Муниципальное автономное общеобразовательное учреждение города Ростова-на-Дону «Школа № 30 имени Героя Советского Союза Кравцова О.Т.»

**Информационный проект**

**«Безопасный способ передачи информации. Квантовое шифрование»**

**Выполнил:** ученик 10 “А” класса

Гайворонский Станислав Константинович

**Научный руководитель:**

Учитель информатики

Воронина Любовь Александровна

Ростов-на-Дону

2021 год

**Оглавление**

**Введение**

Что такое криптография и в чем ее проблемы……………………………………………….3

Шифр Вернама………………………………………………………………………………….4

**Глава 1. Современные методы шифрования**

1.1. Шифрование открытым ключом………………………………………………………….5

1.2 Метод RSA………………………………………………………………………………….5

1.3 Главная проблема современных методов шифрования………………………………….6

**Глава 2. Квантовая криптография**

2.1 Что такое квантовая криптография и в чем ее отличие от классической криптографии…………………………………………………………………………………………...8

2.2 Суперпозиция частиц………………………………………………………………………8

2.3 Поляризация световых волн……………………………………………………………….8

2.4 Метод BB84…………………………………………………………………………………9

2.5 Проблемы метода BB84…………………………………………………………………..10

**Заключение**…………………………………………………………………………………………...11

**Источники информации**……………………………………………………………………………11

**Приложения**…………………………………………………………………………………………..13

**Введение**

**Тип проекта**: информационный

**Цель**: Выявить безопасный способ шифрования данных

**Задачи**:

* Изучить как работает шифрование
* Найти лучшие методы шифрования и изучить их работу
* Сделать безопасный способ передачи данных

**Объект**: Криптография

**Предмет**: Методы шифрования

**Методы, используемые в данной работе**:

* Изучение литературы и других источников информации
* Анализ
* Сравнение

**Что такое криптография и в чем ее проблема**

Люди с давних пор нуждались в защите своей информации, этим нелегким делом занимается такая наука, как криптография. Это древняя наука, которая пытается решить проблему шифрования информации, и в данный момент ее достижения довольно внушительны, без нее мы бы не смогли так легко общаться в интернете или что-либо покупать там, люди не хранили бы деньги на своих банковских карточках, ведь их бы просто украли.

Мною был проведен социальный опрос, в котором участвовали 200 респондентов всех возрастных групп. Главный вопрос опроса был: “На сколько % вы считаете безопасными методы шифрования, которые сегодня используются в интернете, банках, крупных кампаниях и т.д.” (см. приложение 1)

Как можно заметить, около 50% людей считают современные методы шифрования не очень безопасными, но это ошибочные выводы и сейчас мы разберемся, почему.

В классической криптографии выделяют 2 главные проблемы:

* Проблема расшифровки сообщения поиском изъянов или методом перебора
* Проблема безопасной передачи ключа

Практически все шифры имеют некоторые изъяны, используя которые и потратив много времени на расшифровку получается расшифровать код, но существуют методы шифрования, с абсолютной криптографической стойкостью, один из которых шифр Вернама.

**Шифр Вернама**

Шифр Вернама довольно прост в использовании, для него надо иметь сообщение и секретный ключ. Сообщение надо преобразовать в двоичный код. Для 100% безопасности ключ должен быть по длине равен сообщению или быть больше его, также он не должен иметь смысл или использоваться несколько раз. Дальше для каждого бита сообщения берется бит секретного ключа и происходит логическая операция “исключающее или” (см. приложение 2).

По таблице видно, что имея определенные числа в сообщении и ключе, можно получить только одну возможную цифру шифра и также наоборот. Но имея только шифр мы никак не сможем разгадать сообщение, ведь ключ может быть абсолютно любым. И если перебирать все возможные ключи, то получатся все возможные комбинации 0 и 1 в сообщении и понять какое из них является настоящим невозможно.

Но даже у этого метода есть большая проблема. Ключ должен быть и у отправителя, и у получателя для зашифровки и дешифровки, а это значит, что его надо сначала безопасно передать. В этом и заключается проблема большинства шифров. Большинства, но не всех.

**Глава 1. Современные методы шифрования**

**1.1. Шифрование открытым ключом**

Во многих современных методах шифрования используются: односторонняя функция (то есть зная X легко получить Y, но зная только Y очень сложно получить X) и открытый ключ. С односторонней функцией более менее понятно, но как можно шифровать данные через открытый ключ?

Рассмотрим ситуацию: вы хотите безопасно передать вашему товарищу книгу, для этого вы используете ящик и замок с ключами. С таким набором легко отправить книгу, кладете книгу в ящик, закрываете замком и отправляете другу, он открывает его ключом и получает книгу. Но опять возникает проблема передачи ключа, как его безопасно передать?. Совершим передачу немного по-другому.

Пусть друг отправит нам ящик с замком, мы положим книгу в ящик и захлопнем замок, а он своим ключом его откроет, если кто-то и заполучит ящик, то открыть его будет сложно и проблемы с передачей ключа не возникло. Другими словами, ваш друг отправляет вам открытый ключ, вы им шифруете сообщение, а он расшифровывает сообщение секретным ключом.

Такой метод называется шифрование открытым ключом, где открытым ключом выступает замок, а секретным - ключ от замка. Эти же инструменты использует самый популярный и широко использующийся метод шифрования RSA (Rivest, Shamir, Adleman).

**1.2. Метод RSA**

С помощью метода шифрования RSA передается и хранится вся информация в интернете, любое действие шифруется этим методом. RSA использует открытый ключ, для генерации которого используется такая односторонняя функция, как факторизация. Что это такое и как получается открытый ключ?

Факторизация – это поиск множителей, из которых составлено начальное число, к примеру факторизация числа 250: 2,5,5,5, потому, что произведение 2\*5\*5\*5 = 250. Открытый ключ на самом деле произведение двух простых чисел, эти простые числа знают только несколько лиц, которым можно доверять. Зная эти два числа, можно расшифровать сообщение, но зная только открытый ключ – нельзя.

Рассмотрим, как шифруется сообщение этим методом. Представим ситуацию: Боб хочет отправить сообщение Алисе, чтобы зашифровать сообщение методом RSA Алисе надо взять два больших простых числа A и B и перемножить их, получается открытый ключ N. Дальше надо получить функцию Эйлера (ϕ = (A-1)\*(B-1)), следующим этапом будет поиск открытой экспоненты (e), это такое простое число, на которое не должно делиться ϕ, его надо искать перебором. И последним шагом будет расчет секретной экспоненты по формуле: d = (ϕ\*k+1)/e, где k надо перебирать от 1 и до того момента пока d не будет целым. Все данные, кроме открытого ключа и открытой экспоненты (e), следует держать в строжайшем секрете.

Дальше Алиса отправляет открытый ключ и открытую экспоненту Бобу, Боб должен взять сообщение и превратить его в цифры, неважно каким методом, дальше эту последовательность Боб возводит в степень открытой экспоненты (e) и делит это число с остатком на открытый ключ.

Этот остаток и есть зашифрованное сообщение, Боб отправляет это сообщение Алисе, Алисе же предстоит это число возвести в степень секретной экспоненты и поделить с остатком на открытый ключ, что в итоге дает то самое сообщение, которое зашифровал Боб.

Если кто-то извне попытается перехватить данные, которые отправляли друг другу Алиса и Боб, то даже с такими данными не получится расшифровать сообщение, для этого необходимо знать секретную экспоненту, а ее можно рассчитать только владея информацией, на какие простые числа факторизуется открытый ключ (A и B).

**1.3. Главная проблема современных методов шифрования**

Выглядит все это надежно, но есть одна проблема – возможность запуска алгоритма факторизации на квантовых компьютерах. Квантовые компьютеры используют не обычные биты, а кубиты. Кубиты – похожи на обычные битовые ячейки, но если в битовых ячейках хранится только 0 или 1, то в кубитах хранится 0 или 1 или одновременно 0 и 1, такой эффект называется квантовой суперпозицией и позже мы его разберем. Учитывая такое дополнение логика вычислений кардинально меняется.

Благодаря этому квантовый компьютер может обрабатывать сразу все значения, в то время как обычный компьютер будет их перебирать по одному. Из-за этого квантовый компьютер в несколько миллионов раз быстрее обычного компьютера. И так как эти компьютеры очень быстрые, на них можно запустить алгоритм факторизации. Такие компьютеры уже есть, но они довольно слабые, но создание мощного квантового компьютера – это лишь вопрос времени.

И что же в таком случае делать? Придется использовать шифры устойчивые к взлому, однако проблема с передачей ключа все же осталась. Этой проблемой сейчас и занимается криптография, но классическая это сделать не в силах, поэтому на помощь приходит квантовая криптография.

**Глава 2. Квантовая криптография**

**2.1. Что такое квантовая криптография и в чем ее отличие от классической криптографии**

Если классическая криптография работает на математическом уровне, то квантовая на физическом уровне, то есть нам нужно найти такой физический процесс, который легко запустить в одном направлении, но сложно реализовать в обратном. Но какой процесс можно взять?

На ум сразу приходит разбитая тарелка, ведь разбить ее легко, а собрать обратно сложно, но собрать тарелку все же возможно, хоть и сложно. Но ученые нашли процесс, который невозможно запустить в обратную сторону, и этот процесс называется квантовая суперпозиция.

**2.2. Суперпозиция частиц**

Основа квантового шифрования – суперпозиция частиц. Частица может иметь [состояни](https://ru.wikipedia.org/wiki/%D0%A1%D0%BE%D1%81%D1%82%D0%BE%D1%8F%D0%BD%D0%B8%D0%B5_(%D0%BA%D0%B2%D0%B0%D0%BD%D1%82%D0%BE%D0%B2%D0%B0%D1%8F_%D0%BC%D0%B5%D1%85%D0%B0%D0%BD%D0%B8%D0%BA%D0%B0))я, которые не могут быть реализованы одновременно с [классической](https://ru.wikipedia.org/wiki/%D0%9A%D0%BB%D0%B0%D1%81%D1%81%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B0%D1%8F_%D1%84%D0%B8%D0%B7%D0%B8%D0%BA%D0%B0) точки зрения. К примеру, частица может одновременно находиться тут и там, крутиться по часовой и против часовой стрелки одновременно, обладать малой и большой энергией одновременно и многое другое.

По сути, суперпозицию можно сравнить с монетой, которую подбросили, но она еще летит, в этом состоянии монета одновременно и орел, и решка. Что выпадет, мы можем узнать только после падения монеты, но тогда суперпозиция просто пропадает. И вернуть точно такую же суперпозицию частице невозможно, и даже нельзя точно сказать в каком состоянии была частица до этого. И именно такие свойства и используются в квантовом шифровании.

**2.3. Поляризация световых волн**

В методе квантового шифрования, о котором я хочу рассказать также используется поляризация световых волн – раздел квантовой физики. Любой пучок света – это поперечная волна, у которой есть колебания. Причем колебания возможны по всем направлениям, но можно использовать поляризатор – это небольшая пластина, которая пропускает через себя волны, которые колеблются только в одной определенной плоскости. Поляризатор можно сравнить с секцией металлического забора с параллельными прутьями. После прохождения обычной световой волны через поляризатор, все ее колебания будут лежать в одной плоскости.

**2.4. Метод BB84**

Имея представление о суперпозиции и поляризации света, можно начать изучение квантового шифрования. Метод, который сегодня будет обсуждаться: BB84, назван в честь двух физиков Чарльза Беннета и Жиля Брассара, был придуман в 1984 году. Этот метод является самым распространенным из-за его относительной простоты: используется несложная схема и самые основные законы квантовой физики.

Суть метода состоит в передаче фотонов, которые поляризованы в конкретных направлениях, каждый из которых означает 0 или 1. Таким образом, сгенерируется секретный ключ, который будет использоваться для шифрования данных по открытым каналам связи.

Для генерации понадобятся 2 канала связи: квантовый и обычный, а также пару устройств: лазер (первичный источник света), поляризатор, пару линз и фотодетекторы (для измерения фотонов).

В генерации участвуют два человека: Алиса и Боб. Алиса будет “кодировать” фотоны и отправлять их Бобу по оптоволокну. Начнем с того, как будут “кодироваться” фотоны. Алиса берет один фотон и поляризует его в одно из направлений: вертикально, горизонтально, +45°, -45°. Для кодирования будут использоваться 2 базиса: канонический (горизонтально-вертикальный) и диагональный (-45°, +45°). В каждом из базисов фотон в одной поляризации равен 1, в другой - 0. Горизонтальная = 1, вертикальная = 0, +45° = 0, +135° = 1. (см. приложение 3)

Как можно заметить, поляризация в базисах ортогональна, то есть эти направления перпендикулярны друг другу, а значит, если будет лететь горизонтальный фотон, то при измерении его в каноническом базисе с 100% вероятностью измерение покажет, что это горизонтальный фотон. Каждый раз Алиса подкидывает монету (или использует генератор случайных чисел) и выбирает в каком базисе отправить фотон, затем отправляет его. Вся суть в том, что если фотон летит диагональный, то при измерении его в каноническом базисе, фотон будет не чем-то средним, а находится в суперпозиции двух возможных поляризаций канонического базиса и у Боба появится 50% шанс получить верное число.

Таким образом, Алиса отправляет достаточно большую случайную последовательность фотонов в случайных базисах. Бобу же, в свою очередь, тоже при измерении фотона надо выбрать базис, точно так же подкидывая монету. Логично, что Боб не будет каждый раз правильно угадывать базис, примерно 50% выборов будут ошибочными, но это лишь условность, которая нужна в этом методе. (см. приложение 4)

После того, как передача фотонов закончена, Алиса и Боб обмениваются последовательностью базисов по открытому каналу связи и те результаты, где базисы не сходятся, исключаются. Как следствие, остаются только те результаты, где базисы сходятся, а так как поляризация в базисах ортогональна, то ошибок в измерении при одинаковых базисах быть не может. Таким образом, остается просеянный ключ, который никто не знает и которым можно пользоваться для шифрования сообщений по открытому каналу связи.

Но что произойдет, если при генерации ключа канал будет прослушиваться Евой? Вся суть заключается в том, что Ева точно также должна выбирать базис. В процессе измерения фотон полностью поглотится и его не получится скопировать и отправить Бобу из-за запрета клонирования квантовых состояний, в таком случае Еве придется создать такой же фотон и отправить Бобу. “Нет проблем!” - подумает Ева, но ведь при измерении фотона Евой суперпозиция фотона пропадет и в случае выбора неверного базиса, Ева даже не узнает об этом и отправит Бобу неправильный фотон.

Рассмотрим на примере: Алиса отправляет горизонтальный фотон (1) в каноническом базисе Бобу, Ева перехватывает этот фотон, но измеряет его в диагональном базисе, из-за чего шанс того, что выпадет 0 уже не 0%, как в каноническом базисе, а 50%, после того, как Ева получит фотон, она отправит Бобу диагональный фотон и если Боб выберет для измерения канонический базис, то вероятность получить 0 = 50%, ведь базис выбран не тот, в котором отправила Ева.

В итоге Боб может получить 0 и при обмене базисов с Алисой это число останется, так как базисы у Боба и у Алисы одинаковы, а потом при шифровке сообщений этим кодом вылезут ошибки, после которых Алиса и Боб поймут, что было вмешательство и будут генерировать новый ключ. Так как фотонов для генерации ключа будет много, то и процент ошибок, созданных Евой, будет около 25%, что сразу же заметят Алиса и Боб. Такая сложная структура позволяет обеспечить 100% безопасность, ведь если канал будет прослушиваться, об этом сразу узнают.

**2.5. Проблемы метода BB84**

В теории все это звучит безопасно и надежно, но в реальности есть проблемы. Одна из них состоит в источнике, который выпускает фотоны. Как говорилось ранее, фотоны отправляются по одному, но пока еще не были созданы лазеры, которые испускают свет по

одному фотону, иногда они могут отправить 2-3 одинаковых фотона. В таком случае Ева может измерить только один фотон, а остальные полетят дальше без изменений, из-за чего Алиса и Боб не узнают, что канал прослушивали.

**Заключение**

Пока квантовые компьютеры не вошли в нашу жизнь, есть время исправить все недочеты в методе BB84 и тогда используя метод BB84 можно сгенерировать секретный ключ для будущего шифрования любых сообщений методом Вернама. Такая схема обеспечит 100% безопасность шифрования и ни при каких условиях нельзя будет взломать эту схему.

**Источники информации**

1. Квантовая суперпозиция <https://ru.wikipedia.org/wiki/%D0%9A%D0%B2%D0%B0%D0%BD%D1%82%D0%BE%D0%B2%D0%B0%D1%8F_%D1%81%D1%83%D0%BF%D0%B5%D1%80%D0%BF%D0%BE%D0%B7%D0%B8%D1%86%D0%B8%D1%8F>

2. Ортогональность <https://ru.wikipedia.org/wiki/%D0%9E%D1%80%D1%82%D0%BE%D0%B3%D0%BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D0%BE%D1%81%D1%82%D1%8C>

3. Метод квантового шифрования BB84 <https://ru.wikipedia.org/wiki/BB84>

4. Иванова Е.Ю., Ларионцева Е.А. Введение в квантовую криптографию: основные понятия, подходы и алгоритмы. Инженерный журнал: наука и инновации, 2013, вып. 11.

5. Секреты квантового шифрования <https://www.youtube.com/watch?v=mVQE40eWISg>

6. Квантовая криптография: алгоритм BB84 <https://www.youtube.com/watch?v=p7fNCe-ztAs>

7. Асимметричное шифрование <https://www.youtube.com/watch?v=sGFbM-X6W_4>

8. Квантовый компьютер вместо мозга? <https://www.youtube.com/watch?v=khtLYce_WR8&t=514s>

9. Поляризация света. Закон Малюса <https://www.youtube.com/watch?v=1PK__XxPmmE&t=516s>

10. Что такое квантовая суперпозиция? <https://www.youtube.com/watch?v=oU1HPrYvJJk>

11. Как работает алгоритм RSA? <https://www.youtube.com/watch?v=Oc4QSFxTuXQ>

12. Поляризация волн <https://ru.wikipedia.org/wiki/%D0%9F%D0%BE%D0%BB%D1%8F%D1%80%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F_%D0%B2%D0%BE%D0%BB%D0%BD>

13. Кубит <https://ru.wikipedia.org/wiki/%D0%9A%D1%83%D0%B1%D0%B8%D1%82>

14. Загадка квантовой физики - эксперимент с двумя щелями <https://www.youtube.com/watch?v=QGq2YNyVbGs>

15. BB84 Protocol of quantum key distribution <https://www.youtube.com/watch?v=44G9UuB2RWI&t=182s>

16. Метод квантового шифрования RSA <https://ru.wikipedia.org/wiki/RSA>

17. Квантовая запутанность <https://ru.wikipedia.org/wiki/%D0%9A%D0%B2%D0%B0%D0%BD%D1%82%D0%BE%D0%B2%D0%B0%D1%8F_%D0%B7%D0%B0%D0%BF%D1%83%D1%82%D0%B0%D0%BD%D0%BD%D0%BE%D1%81%D1%82%D1%8C>

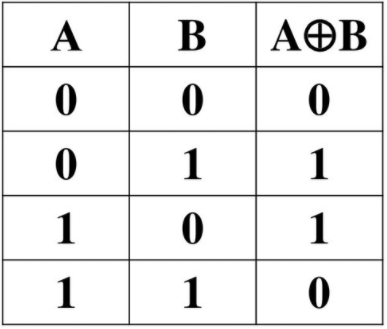
18. Что такое квантовый компьютер? <https://www.youtube.com/watch?v=dYSb3mS6kPc>

19. Квантовый компьютер <https://ru.wikipedia.org/wiki/%D0%9A%D0%B2%D0%B0%D0%BD%D1%82%D0%BE%D0%B2%D1%8B%D0%B9_%D0%BA%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80>

**Приложения**

Приложение 1. **Результаты соц. опроса**

Приложение 2. **Таблица истинности “исключающее или”**



Приложение 3. **Виды базисов**



Приложение 4. **Формирование квантового ключа**

