Криптография на эллиптических кривых

ВЫПОЛНИЛ: ГУТРОВ РОМАН, МК-301

НАУЧНЫЙ РУКОВОДИТЕЛЬ: ШАЛАГИНОВ ЛЕОНИД ВИКТОРОВИЧ, ДОЦЕНТ, ДОКТОР ФИЗ.-МАТ НАУК

НАУЧНЫЙ РУКОВОДИТЕЛЬ: ПАНАСЕНКО ДМИТРИЙ ИГОРЕВИЧ, СТ.ПРЕПОДАВАТЕЛЬ

Цели курсовой работы

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

Актуальность курсовой работы

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.

Основа криптографии на эллиптических кривых

Эллиптическая кривая в нормальной форме Вейерштрасса – кривая вида: $E\colon\ y^2 = x^3 + ax + b\ (mod\ n)$.

Для некоторой точки $Q \in E, Q = k * P$, где $P \in E, k\ \in F_n$, невозможно провести обратную операцию разложения на скаляр k и точку P за разумное время в достаточно большом поле.

Реализация класса эллиптической кривой

Класс ELLEPTIC_CURVE. Реализует абстракцию эллиптической кривой.
Предоставляет следующие методы:

- 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.

Протокол ECDH. (Elliptic Curve Diffie-Hellman)

Протокол использующий эллиптическую кривую, позволяющую двум абонентам установить общий секретный ключ по незащищенному каналу связи.

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.

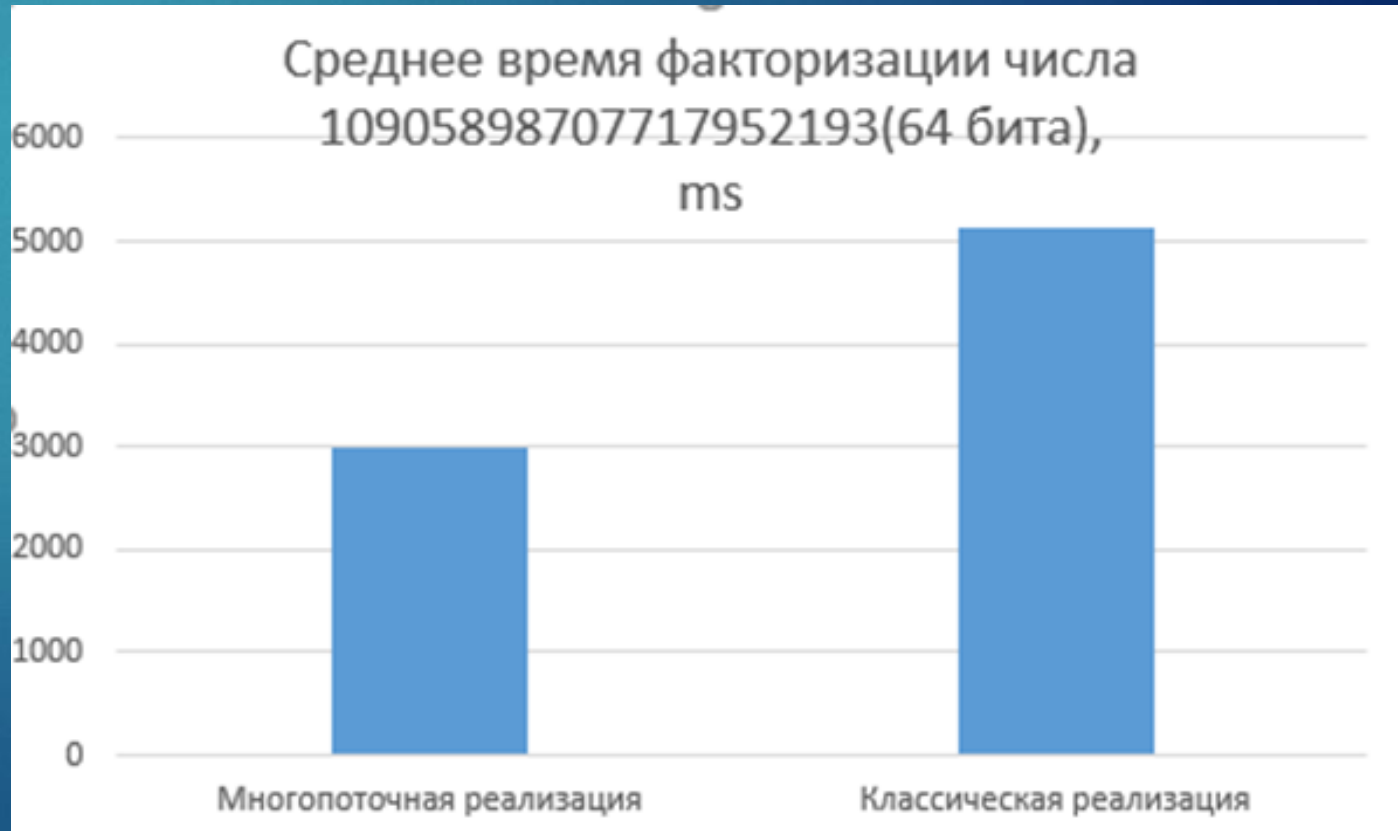
Алгоритм Ленстры

Алгортм Ленстры – эффективный алгоритм факторизации чисел, основанный на использовании свойств групп точек на эллиптической кривой.
E_n - исходная кривая.
E_p - кривая, меньшая чем E_n, по модулю p. N_p - порядок кривой.
E_q - кривая, меньшая чем E_n, по модулю q. N_q - порядок кривой.
p,q – два простых делителя n.
Маловероятно, что большинство простых делителей N_p и N_q совпадают, и вероятно, при вычислении eP найдется точка на бесконечности pK (mod q|p). Если это так, pK не существует и на исходной кривой, следовательно в вычислениях найдено такое v, что НОД(v, n) является простым делителем исходного n.

Ускорение работы алгоритма

Реализовано два способа, направленных на уменьшения времени работы алгоритма:

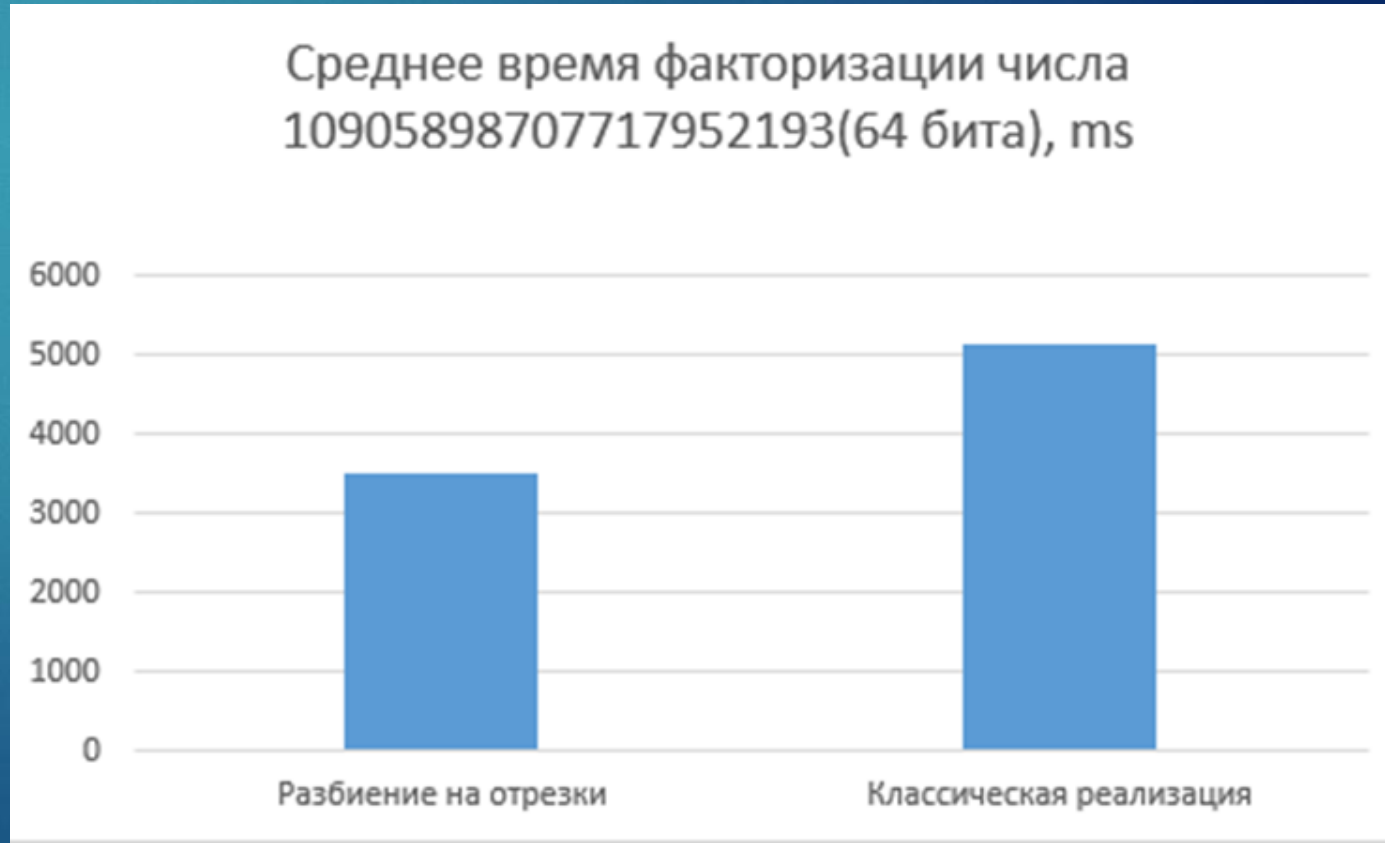
1. Запуск алгоритма на нескольких различных ЭК. Поскольку алгоритм Ленстры является вероятностным, это позволит увеличить шансы сгенерировать оптимальную(удачную) ЭК. В итоге, при использовании 5 потоков это позволило сократить время работы, в среднем, на 70%.



Ускорение работы алгоритма

Реализовано два способа, направленных на уменьшения времени работы алгоритма:

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%.



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.

Протоколы цифровой подписи:

1. ECDSA
2. EdDSA
3. BLS

Протоколы установления общего секретного ключа:

1. ECDH

Протоколы аутентификации:

1. ECMQV

Выводы

Криптография на эллиптических кривых имеет ряд преимуществ, включая высокую стойкость криптографии при использовании коротких ключей, компактность и эффективность вычислений. Ее использование находит широкое применение в различных областях, включая защиту данных, аутентификацию, электронную коммерцию, мобильные приложения и другие. Она предлагает эффективные и надежные методы обеспечения безопасности информации.