**1.Цели**

Целями курсовой работы являются:

1. Изучение эллиптических кривых и операций с точками на них.
2. Реализация класса эллиптических кривых
3. Изучение и реализация алгоритма факторизации Ленстры
4. Изучение и реализация криптографического протокола ECDH
5. Рассмотрение сферы применения криптографии на эллиптических кривых

**2.Актуальность**

Криптография на эллиптических кривых представляет собой одну из наиболее актуальных и востребованных областей криптографии в современном мире.

Это обусловлено высокой степенью криптостойкости при меньшем размере ключа, по сравнению с классической криптографией, что делает ее особенно полезной в ограниченных вычислительных ресурсах**.**

**3. Основа криптографии на ЭК**

Так как в основе изученных алгоритмов лежит эллиптическая кривая в нормальной форме Вейерштрасса, в данной работе рассмотрен только такой вид ЭК. Итак, ЭК в нормальной форме Вейерштрасса, это гладкая кривая вида , определенная над конечным полем , образующая группу по сложению для множества точек на ней. Интерес для криптографии она представляет благодаря своим свойствам и сложности задачи дискретного логарифмирования. Идея ее применения заключается в том, что для некоторой точки , невозможно провести обратную операцию разложения на скаляр k и точку P за разумное время.

**4. Реализация класса ЭК**

Поскольку в основе криптографии на ЭК лежат операции на этих кривых в достаточно больших полях, был реализован соответствующий класс, поддерживающий основные операции. Такие как:

* сложение двух точек методом “double and add”;
* умножение точки на скаляр;
* проверка принадлежности точки заданной кривой;
* нахождение всех точек, определенных на кривой
* нахождение порядка точки

Операции с целыми числами произвольной длины поддерживается благодаря библиотеке boost.multiprecision.

**5. Протокол ECDH**

Одним из протоколов, использующих ЭК является ECDH (Elliptic Curve Diffie-Hellman), позволяющий двум абонентам установить общий секретный ключ по незащищенному каналу связи.

В основе алгоритма также лежит проблема дискретного логарифмирования. Реализация соответствует описанию алгоритма.

* Для генерации основных параметров используется метод ECDH.gen\_main\_parameters(), который генерирует случайную ЭК над заданным полем и пару секретный ключ(число) – публичный ключ(точка на кривой).
* Для корректной работы алгоритма основные параметры должны совпадать у обоих абонентов. Метод ECDH. set\_main\_parameters(publicParameter pp) позволяет установить их принимая на вход вспомогательную структуру publicParameter полученную от второго абонента.
* В завершении вызывается метод ECDH. gen\_shared\_secret(POINT PK) который формирует общий секретный ключ. В дальнейшем он может быть использован как ключ симметричной криптографии.

**6. Алгоритм Ленстры**

Алгортм Ленстры – эффективный алгоритм факторизации чисел, основанный на использовании свойств групп точек на эллиптической кривой. В основе алгоритма лежит следующая идея: для двух кривых Ep Eq, меньших исходной E, по модулю p и q соответственно с порядками N\_p и N\_q. Маловероятно, что большинство простых делителей N\_p N\_q совпадают, и вероятно при вычислении eP встретится некоторый kP = бесконечно удаленной точке по модулю p, но не по модулю q или наоборот. Если это так, то kP не существует на исходной кривой и в вычислениях было найдено такое v, что НОД(v, n) является простым делителем исходного числа.

Данный алгоритм имеет субэкспоненциальную сложность и время работы зависит от минимального размера делителя. Так же время работы может варьироваться для одного входного числа в зависимости от того, насколько удачная сгенерирована кривая и от внутреннего параметра B, используемого в основном цикле алгоритма. В связи с этим было реализовано два способа уменьшения времени работы.

1. Запуск алгоритма на нескольких различных ЭК. Поскольку алгоритм Ленстры является вероятностным, это позволит увеличить шансы сгенерировать оптимальную(удачную) ЭК. В итоге, при использовании 5 потоков это позволило сократить время работы, в среднем, на 70% (~2900 vs 5100 ms).
2. Разбиение внутреннего цикла с диапазоном [1,B] на равные части и вычисление точек в цикле в отдельных потоках. Этот способ при использовании 5 потоков позволил сократить время работы, в среднем, на 45%.

**7. Применение криптографии на ЭК**

Криптография на ЭК имеет широкое применение. На сегодняшний день она используется для обмена секретными ключами по незащищенному каналу, получения цифровой подписи, шифрования данных. Это обусловлено высокой криптостойкостью, эффективностью и сложностью задачи дискретного логарифмирования на ЭК. Используется в таких протоколах как, ECDSA(цифровая подпись), EdDSA(на кривой Эдвардса), ECDH, ECMQV(аутентификационный протокол).

**8. Выводы**

В ходе выполнения данной работы были изучены алгоритм Ленстры, протокол ECDH, а также эллиптические кривые, их параметры, математическое определение и свойства. Из результатов работы можно сделать вывод, что эллиптическая криптография является актуальным, эффективным и мощным инструментом защиты информации. Реализация изученного материала позволило лучше понять и применить принципы и методы этой области, что в дальнейшем может быть реализовано в проектах и научно-исследовательских работах на тему реализации безопасности, целостности и конфиденциальности информации.