

Лабораторная работа № 4. Реализация протокола Диффи Хеллмана на эллиптических кривых

Цель работы:

Изучение особенностей реализации криптографических протоколов распределения ключей, асимметричной криптографии на эллиптических кривых, разработка системы распределения криптографических ключей.

Постановка задачи:

1. Выбрать коэффициенты a, b и модуль p эллиптической кривой, координаты x, y точки G , а также секретные значения k_1, k_2 абонентов из таблицы в соответствии с вариантом.
2. Разработать программную реализацию метода Диффи-Хеллмана. Предусмотреть проверку эллиптической кривой по формуле $4 * a^3 + 27 * b^2 \neq 0 \pmod{p}$. Исходными данными являются параметры кривой, координаты точки и секретные значения каждого участника обмена. Результат работы программы – координаты произведения точки G на число, которые должны совпасть у каждого из участников.
3. Оформить отчет.

Описание используемого метода

Для установления защищенной связи два пользователя A и B совместно выбирают эллиптическую кривую E и точку $G(x, y)$ на ней. На первом этапе пользователь A выбирает свое секретное целое число k_1 , вычисляет произведение $k_1 \cdot G$ и посылает результат абоненту B . Пользователь B генерирует свое секретное большое число k_2 , вычисляет произведение $k_2 \cdot G$ и пересылает его получателю A .

При этом параметры самой кривой, координаты точки на ней и значения произведений являются открытыми и могут передаваться по незащищенным каналам связи. Предполагается, что злоумышленник может получить оба этих значения, но не модифицировать их.

На втором этапе абонент A на основе имеющегося у пользователя числа и полученного по сети значения вычисляет ключ $K = k_1 \cdot k_2 \cdot G$. Абонент B аналогично вычисляет значение $K = k_2 \cdot k_1 \cdot G$. В силу свойств операции умножения на число оба пользователя получают общее секретное значение (координаты точки), которое они могут использовать для получения ключа шифрования. Секретное значение представляет собой пару чисел, для получения ключа симметричного шифрования из пары получают одно значение.

Стойкость шифрования с помощью эллиптических кривых базируется на сложности нахождения множителя k точки P по их произведению

Описание исходных данных:

В данной работе я выбираю 1 вариант, поэтому у меня будет следующий набор исходных параметров: $a = -1$, $b = 1$, $p = 29$, $G(x, y) = (9, 27)$, $k_1 = 4$, $k_2 = 17$.

Алгоритм работы программы:

Следует заметить, что в качестве вспомогательных алгоритмов, я использую расширенный алгоритм Евклида (см., например, [здесь https://en.wikipedia.org/wiki/Extended_Euclidean_algorithm](https://en.wikipedia.org/wiki/Extended_Euclidean_algorithm)).

Расширенный алгоритм Евклида - это модификация алгоритма Евклида, вычисляющая, кроме наибольшего общего делителя (НОД) целых чисел a и b , ещё и коэффициенты соотношения Безу, то есть такие целые x и y , что $a * x + b * y = GCD(a, b)$. В данной работе это соотношение позволяет найти обратное по модулю для некоторого числа, т.е. решить следующее уравнение: $a * x = 1 \pmod{n}$

Сложение точек на эллиптической кривой:

1. Вычисляем $\lambda = (y_2 - y_1) / (x_2 - x_1) \pmod{p}$. Для вычисления знаменателя используем расширенный алгоритм Евклида и считаем число обратное знаменателю.
2. Вычисляем $x_3 = \lambda^2 - x_1 - x_2 \pmod{p}$.
3. Вычисляем $y_3 = \lambda * (x_1 - x_3) - y_1 \pmod{p}$.
4. Возвращаем точку (x_3, y_3)

Примечание: При вычислении координат используются правила модульной арифметики - все действия выполняются по модулю p , отрицательные результаты приводят к положительным последовательным сложением с модулем p

Удвоение точки на эллиптической кривой:

1. Вычисляем $\lambda = (3 * x_1^2 + a) / (2 * y_1) \pmod{p}$. Для вычисления знаменателя используем расширенный алгоритм Евклида и считаем число обратное знаменателю.
2. Вычисляем $x_3 = \lambda^2 - 2 * x_1 \pmod{p}$.
3. Вычисляем $y_3 = \lambda * (x_1 - x_3) - y_1 \pmod{p}$.
4. Возвращаем точку (x_3, y_3)

Примечание: При вычислении координат используются правила модульной арифметики - все действия выполняются по модулю p , отрицательные результаты приводят к положительным последовательным сложением с модулем p

Умножение точки на скаляр:

Умножение точки на число реализуется последовательностью сложений и удвоений точки эллиптической кривой.

Вход: точка P , число, представленное в двоичном виде $m = (m_t, m_{t-1}, \dots, m_1)$.

Выход: $Q = [m]P$.

1. $Q = O$.
2. Для каждого $i = t, t-1, \dots, 1$ выполнить
 - 2.1. $Q = [2]Q$
 - 2.2. Если $m_i = 1$, то $Q = Q + P$.
3. Возвращаем Q .

Основная программа:

1. Вычисляем произведение $k_1 * G$ для пользователя A (и отправляем его пользователю B).
2. Вычисляем произведение $k_2 * G$ для пользователя B (и отправляем его пользователю A).
3. Вычисляем для пользователя A на основе имеющегося у него числа и полученного по сети значения, ключ $K = k_1 * (k_2 * G)$.

4. Вычисляем для пользователя В на основе имеющегося у него числа и полученного по сети значения, ключ $K = k_2 * (k_1 * G)$.
5. Сравниваем значение ключа К у пользователей А и В: они должны совпасть.

Тексты программы:

В качестве языка программирования я использую C#. Исходный текст программы приведен в отдельном файле Program.cs (без дополнительных файлов проекта - *.csproj и решения - *.sln).

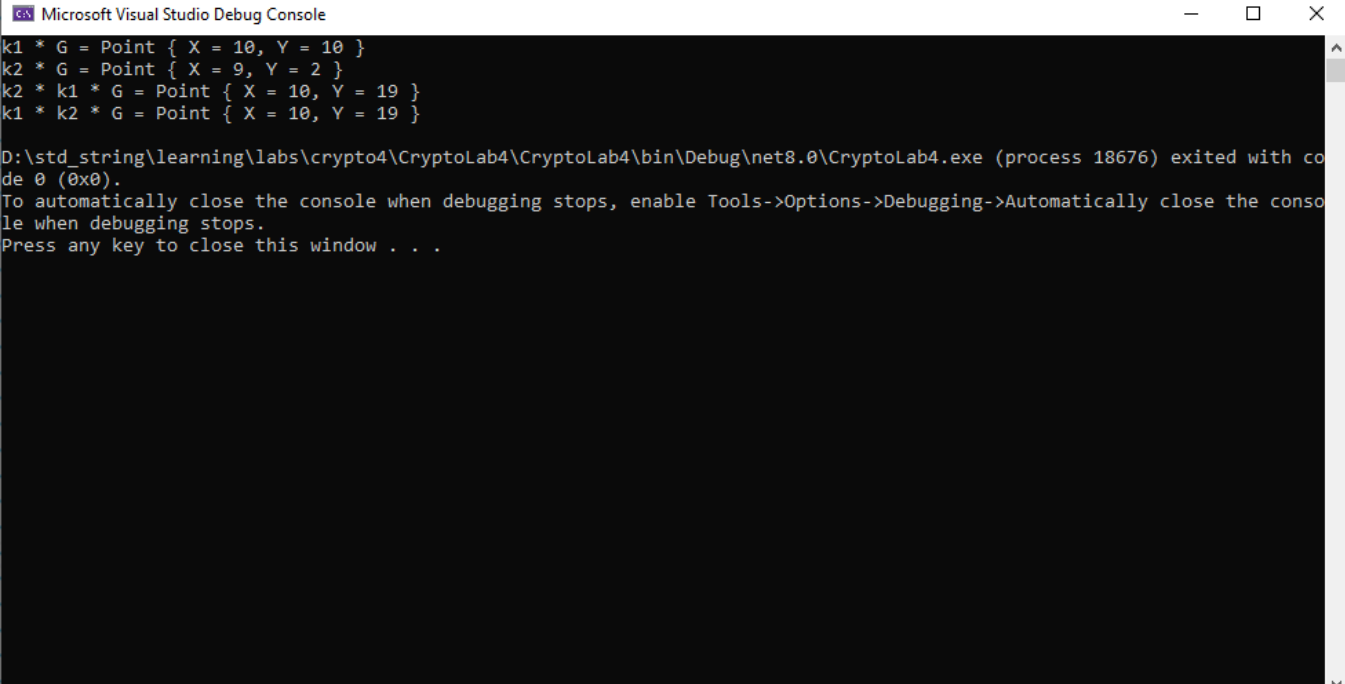
Результаты работы программы:

Произведение $k_1 * G$ для пользователя А: $X = 10, Y = 10$

Произведение $k_2 * G$ для пользователя В: $X = 9, Y = 2$

Ключ $K = k_1 * (k_2 * G)$ для пользователя А: $X = 10, Y = 19$

Ключ $K' = k_2 * (k_1 * G)$ для пользователя В: $X = 10, Y = 19$



```
Microsoft Visual Studio Debug Console

k1 * G = Point { X = 10, Y = 10 }
k2 * G = Point { X = 9, Y = 2 }
k2 * k1 * G = Point { X = 10, Y = 19 }
k1 * k2 * G = Point { X = 10, Y = 19 }

D:\std_string\learning\labs\crypto4\CryptoLab4\CryptoLab4\bin\Debug\net8.0\CryptoLab4.exe (process 18676) exited with code 0 (0x0).
To automatically close the console when debugging stops, enable Tools->Options->Debugging->Automatically close the console when debugging stops.
Press any key to close this window . . .
```

Анализ результатов:

1. Мы увидели, как с помощью математических операций над эллиптической кривой мы можем создавать и распространять ключи между двумя пользователями А и В.
2. Мы увидели и реализовали операции над точками на эллиптической кривой и убедились насколько сильно они отличаются от операций над обычными числами.

Выводы:

Мы изучили и реализовали протокол Диффи Хеллмана на эллиптических кривых, а также увидели, как с его помощью через обмен соответствующими сообщениями, пользователи А и В могут получить общий ключ симметричного шифрования.

Контрольные вопросы:

1. Цель применения протокола Диффи-Хеллмана.

Основной задачей протоколов распределения ключей является выработка участниками общего ключа на основе действий пользователей по созданию защищенного канала связи, заключающаяся в генерации и обмене сеансовыми ключами и аутентификации сообщений.

Одним из самых распространенных способов ключевой генерации и обмена является протокол Диффи-Хеллмана, основанный на асимметричной криптографии.

2. Что представляет собой эллиптическая кривая?

В криптографии применяется уравнение эллиптической кривой E вида:
 $y^2 = x^3 + a * x + b \pmod{p}$.

3. Какие операции определены на эллиптической кривой при использовании в криптографических приложениях?

Базовые операции, которые определены на эллиптической кривой: сложение точек и удвоение точки. На основе этих двух операций может быть определена операция умножения точки на скаляр

4. Как выполнить умножение точки эллиптической кривой на число?

По следующему алгоритму (через использование базовых операций - сложение точек и удвоение точки):

Вход: точка P , число, представленное в двоичном виде $m = (m_t, m_{t-1}, \dots, m_1)$.

Выход: $Q = [m]P$.

1. $Q = O$.

2. Для каждого $i = t, t-1, \dots, 1$ выполнить

2.1. $Q = [2]Q$

2.2. Если $m_i = 1$, то $Q = Q + P$.

3. Возвращаем Q .

5. Как вычислить число, обратное к данному по заданному модулю?

Найти обратное по модулю для некоторого числа - это означает, что нужно решить следующее уравнение: $a * x = 1 \pmod{n}$. Его решение можно найти с помощью расширенного алгоритма Евклида (см., например, [здесь https://en.wikipedia.org/wiki/Extended_Euclidean_algorithm](https://en.wikipedia.org/wiki/Extended_Euclidean_algorithm)).

6. Что является нулем эллиптической кривой?

Нулем является точка O , также называемая «бесконечно удаленная точка». В этой точке сходятся все вертикальные прямые. Она обладает следующим свойством: сумма трех точек лежащих на одной прямой равна O