РАЗРАБОТКА ГИБРИДНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Бочков П.А.

г. Саров, ГБПОУ СПТ им. Б.Г. Музрукова, 4 курс

Научный руководитель: Столяров И.В., преподаватель ГБПОУ СПТ им. Б.Г. Музрукова, г. Саров

Цель работы

Создать метод квантово-«золотой» криптографии, который можно отнести к классу гибридных криптосистем, и оценить точность передачи данных при программной реализации в программе, созданной по основным существующим протоколам распределения ключей: BB84, B92, 4+2, с шестью состояниями, Гольденберга-Вайдмана, Коаши-Имото и E91 (EPR).

Основные задачи

– проанализировать современные алгоритмы шифрации и дешифрации информации [1-5];

– на основе модифицированного метода «золотой» криптографии [6] создать новый квантово – «золотой» метод гибридной криптографии;

– создать модель метода;

– создать работающую версию программы, реализующую данный метод шифрации и дешифрации информации;

– оценить точность метода.

Новизна и актуальность

Квантовое распределение ключей [7] предоставляет отличную возможность передачи секретной информации по открытому каналу и при этом позволяет быть полностью уверенными в том, что ее никто не перехватит. Последние разработки в области квантовой криптографии позволяют создавать системы, обеспечивающие практически 100%-ю защиту ключа и ключевой информации [8].

«Золотая» криптография Стахова [9] основана на применении специального класса матриц, называемых матрицами Фибоначчи [10], для кодирования информации. При этом планировалось использование так называемых «золотых» матриц, элементами которых являются гиперболические функции Фибоначчи, введенные в работе [11].

В [6] был предложен модифицированный метод «золотой» криптографии, основанный на введении дополнительных целочисленных переменных, описывающих кратность применимости матричных преобразований, из которых и формируется итоговый «секретный ключ», который и будет передан в нашем методе квантово-«золотой» криптографии по квантовому каналу. Исходная информация разбивается на квадратные матрицы S на порядок 2x2 с последующим преобразованием в зашифрованное сообщение: $S \times (G_\lambda(x))^Z = C$, где $G_\lambda(x)$ – «золотые» G_λ – матрицы Фибоначчи двух непрерывных переменных λ и x, являющихся ключами для каждой четверки s_1, s_2, s_3, s_4 ; z – целочисленная переменная, задающая степень применения операции; C – зашифрованная матрица. Обратное преобразование: $C \times (G_\lambda^*(x))^Z = S$, с помощью $G_\lambda^*(x)$ – матриц, инверсных к $G_\lambda(x)$, позволяет провести дешифровку сообщения. Таким образом, для шифрования сообщения из $n = 4 * t$ (n, t – целые) значений необходим ключ из t переменных λ и t переменных x, которые размещаем в итоговой матрице вместе с зашифрованной матрицей C для отправки по открытому каналу, при этом в нашем методе квантово-«золотой» криптографии t целочисленных ключей z передаются по квантовому каналу.

Основными преимуществами данного метода квантово-«золотой» криптографии являются:

1) простота алгоритма шифрации-дешифрации, основанного на матричном умножении, что обеспечивает высокую скорость работы и задает возможность использования метода для криптографической защиты сигналов в реальном масштабе времени;

2) частая смена ключей λ и x, выбираемых по случайному закону, а также их расположения в шифрованной матрице, обеспечивают достаточно высокий уровень криптографической защиты;

3) передача ключей z по квантовому каналу обеспечит абсолютную крипкостойкость метода.

Новизна проекта состоит в отсутствии подобных программ по работе с информацией, что также подтвердил обзор Интернет-ресурсов.

Данный метод квантово – «золотой» криптографии и созданная в работе программа Kvant_Gold_Crypt могут послужить основой для создания на их основе достаточно простых с точки зрения реализации, и в тоже время быстрых и сверхнадежных криптографических систем.

Программная реализация

При создании проекта были использованы специализированные среды разработки графического интерфейса: языки объектно-

ориентированного программирования Microsoft Visual Basic 5.0 (SP2) CCE и Microsoft Visual Basic 6.0 [12].

Была разработана программа Kvant_Gold_Crypt на языке объектно-ориентированного программирования, которая осуществляет шифрование и дешифровку «дискретных сигналов», представляющих собой значения некоторой непрерывной функции. Предусмотрен ввод данных из текстового файла, состоящего из вещественных чисел, разделителем в котором может служить как пробел, так и запятая; создание ключа; зашифровка исходных данных и запись в файл для отправки. В данный файл входят не только зашифрованные данные, но и часть общего ключа, которые могут распределяться в файле по особым правилам, которые могут быть в свою очередь легко и часто изменяемы пользователем для обеспечения надежности шифрования.

Данная версия программы содержит главное меню, а также криптографическое меню для быстрого ввода команд. В итоге получаем файл для отправки по открытому каналу (зашифрованная матрица и ключи λ и x) и совсем небольшой файл, состоящий из степеней кратности матричных преобразований для отправки по квантовому каналу.

Основная часть

Основные виды криптографических систем

На данный момент существуют три вида криптосистем: симметричная, асимметричная и гибридная. Суть системы с «открытым ключом» или по-другому асимметричной криптосистемы в том, что получатель зашифрованного сообщения создаёт шифрующие и дешифрующие коды, при этом отправителю сообщения он отправляет только шифрующий ключ по открытому каналу, другой ключ остаётся известным только получателю. В симметричной криптосистеме, наоборот, и получатель, и отправитель знают ключи для шифрации и дешифрации.

Как известно, все существующие криптографические методы и алгоритмы (как «симметричные», «асимметричные») [1-5] были созданы для «идеальных условий», когда мы предполагаем, что кодировщик, канал связи и расшифровщик функционируют «идеально». Это значит, что кодировщик осуществляет «идеальное» преобразование исходного текста в шифрованный текст, канал осуществляет «идеальную» передачу зашифрованного текста, и расшифровщик осуществляет «идеальное» преобразование зашифрованного текста в исходный текст. Чтобы убедиться в том, что он не имеет ошибок, достаточно произвести его обратное преобразование в исходный текст. Однако это невозможно сделать в криптографических системах с «открытым ключом», поскольку отправитель не знает «секретного ключа». Таким образом, эти рассуждения приводят нас к выводу, что «системы с открытым ключом» обладают существенным недостатком с точки зрения обеспечения контроля криптографической системы: они наиболее уязвимы по отношению к ошибкам, которые могут возникнуть в кодировщике в процессе преобразования исходного сообщения в зашифрованный текст.

Криптосистемы с «открытым ключом» [3] наиболее часто основаны на вычислительной сложности «сложных» математических проблем, наиболее часто из области теории чисел (проблема факторизации целых чисел, проблема дискретных логарифмов, эллиптические кривые и др.). Известно, что криптографические системы с «открытым ключом» существенно «медленнее» по сравнению с системами с «симметричным ключом». Известный специалист в области криптографии Р. Молин указал на это в [5]: «Криптографические методы с публичным ключом существенно медленнее по сравнению с «симметричными» криптографическими системами».

Таким образом, можно сформулировать ряд существенных недостатков криптографических систем с «открытым ключом»:

1. Системы с «открытым ключом» требуют более сложных вычислений или большее число логических элементов при практической реализации кодировщика и расшифровщика, что порождает первый недостаток систем с «открытым ключом» – очень низкое быстродействие по сравнению с «симметричными» системами (в 1000 и более раз).

2. К сожалению, системы с «открытым ключом» являются более уязвимыми для ошибок, которые могут возникнуть в кодировщике, поскольку «отправитель» не знает «секретный ключ» и не сможет осуществить обратное преобразование зашифрованного текста в исходный текст с целью его проверки.

Как известно [5], «недостаток «асимметричных» систем состоит в том, что они значительно более медленные (в 1000 и более раз), чем «симметричные» системы. Во многих качественных системах используются оба вида криптосистем. Как говорил Р. Молин: «системы с «открытым ключом» и «симметричным ключом» могут быть использованы совместно, чтобы обеспечить

объединение эффективности «симметричного» шифрования с высокой криптографической защитой систем с «открытым ключом»[5]. При этом «публичный ключ» получателя шифрует ключ симметричного алгоритма, который используется для передачи основного сообщения. Такие комбинированные криптографические системы называются гибридными криптосистемами».

«Золотая» криптография Стахова

В последние годы в работах [9-11,13-14] «теория чисел Фибоначчи» получила дальнейшее развитие. При этом получено ряд новых приложений этой теории, имеющих прямое отношение к теории кодирования и криптографии [9]. В [11] были приведены результаты исследований по созданию нового метода криптографии, изложенного в [9] и основанного на использовании так называемых «золотых» матриц.

Под «золотыми» матрицами понимаются квадратные матрицы следующего типа:

$$Q(2x)=\begin{pmatrix} cFs(2x+1) & sFs(2x) \\ sFs(2x) & cFs(2x-1) \end{pmatrix} \quad (1)$$

$$Q(-2x)=\begin{pmatrix} cFs(2x-1) & -sFs(2x) \\ -sFs(2x) & cFs(2x+1) \end{pmatrix} \quad (2)$$

где x – непрерывная переменная, принимающая значения из множества действительных чисел, sFs(x), cFs(x) – соответственно симметричный гиперболический синус и косинус [9], задаваемые математическими выражениями:

$$sFs(x)=\frac{\tau^x-\tau^{-x}}{\sqrt{5}} \quad cFs(x)=\frac{\tau^x+\tau^{-x}}{\sqrt{5}} \quad (3)$$

$\tau=\frac{1+\sqrt{5}}{2}$ – «золотая пропорция».

Заметим, что матрицы (3), (2) обладают замечательными математическими свойствами. Матрица (2) является инверсной к матрице (1), то есть, для любого x имеет место следующее тождество:

$$Q(2x)\times Q(-2x)=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad (4)$$

Кроме того, для любого x детерминанты указанных матриц тождественно равны 1, то есть,

$$DetQ(2x)=DetQ(-2x)=1 \quad (5)$$

Следует отметить, что гиперболические функции (3), введенные в [11], являются расширением на непрерывную область так называемой формулы Бине для чисел Фибоначчи, введенной французским математиком Бине в 19-м столетии; а «золотые» матрицы (1), (2) являются обобщением Q-матрицы, введенной американским математиком Вернером Хоггаттом [13] в начале 60-х годов 20-го столетия, то есть «золотые» матрицы (1), (2) являются итогом около 200-го периода в развитии теории чисел Фибоначчи.

Суть «золотой» криптографии состоит в следующем. В качестве «криптографического ключа» используется некоторое значение переменной x. Это означает, что количество «криптографических ключей» для данного метода теоретически бесконечно. Метод может быть применен для криптографической защиты так называемых «дискретных сигналов», представляющих последовательность «отсчетов» некоторой непрерывной функции:

$$a_1,a_2,a_3,a_4,a_5,a_6,a_7,a_8,... \quad (6)$$

Шифрация сообщения состоит в последовательном представлении четверок «отсчетов» типа a1, a2, a3, a4 из (6 в виде квадратной матрицы:

$$M=\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \quad (7)$$

и последующим ее умножением на прямую «золотую» матрицу (1). При этом образуется «кодовая матрица» E,

$$M\times Q(2x)=\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}\times\begin{pmatrix} cFs(2x+1) & sFs(2x) \\ sFs(2x) & cFs(2x-1) \end{pmatrix}=\begin{pmatrix} e_{11} & e_{12} \\ e_{21} & e_{22} \end{pmatrix}=E(x), \quad (8)$$

которая представляет собой «зашифрованное сообщение», передаваемое затем по «каналу связи».

Дешифрация зашифрованного сообщения, полученного из «канала связи», состоит в умножении «кодовой матрицы» (8) на инверсную матрицу (2).

Между детерминантами исходной матрицы (7) и «кодовой матрицы» (8) существует следующая связь:

$$DetE=DetM, \quad (9)$$

что непосредственно вытекает из свойства (5).

Предложенный А.П. Стаховым метод [9] принадлежит к так называемой «симметричной» криптографии. Для передачи криптографического ключа предлагалось использовать существующие асимметричные криптографические системы, то есть криптографическая способность данного

метода определяется криптографической способностью соответствующей асимметричной системы, используемой для передачи криптографического ключа.

В работе [9] А.П. Стаховым был введен новый класс матриц, основанных на гиперболических λ – функциях Фибоначчи:

$$sF_\lambda(x)=\frac{\Phi_\lambda^x-\Phi_\lambda^{-x}}{\sqrt{4+\lambda^2}}=\frac{1}{\sqrt{4+\lambda^2}}\left(\frac{\lambda+\sqrt{4+\lambda^2}}{2}^x-\frac{\lambda+\sqrt{4+\lambda^2}}{2}^{-x}\right) \quad (10)$$

$$cF_\lambda(x)=\frac{\Phi_\lambda^x+\Phi_\lambda^{-x}}{\sqrt{4+\lambda^2}}=\frac{1}{\sqrt{4+\lambda^2}}\left(\frac{\lambda+\sqrt{4+\lambda^2}}{2}^x+\frac{\lambda+\sqrt{4+\lambda^2}}{2}^{-x}\right) \quad (11)$$

Эти матрицы названы «золотыми» G_λ – матрицами:

$$G_{0,\lambda}(x)=\begin{pmatrix} cF_\lambda(2x+1) & sF_\lambda(2x) \\ sF_\lambda(2x) & cF_\lambda(2x-1)\end{pmatrix} \quad (12)$$

$$G_{1,\lambda}(x)=\begin{pmatrix} sF_\lambda(2x+2) & cF_\lambda(2x+1) \\ cF_\lambda(2x+1) & sF_\lambda(2x)\end{pmatrix} \quad (13)$$

$$\overline{G_{0,\lambda}}(x)=\begin{pmatrix} cF_\lambda(2x-1) & -sF_\lambda(2x) \\ -sF_\lambda(2x) & cF_\lambda(2x+1)\end{pmatrix} \quad (14)$$

$$\overline{G_{1,\lambda}}(x)=\begin{pmatrix} -sF_\lambda(2x+2) & sF_\lambda(2x+1) \\ cF_\lambda(2x+1) & -sF_\lambda(2x)\end{pmatrix} \quad (15)$$

Матрицы (12 и (13) обладают следующим уникальными свойствами:

$$\det G_{0,\lambda}(x)=cF_m(2x+1)\times cF_m(2x-1)-\left[sF_m(2x)\right]^2=1 \quad (16)$$

$$\det G_{1,\lambda}(x)=sF_m(2x+2)\times sF_m(2x)-\left[cF_m(2x+1)\right]^2=-1 \quad (17)$$

Таким образом, особенность матриц (12) – (15) состоит в следующем. Во-первых, они являются функциями двух непрерывных переменных *x и* $\lambda>0$. Во-вторых, элементами матриц (12) – (15) являются гиперболические λ – функции Фибоначчи (10) и (11). В-третьих, их детерминанты не зависят от значений переменных *x* и λ и тождественно равны +1 или -1.

Модификация метода «золотой» криптографии Стахова

Модификация метода «золотой» криптографии [6] была основана на введении дополнительных целочисленных переменных, описывающих кратность применимости матричных преобразований, из которых и формируется итоговый двоичный «секретный ключ», который может быть легко преобразован по существующим ныне технологиям шифрования. Исходная информация разбивается на квадратные матрицы S порядка 2x2 с последующем преобразованием в зашифрованное сообщение:

$$S \times (G_\lambda(x))^z = C, \quad (18)$$

где $G_\lambda(x)$ – «золотые» матрицы Фибоначчи [9] двух непрерывных переменных λ и x, являющихся ключами для каждой четверки s_1, s_2, s_3, s_4 ; z – целочисленная переменная, задающая степень применения операции; C – зашифрованная матрица. Обратное преобразование:

$$C \times (G_\lambda^*(x))^z = S, \quad (19)$$

с помощью $G_\lambda^*(x)$ – матриц, инверсных к $G_\lambda(x)$ [9], позволяет провести дешифровку сообщения. Таким образом, для шифрования сообщения из n = 4*t (n, t – целые) символов необходим ключ из t переменных λ, x и z, которые мы размещаем в итоговой матрице для отправки. В ключевой «секретный» файл передаются только двоичные состояния наличия (>1) или отсутствия (= 1) кратности степени z.

Число элементов исходной матрицы S должно быть кратно четырем, в противном случае матрица добавляется нулевыми эле-

ментами. Далее она разбивается на четверки s_1, s_2, s_3, s_4, для каждой из которых определяется свои λ, x и z, которые могут быть сгенерированы автоматически (что предусмотрено в программе), или могут быть вручную введены пользователем (тоже предусмотрено в программе). Например, для матрицы S из 36 элементов необходимо определить 9 вещественных λ_i, 9 вещественных x_i и 9 целых степеней z_i, которые также помещаются в шифрованную матрицу. По последним 9 целым числам z_i определяется итоговый «секретный» ключ, который содержит только 1 или 0 (наличия (>1) или отсутствия (= 1) кратности степени z). Этот «двоичный» файл легко может быть сжат, например, в два числа – порядок системы счисления и число, в которое в данной системе счисления переведен данный «двоичный секретный» ключ.

Матрицы шифрования G_λ (x) и инверсные к ним G_λ^* (x) [9] определены для k = x – четного или нечетного, однако для непрерывной переменной x возникает проблема выбора соответствующих матриц преобразований. Эта проблема была нами решена в программе выбором матрицы для x, находящегося к ближайшему четному x, или нечетному x. Однако, как показали дополнительные исследования, можно было даже ограничиться и матрицами шифрования только типа $G_{0,\lambda}$ (x) и $G_{0,\lambda}^*$ (x); или только матрицами $G_{1,\lambda}$ (x) и $G1,_{,\lambda}^*$ (x); их применение дает достаточно высокие результаты по точности вычислений – абсолютная погрешность не ниже порядка $10^{-4} – 10^{-5}$, что подтверждается большим количеством проведенных расчетов в специально составленной для этого программе для отладки всего метода, относительная погрешность результата не превосходит $10^{-9} - 10^{-10}$.

Надежность шифрования данных может быть повышена за счет определенных закономерностей расположения данных и ключей в шифрованной матрице.

Квантово-«золотая» криптография

Если в [6] был предложен модифицированный метод «золотой» криптографии, основанный на введении дополнительных целочисленных переменных, описывающих кратность применимости матричных преобразований, из которых и формируется итоговый «секретный ключ», то в данном методе квантово-«золотой» криптографии он будет передан по квантовому каналу. Исходная информация также разбивается на квадратные матрицы S на порядок 2x2 с последующим преобразованием в зашифрованное сообщение по (21). Обратное преобразование (22) с помощью инверсных матриц, позволяет провести дешифровку сообщения.

Таким образом, для шифрования сообщения из n = 4 * t (n, t – целые) значений необходим ключ из t переменных λ и t переменных x, которые размещаем в итоговой матрице вместе с зашифрованной матрицей C для отправки по открытому каналу, при этом t целочисленных ключей z передаются нами по квантовому каналу.

Основными преимуществами данного метода являются:

1) простота алгоритма шифрации-дешифрации, основанного на матричном умножении, что обеспечивает высокую скорость работы и задает возможность использования метода для криптографической защиты сигналов в реальном масштабе времени;

2) частая смена ключей λ и x, выбираемых по случайному закону, а также их расположения в шифрованной матрице, обеспечивают достаточно высокий уровень криптографической защиты;

3) передача ключей z по квантовому каналу обеспечит абсолютную крипкостойкость метода.

В итоге получаем файл для отправки по открытому каналу и совсем небольшой файл, состоящий из степеней кратности матричных преобразований для отправки по квантовому каналу для диапазона:

1) z∈ [1;2] для протокола B92, Гольденберга-Вайдмана, Коаши-Имото;

2) z∈[1;3] для протокола E91(EPR);

3) z∈[1;4] для протокола BB84, BB84(4+2) в одном базисе;

4) z∈[1;6] для протокола с шестью состояниями.

Программная реализация метода квантово-«золотой» криптографии

Была разработана программа Kvant_Gold_Crypt на языке объектно-ориентированного программирования, которая осуществляет шифрование и дешифровку «дискретных сигналов», представляющих собой значения некоторой непрерывной функции. Предусмотрен ввод данных из текстового файла, состоящего из вещественных чисел, разделителем в котором может служить как пробел, так и запятая; создание ключа; зашифровка исходных данных и запись в файл для отправки. В данный файл входят не только зашифрованные данные, но и часть общего ключа, которые могут распределяться в файле по особым правилам, которые могут быть в свою очередь легко и часто изменяемы пользователем для обеспечения надежности шифрования.

Язык объектно-ориентированного программирования Microsoft Visual Basic 6.0, был применен для компиляции проекта и стандартного программного модуля и получения exe-файла, то есть для преобразования проекта в приложение, которое может выполняться непосредственно в среде операционной системы [12].

Отладка программы в среде Microsoft Visual Basic 6.0 (рис. 1).

Данная версия программы содержит главное меню, а также криптографическое меню для быстрого ввода команд (дополнительные наборы управляющих элементов Microsoft Windows Common Controls – элементы ToolBar и ImageList; Microsoft Common Dialog Controls – CommonDialog), а также усовершенствованные поля RichTextBox для отображения информации. Также в программе предусмотрен и полный процесс дешифровки получаемого сообщения. Для проверки работы программа содержит несколько окон, в которых легко можно наблюдать за работой программы с исходным файлом. Данные окна предназначены больше для проверки и демонстрации работы программы, в профессиональной версии программы они могут отсутствовать.

Для создания меню использовался специальный редактор меню Menu Editor (рис. 2).

Внешний вид раскрывающихся пунктов меню показан на рис. 3.

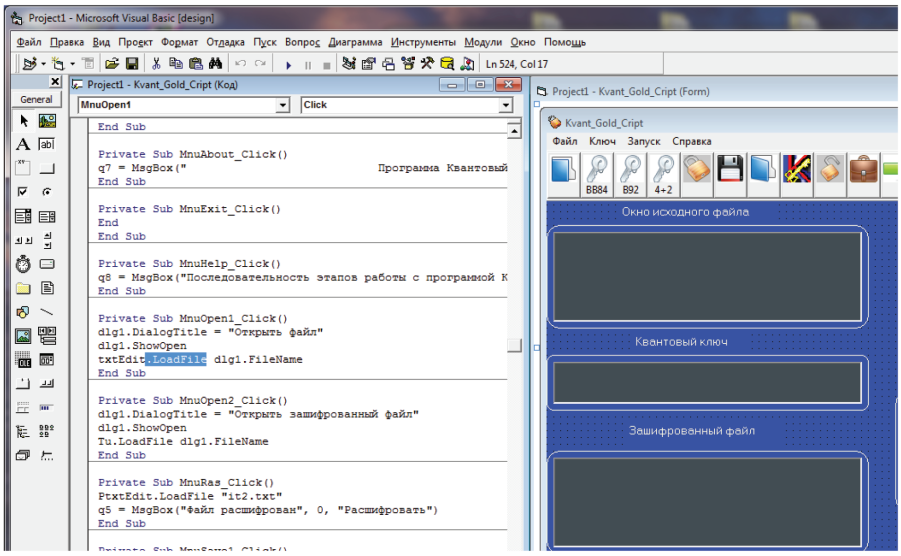

Рис. 1

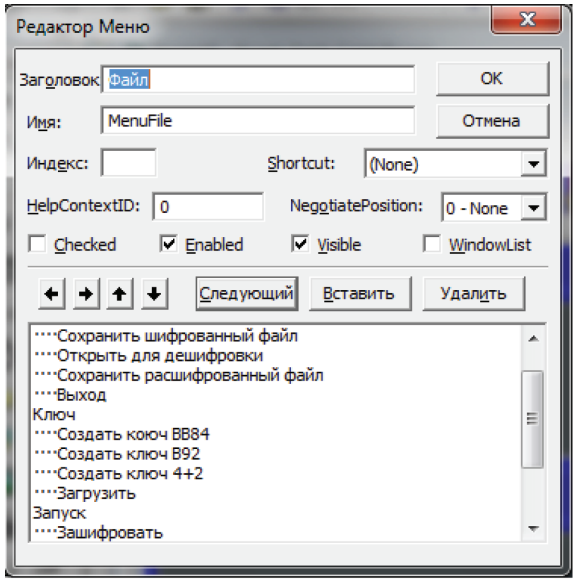

Рис. 2

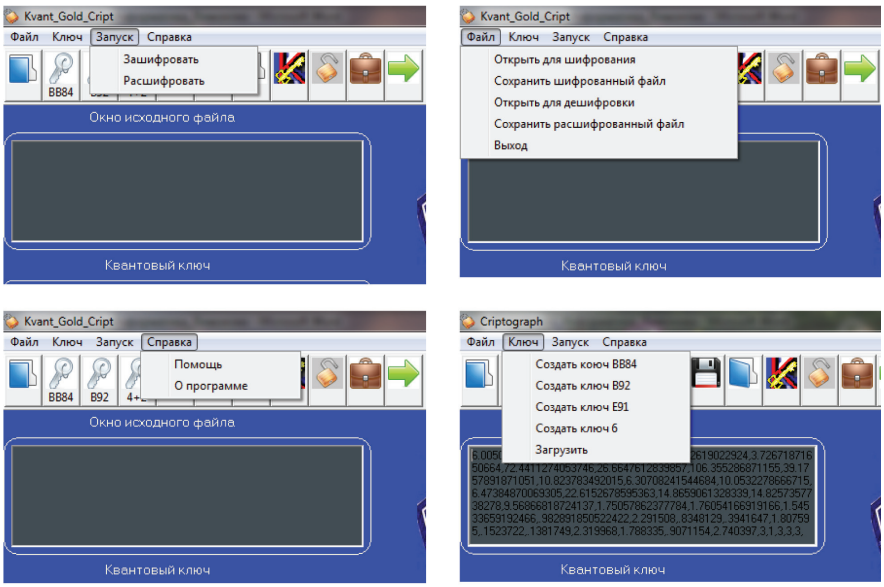

Рис. 3

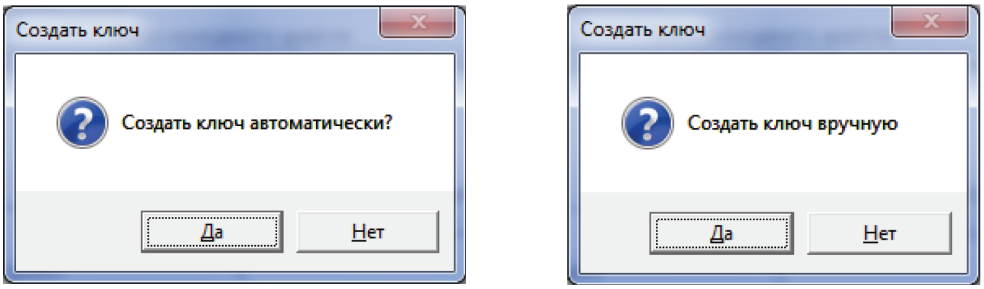

Рис. 4

Рис. 5

Для выполнения операций с файлами был использован дополнительный элемент управления Microsoft Common Dialog Controls – CommonDialog (Общий диалог), который реализовывал событийные процедуры открытия и сохранения файлов

Создание ключа также возможно автоматически, или вводом значений ключей λ, x и z вручную (рис. 4).

Криптографическое меню (дополнительные наборы управляющих элементов Microsoft Windows Common Controls – элементы ToolBar и ImageList) с всплывающей подсказкой, как, например, на рис.5 позволяет быстро вводить необходимые команды.

В итоге получаем файл для отправки по открытому каналу и совсем небольшой файл, состоящий из степеней кратности матричных преобразований для отправки по квантовому каналу для диапазона z в зависимости от выбранного протокола: BB84, B92, Гольденберга-Вайдмана, Коаши-Имото, E91(EPR), BB84(4+2) или для протокола с шестью состояниями.

Также в программе предусмотрен и полный процесс дешифровки получаемого сообщения. Для проверки работы программа содержит несколько окон, в которых легко можно наблюдать за работой программы с исходным файлом.

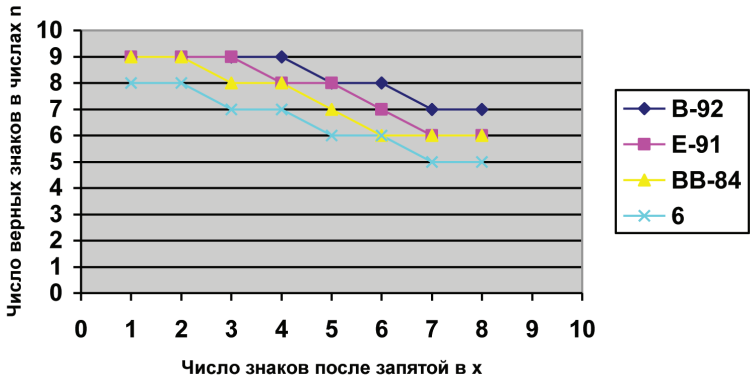

Рис. 6

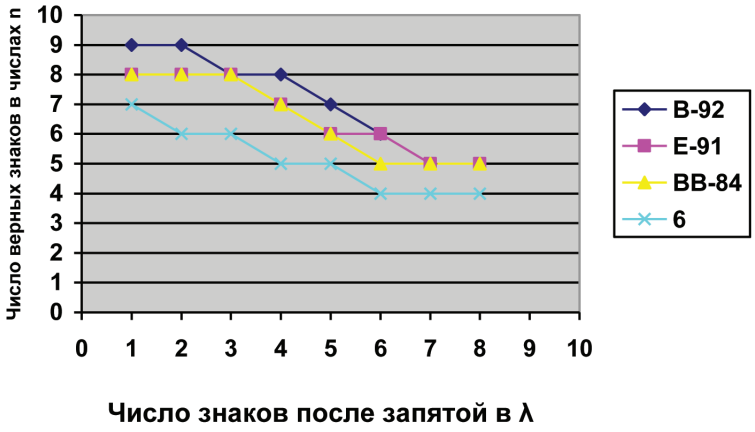

Рис. 7

Оценка точности и криптостойкости данного метода

В ходе выполнения работы была оценена операционная погрешность [16] вычислений, которая получается в результате проведения арифметических операций над числами. Для данной программы абсолютная погрешность не вычислений не превосходит 10^{-4} , что подтверждается большим количеством проведенных экспериментальных расчетов, выполненных при отладке программы, относительная погрешность результата не превосходит 10^{-9}.

При разработке данной программы была оценена абсолютная и относительная точность метода по основным существующим протоколам распределения ключей: BB84, B92, 4+2, с шестью состояниями, Гольденберга-Вайдмана, Коаши-Имото и ЭПР. Проведено тестирование на определение точности шифрования и дешифрования в различных диапазонах для переменных x и λ, определяющих кодирующие матрицы, при условии, что переменная z имеет значения в диапазоне:

1) z∈[1;2] для протокола B92, Гольденберга-Вайдмана, Коаши-Имото;

2) z∈[1;3] для протокола E91(EPR);

3) z∈[1;4] для протокола BB84, BB84(4+2) в одном базисе;

4) z∈[1;6] для протокола с шестью состояниями.

На рис. 6 приведён график зависимости числа верных знаков исходной и расшифрованной матриц n (x) при $0 < \lambda < 3$ для различных протоколов (для x по оси указывается число знаков после запятой).

На рис.7 приведён график зависимости числа верных знаков n (λ) при $0 < x < 3$ для диапазонов z аналогично рис.8.

Квантовое распределение ключей [7] предоставляет отличную возможность передачи секретной информации по открытому каналу и при этом позволяет быть полностью уверенными в том, что ее никто не перехватит. Последние разработки в области квантовой криптографии позволяют создавать системы, обеспечивающие практически 100%-ю защиту ключа и ключевой информации [8]. Учитывая характер

передаваемой информации, сложность математических преобразований и огромную трудоёмкость по возможному подбору ключей можно утверждать, что данный метод имеет широкие возможности для его использования при кодировании и передачи информации в системах реального времени. Частая смена ключей λ и x, выбираемых по случайному закону, а также их расположения в шифрованной матрице, обеспечивают достаточно высокий уровень криптографической защиты, а передача ключей z по квантовому каналу обеспечит абсолютную крипкостойкость метода.

Выводы

Все поставленные цели, а также задачи по работы были достигнуты. По окончанию работы над проектом получен новый метод криптографии и готовый программный продукт, способный работать под управлением операционной системы Windows.

Основными преимуществами данного метода квантово-«золотой» криптографии являются:

1) простота алгоритма шифрации-дешифрации, основанного на матричном умножении, что обеспечивает высокую скорость работы и задает возможность использования метода для криптографической защиты сигналов в реальном масштабе времени;

2) частая смена ключей λ и x, выбираемых по случайному закону, а также их расположения в шифрованной матрице, обеспечивают достаточно высокий уровень криптографической защиты;

3) передача ключей z по квантовому каналу обеспечит абсолютную крипкостойкость метода.

Данный метод квантово – «золотой» криптографии и программа Kvant_Crypt могут послужить основой для создания на их основе достаточно простых с точки зрения реализации, и в тоже время быстрых и сверхнадежных криптографических систем. Удобный интерфейс и оригинальный дизайн могут вызвать интерес у всех тех, кто интересуется вопросами криптографии и защиты данных.

Список литературы

1. Seberry J., Pierzyk J. Cryptography. An Introduction to Computer Security: Prentice Hall, New York-London-Toronto-Sydney-Tokyo, 1989.

2. Davies D.W., Price W.L. Security for Computer Networks. An Introduction to Data Security in Teleprocessin and Electronic Funds Transfer: John Wiley & Sons, Chichester-New York-Brisbane-Toronto-Singapure. Second Edition, 1989.

3. Diffie W. and Hellman M. E. New Directions in Cryptography. IEEE Trans. on Info. Theory, 1976, Vol. IT-22, p. 644-654.

4. Menezes A., Van Oorshot P.C. and Vanstone S.A. Handbook on Applied Cryptography: CRC Press. Boca Raton, Florida, 1999.

5. Mollin R.A. An Introduction to Cryptography. Second Sedition: CRC, Champan & Hall, 2001.S. Wiesner, «Conjugate coding», Sigact News 15, 78-88 (1983).

6. Большакова Д. Реализация модифицированного метода «золотой» криптографии. XIII Школьные Харитоновские чтения. Межрегиональная олимпиада школьников «Будущие исследователи – будущее науки». Тезисы. Саров: ФГУП «РФЯЦ-ВНИИЭФ», 2013, с.5-7.

7. Килин С. Я., Хорошко Д.Б., Низовцев А.П. Квантовая криптография: идеи и практика. Минск: Беларуская навука, 2007, 391с.

8. Румянцев К.Е., Голубчиков Д.М. Квантовая криптография: принципы, протоколы, системы. /Всероссийский конкурсный отбор обзорно-аналитических статей по приоритетному направлению «Информационно-телекоммуникационные системы»/ Таганрог: ТТИ ЮФУ, 2008. 37с.

9. Stakhov A. The «golden» matrices and a new kind of cryptography. Chaos, Solitons & Fractals, 2007, Volume 32, Issue 3, p. 1138-1146.

10. Стахов А.П. Кодирование данных, основанное на фибоначчиевых матрицах. Труды Международной конференции «Проблемы Гармонии, Симметрии и Золотого Сечения в Природе, Науке и Искусстве». Винница, 2003.

11. Stakhov A, Rozin B. On a new class of hyperbolic function. Chaos, Solitons & Fractals, 2004, Volume 23, Issue 2, p. 379-389.

12. Дан Эпплан. Win32 API и Visual Basic. СПб: Питер, 2001, 1120с.

13. Стахов А.П. Формулы Газале, новый класс гиперболических функций Фибоначчи и Люка и метод «золотой» криптографии // «Академия Тринитаризма», М., Эл № 77-6567, публ.14098, 21.12.2006 (http://www.trinitas.ru/rus/doc/0232/004a/02321063.htm)

14. Stakhov A. Fibonacci matrices, a generalization of the «Cassini formula», and a new coding theory. Chaos, Solitons & Fractals, 2006, Volume 30, Issue 1, p. 56-66.

15. Hoggat V.E. Jr. Fibonacci and Lucas Numbers. – Boston, MA: Houghton Mifflin, 1969.

16. Дьяконов В.П. Справочник по расчетам на микрокалькуляторах. М., Наука, 1989, 464с.