делает систему менее надёжной, но меньше нагружает аппаратное обеспечение) и с асимметричным ключом (для шифрования используется открытый ключ, для расшифровки – секретный). Обе имеют недостатки, главными из которых являются необходимость доверия между пользователями у симметричного метода и необходимость доверия публичному ключу у ассиметричного метода. Всё же, именно эти способы являются наиболее надёжными на данный момент.

* 1. **Криптографические примитивы**

Примитивы криптографии – это основные методы и инструменты для обеспечения безопасности в современных реалиях. Основными примитивами являются:

- Хеширование – преобразование строки в уникальную последовательность чисел, пригодную, например, для проверки целостности сообщения.

- Схема обязательства – метод привязки какого-либо действия к определённому лицу с целью зафиксировать выбранное действие и обеспечить основой принцип неотрекаемости.

- Цифровая подпись – метод обеспечения основного принципа аутентичности, подлинности авторства, исключающий возможность искажать данные от имени другого пользователя.

- Генератор псевдослучайных чисел – алгоритм, который на основе определённых правил создаёт случайные числа, использующиеся в криптографии.

- Симметричное шифрование – способ шифрования, при котором используется одинаковый ключ для работы как с исходным, так и с зашифрованным текстом.

- Асимметричное шифрование – способ шифрования, при котором имеется открытый и секретный ключ, работа которых гарантируется только в паре. Текст, зашифрованный открытым ключом, будет доступен для расшифровки только секретным.

Сами по себе примитивы не способны предоставить должный уровень безопасности, поскольку каждый из них выполняет определённую функцию. Их применяют в совокупности: так свойства примитивов суммарно могут давать высокий уровень безопасности, но всё будет зависеть от применяемых методов. Например, хэш-функция в совокупности с шифрованием способна защитить сообщение не только от прочтения, но и от подмены.

* 1. **Примеры современных криптографических систем**

Одним из основных стандартов при проектировании устройств шифрования некогда являлся симметричный алгоритм DES. Он был принят как стандарт в США в 1977 году. Это блочный шифр (разновидность симметричного шифра, разделяющий данные на блоки, остаток места в последнем блоке заполняется), чью кандидатуру поддерживали Американская ассоциация банков и Американский национальный институт стандартов. Основным удобством является основа данного стандарта: блочный шифр работает примерно похожим образом при шифровании и дешифровании, в основном меняется только порядок действий, что упрощало производство устройств для работы с этим алгоритмом. Главным свойством являлся эффект «обвала» – малейшее изменение исходного текста полностью меняет его зашифрованный вариант, в то время как изменение зашифрованного текста приводит исходный в нечитаемый вид. На момент 1977 года данному алгоритму не было равных, но в 1998 году расшифровать засекреченный этим методом текст смогли за 3 дня с помощью компьютера, впоследствии названного «EFF DES Cracker». Это подтолкнуло на создание нового стандарта шифрования для всей страны, ведь для «взлома» данного алгоритма уже в 2004-2005 году потребовался бы простой домашний компьютер.

Среди методов асимметричного шифрования наиболее популярным стоит выделить алгоритм RSA, созданный 40 лет назад, но не утративший своей популярности и по сей день. В основе данного алгоритма лежит вычислительная сложность факторизации (разложения на множители), что при использовании больших чисел делает его крайне сложным для расшифровки третьей стороной. Главной отличительной чертой RSA является создание цифровых подписей на основе секретного ключа пользователя. Подпись, например, может ставиться на документы для дальнейшего доступа. Функция проверки подписи проверяет, соответствует ли данная подпись данному документу и открытому ключу пользователя. Открытый ключ пользователя доступен всем, так что любой может проверить подпись под данным документом. В связи с развитием вычислительной техники данный алгоритм становится всё менее пригодным для использования и, в большинстве случаев, заменяется на более новые аналоги, хотя варианты этого алгоритма с ключами размером 1024 и 2048 бит пользуются среди некоммерческих групп разработчиков-энтузиастов, поскольку алгоритм быстрый, не требует больших вычислительных мощностей, а эффективных методов его расшифровки никто не будет искать ввиду неактуальности сокрытых в нём данных, ведь все огромные транснациональные компании и крупные организации вряд ли будут применять тот же известный всем алгоритм, что и группа разработчиков бесплатного ПО с открытым исходным кодом.

Отдельно идёт развитие алгоритмов, используемых в политике, как и тысячи лет назад. Российский криптографический стандарт ГОСТ 34.10-2018 был введён в эксплуатацию 1 июня 2019 года, применяется государственными структурами как стандарт для всех методов шифрования на уровне международного сообщения и даёт описание применяемых алгоритмов как более стойких, чем применяемые ранее системы, основанные на задаче дискретного логарифмирования в мультипликативной группе простого конечного поля большого порядка, в то время как алгоритмы данного криптографического стандарта работают с вычислением дискретного логарифма в группе точек эллиптической прямой, что усиливает безопасность в сравнении с применением конечного поля. Данный стандарт требует от секретного ключа длины 512 или 1024 бит (против 56 бит у DES в 1977 году, что говорит о всё более нарастающих требованиях к мерам безопасности, хотя требования, всё же, меньше, чем у приведённого выше RSA, ведь в данном случае описываются алгоритмы с куда более сложным методом преобразования данных). «Взломать» шифры этих алгоритмов пока что не представляется возможным, хотя слабые места уже намечены.

1. **Практическое применение алгоритма RSA для защиты переписки в Интернете**
   1. **Начало работы**

Изучив тему защиты данных с применением криптографии, было принято решение создать клиент-серверное приложение на языке программирования C# на платформе .NET с применением Windows Presentation Foundation для визуального оформления написанного приложения. Данный проект разделён на серверное (1 экземпляр в один момент времени) и клиентское приложение (множество экземпляров с именем и уникальным идентификатором, связываются на одном сервере) и выполняет функцию обмена сообщениями между клиентами посредством преобразования текстовой строки в битовую последовательность и отправки получившегося массива битов на сервер, обратного преобразования в строку на сервере и трансляции содержимого сообщения всем текущим участникам чата путём отправки тех же битовых последовательностей, которые, в конце концов, преобразуются в читаемое человеком сообщение на экранах всех пользователей (уточнение: новые участники чата не видят всей истории переписки, только новые сообщения, появившиеся в их присутствии).

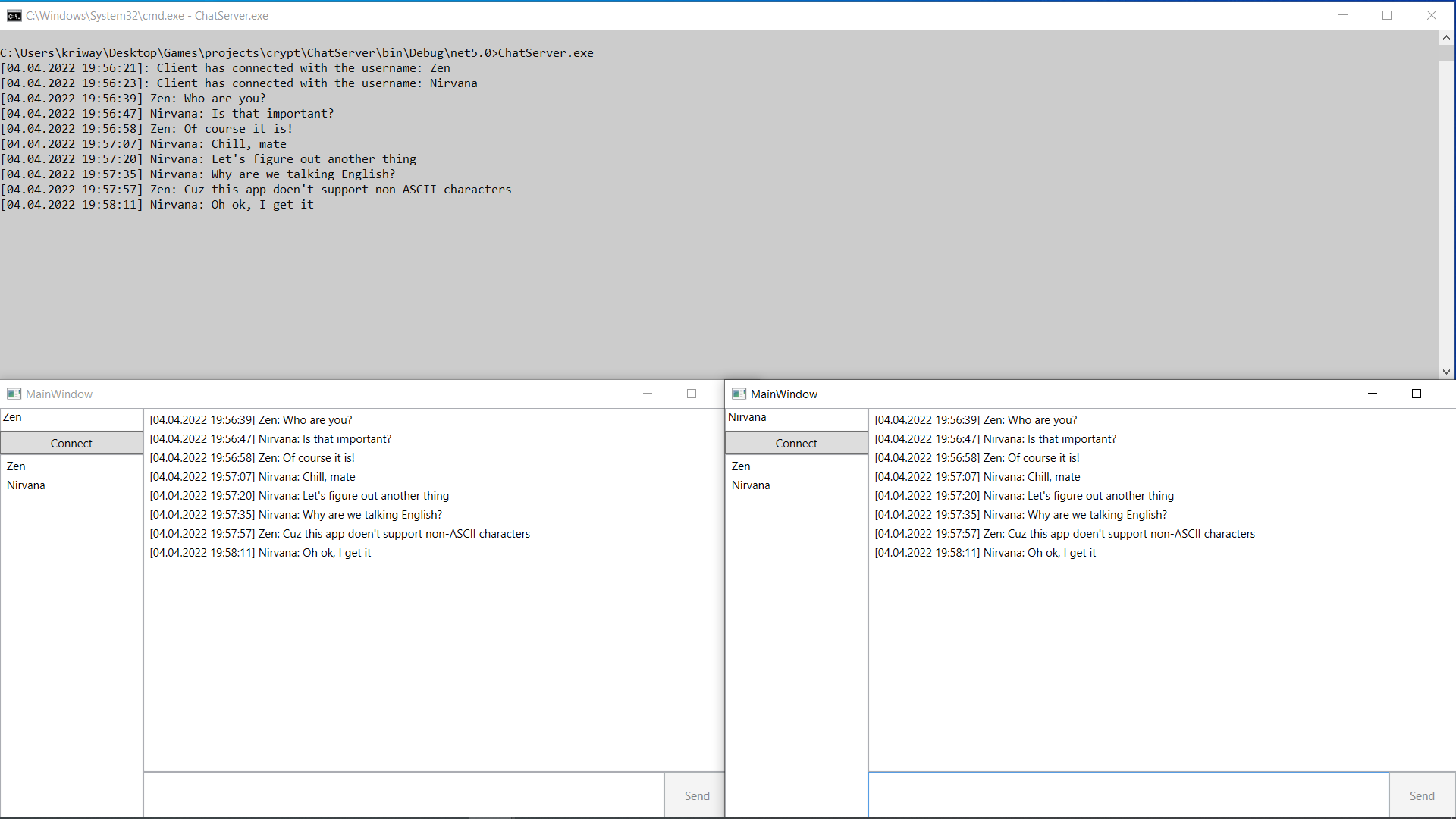


Рисунок 2 – Пример переписки двух участников чата.

На данном фото можно пронаблюдать переписку двух пользователей. Серверная часть записывает каждое действие пользователей во время сеанса, в то время как клиентская часть отображает список подключённых собеседников, сообщения (от момента подключения к серверу), а также момент выхода любого пользователя из чата. В данный момент эта система обмена сообщениями не имеет какого-либо метода защиты: сообщения передаются открытыми пакетами в виде битовых последовательностей, что крайне небезопасно, ведь вся переписка может быть прочитана просто преобразованием перехваченных пакетов битовых последовательностей в исходные сообщения. В качестве алгоритма защиты данных был выбран RSA с ключом длиной 1024 бит, так как для проекта любительского уровня этого метода защиты будет более чем достаточно.

* 1. **Описание связи «клиент-сервер»**

Процессор компьютера, очевидно, неспособен читать строки напрямую, как и отправлять их по Интернету, потому для отправки данных применяется преобразование информации в битовые последовательности, пересылаемые по интернету и преобразуемые на концах в понятные для человека строки, числа и различные аудио- и видеофайлы. В рамках своего проекта я применяю как метод создания битовых последовательностей (рис. 3), так и метод их чтения (рис. 4).

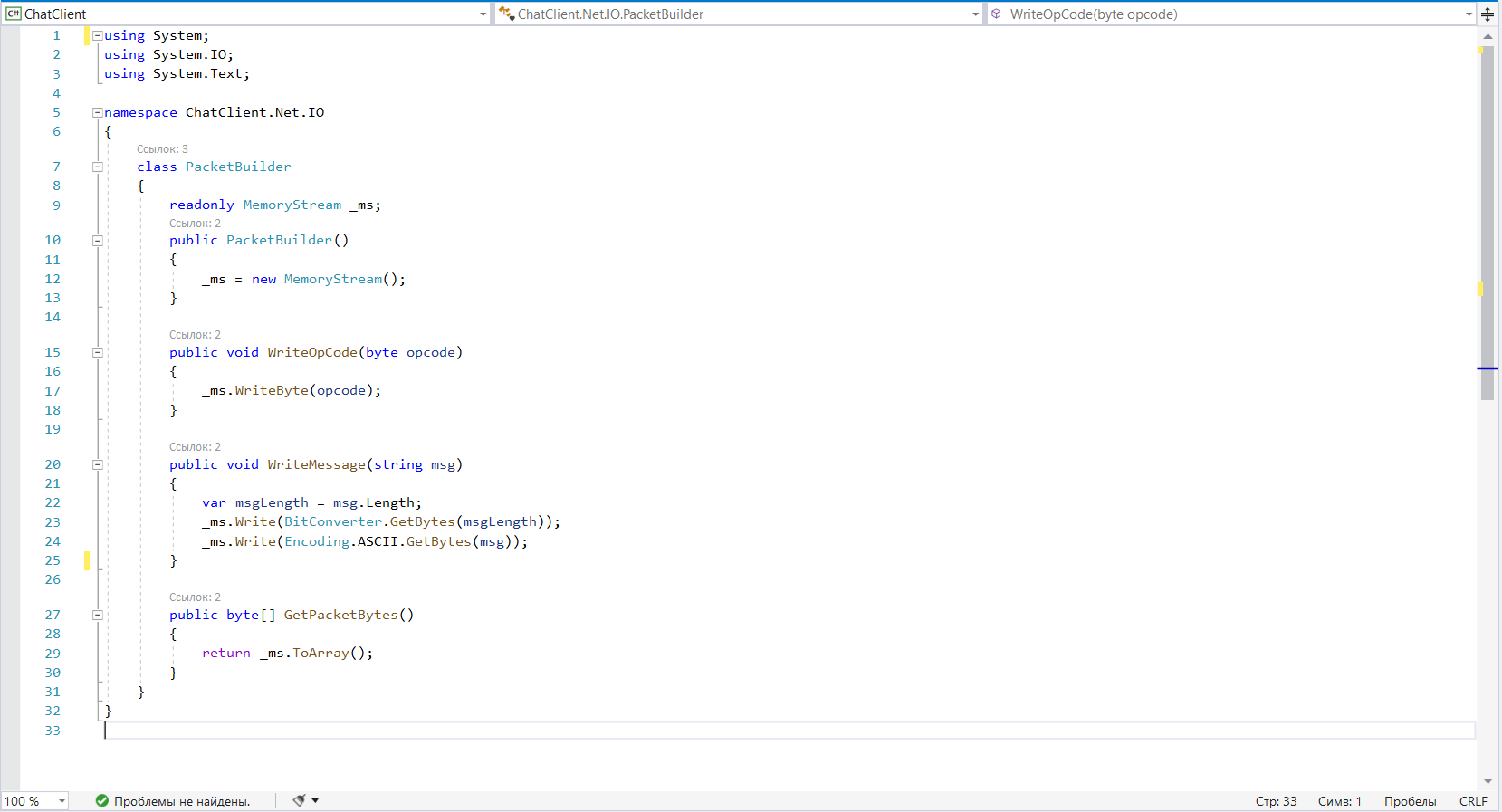


Рисунок 3 – Код для «построения» пакетов с битовыми последовательностями.

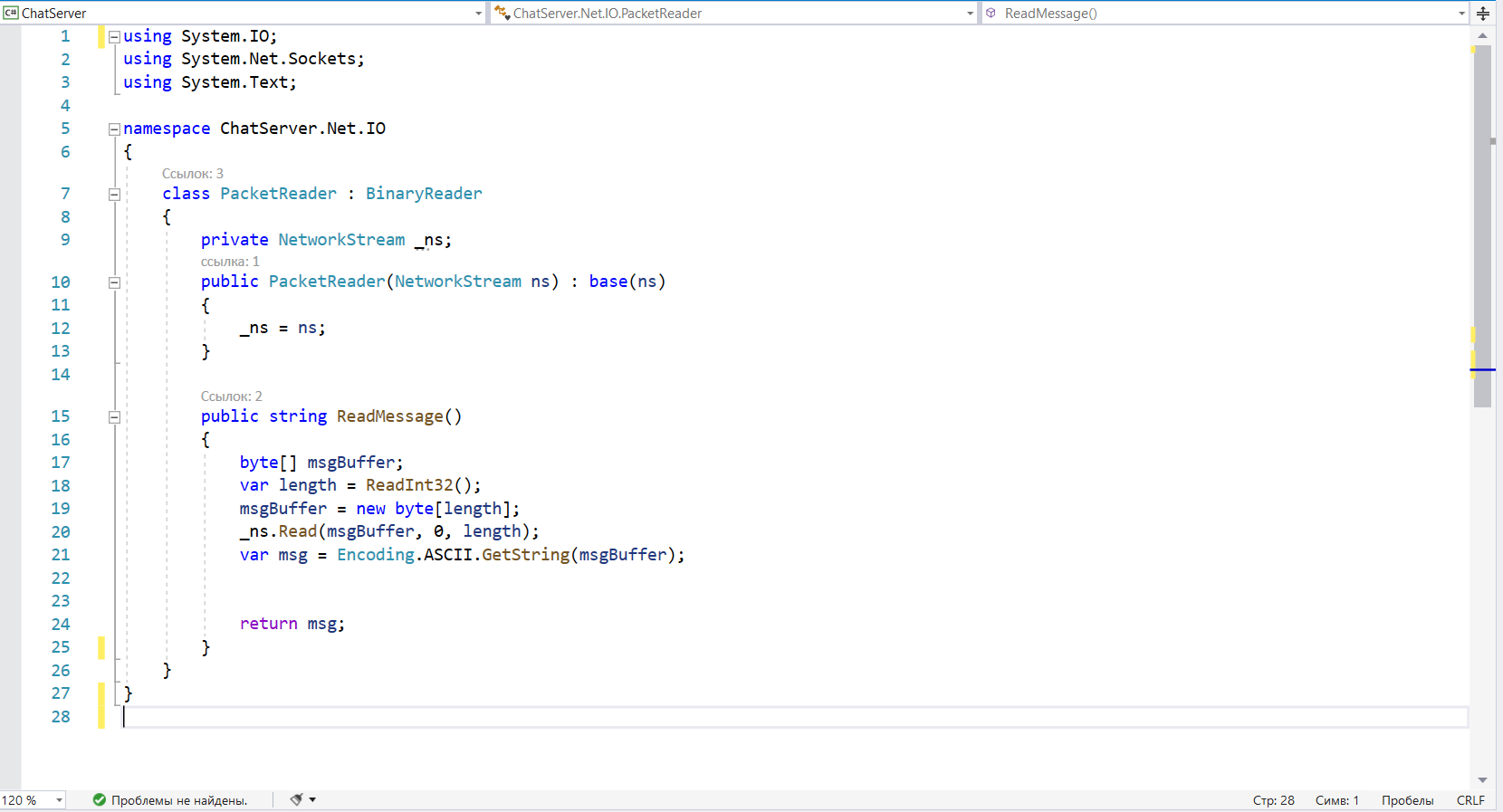


Рисунок 4 – Код для «чтения» битовых последовательностей.

На изображении 3 показан класс для создания «пакетов», отправляемых между участниками сети (сервер и клиент). Данный класс способен записать в виде битов код операции (целое число, которое указывает серверу на метод обработки последующего «пакета») и сообщение, а также вернуть массив битовой последовательности, который и является пакетом, отправляемым серверу пользователем или пользователю сервером. Изображение 4 показывает класс для «чтения» получаемых сообщений, но он имеет только один метод, который преобразует биты обратно в строку. Для корректной работы системы такой код имеют как серверная, так и клиентская часть, причём он абсолютно одинаков как в первом, так и во втором случае. На изображениях видно, что с битовой последовательностью не происходит никаких преобразований для защиты данных от прочтения посторонними, только стандартный перевод информации из одного вида в другой.

* 1. **Внедрение алгоритма шифрования**

Работа асимметричного шифрования между двумя пользователями представляется просто: по открытому каналу передаётся открытый ключ, способный только шифровать данные, в то время как секретный остаётся только у владельца и применяется исключительно для расшифровки данных. Для работы между двумя системами – оптимальный вариант с высокой степенью надёжности, но в случае наличия сервера-посредника между компьютерами, которых может быть не два, а три или больше, задача несколько усложняется. Для установки связи между пользователем и сервером необходим обмен открытыми ключами, но не всё так просто. Выделяют два основных подхода работы с ключами: либо один открытый ключ сервера для всех, либо отдельные ключи для каждого из пользователей. В своей работе я применил первый подход с единым открытым ключом сервера для всех подключённых пользователей, что облегчит работу с кодом, при этом не очень сильно упростит работу мошенников по «взлому» шифров.

Для реализации алгоритма шифрования был создан класс Asymmetric Encryption (рис. 6), самостоятельно генерирующий и хранящий в себе значения открытого и секретного ключей с соответствующими модификаторами доступа: открытый ключ является публичным, в то время как секретный ключ – приватным. Также в данном классе находятся методы «чтения» секретного ключа (в моменты, когда ключ не используется, он зашифрован в целях дополнительной безопасности), шифровки и дешифровки информации.

Конечно же, для работы с шифрованием требуют переработки и методы создания и получения пакетов данных. Наиболее оптимальное решение: перегрузить методы, создав их копию с новыми входными аргументами.

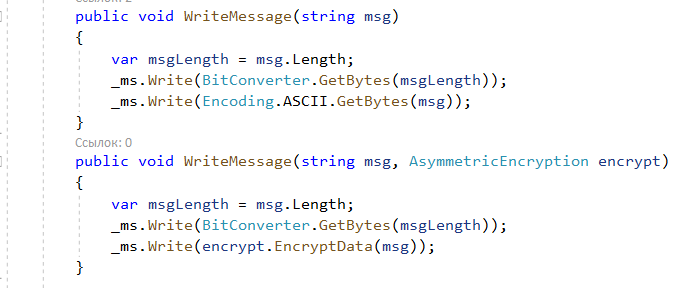


Рисунок 5 – Перегрузка метода преобразования сообщения.

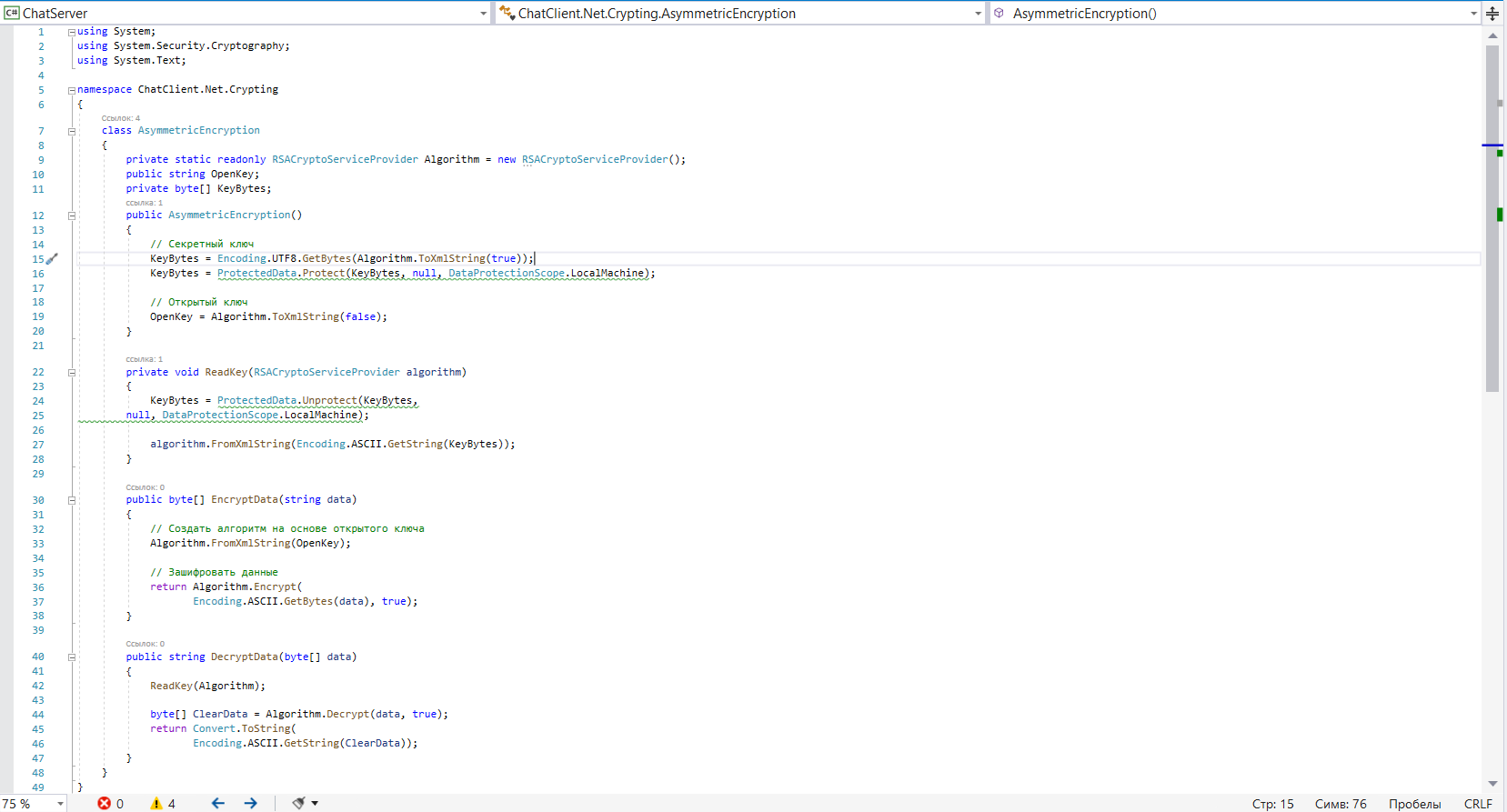


Рисунок 6 – Код класса для реализации шифрования.

И, конечно же, стоит отменить тот факт, что при подключении пользователя к серверу оба должны получить друг от друга открытый ключ, что реализуется прямой передачей без защиты данных, потому допустима только перегрузка изначальных методов, а не их полная переработка.

Такой же процесс нужно провести и с чтением пакетов: кроме обычного чтения битовой последовательности, теперь требуется ещё и дешифровка большинства сообщений, что также требует перегрузки метода.

Дополнительной обработке будут подвергнуты оба приложения, поскольку необходимо организовать хранение массива ключей на серверной стороне, а также реализовать обращение к открытому ключу каждого пользователя по уникальному идентификатору приложения.

* 1. **Результат работы**

Итак, по итогу проведённой работы было создано приложение для обмена сообщениями как между двумя людьми, так и между группой лиц. Оно не отличается разнообразным функционалом, но может быть использовано с точной гарантией того, что передаваемые сообщения защищены надёжным алгоритмом без возможности скомпрометировать секретные ключи сервера или пользователей. Приложение требует доработки, но даже в нынешнем состоянии выполняет свою функцию обеспечения связи с другими пользователями, сохраняя конфиденциальность пересылаемых данных.

**Заключение**

Применяемые сегодня методы сокрытия текста значительно отличаются от тех, что предлагались сотни и тысячи лет назад. От необходимости преобразить текст и завлечь читателя мы пришли сначала к секретности для важных политических и военных сообщений, затем к шифрованию в реальном времени, а совсем недавно – к сложнейшим криптосистемам, «взломать» которые не предоставляется возможным даже за десятки дней с применением мощнейших из возможных устройств. Менялись способы: от стеганографии к перестановкам и подстановкам знаков, от моно- и полиалфавитных шифров к математическим преобразованиям, от кодов перешифровки и ручной работы к работе с двоичными последовательностями и автоматизации безопасности. Менялась психология всей науки, когда вместо обеспечения безопасности за счёт неизвестности метода стали применять общеизвестные алгоритмы, безопасность которых строилась на неизвестности ключа и сохранности его в тайне. Даже сама наука криптография изначально была искусством сокрытия текста, а не сложной математической областью знаний, но всё изменилось с её развитием. Современная криптография обеспечивает безопасность не только для политики и торговли, но и для всех пользователей сети Интернет. Для современных криптографов важно создавать новые надёжные методы обеспечения конфиденциальности с высокой скоростью работы, что представляется непростым в свете постоянного развития компьютерной техники. Современная криптография способна обеспечить высокий уровень безопасности для любого устройства и действия за счёт множества созданных за последние 50 лет криптосистем и шифров, работа которых делает одинаково безопасным как просмотр Интернет страниц, так и хранение особо важных данных. Наука востребована и требует постоянного изучения, так что данные любого человека в интернете будут надёжно защищены, покуда он и сам озабочен об их сохранности.

**Список использованной литературы**

Кан, Д. Взломщики кодов: документальное произведение / Д. Кан; пер. А. Ключевский. – Москва: Центрополиграф, 2000. – 472 с.

Мао, В. Современная криптография: Теория и практика / В. Мао; пер. Д. А. Клюшина — Москва: Вильямс, 2005. — 768 с.

Рябко Б. Я., Фионов А. Н. Основы современной криптографии для специалистов в информационных технологиях / Б. Я. Рябко, А. Н. Фионов. — Москва: Научный мир, 2004. — 173 с.

Ухлинов Л. М. Управление безопасностью информации в автоматизированных системах / Л. М. Ухлинов. — Москва: МИФИ, 1996. — 109 с.

Эксперт | Телекоммуникации вчера, сегодня, завтра [Электронный ресурс]: многопредмет. науч. рес. / Центр анализа электромагнитной совместимости – электрон. текст. дан. – Москва: [б.и.]. - . – режим доступа к журн.: http://www.rfcmd.ru