Министерство образования Республики Беларусь

Учреждение образования  
БЕЛОРУССКИЙ  ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

                        Факультет      Информационных технологий и управления

                        Кафедра         Интеллектуальных информационных технологий

**ОТЧЁТ**

по лабораторной работе №4

по дисциплине “Средства и методы защиты

информации в интеллектуальных системах”

Вариант 10

Выполнила:

Демидовец Д.В. , гр. 221703

Проверил:

Крищенович В.А.

Минск, 2024

**ОТКРЫТОЕ РАСПРОСТРАНЕНИЕ КЛЮЧЕЙ**

Теоретические сведения:

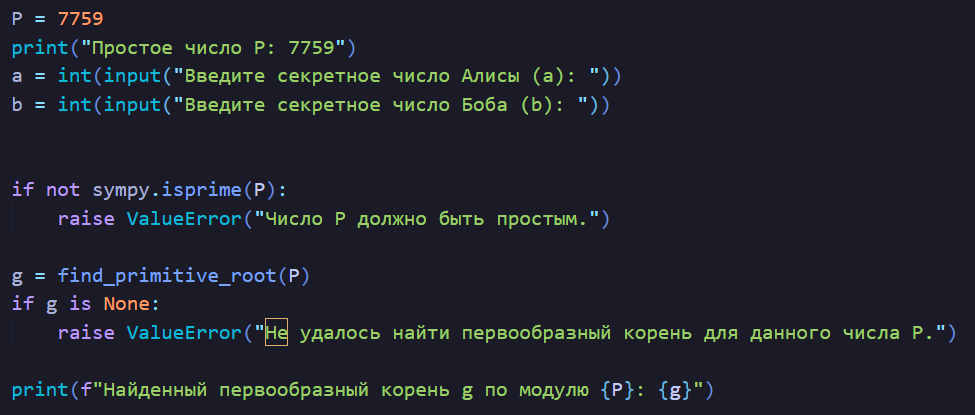
Протокол Диффи-Хеллмана (или алгоритм Диффи-Хеллмана) — это криптографический метод для безопасного обмена ключами по незащищённому каналу. Он был разработан в 1976 году Уитфилдом Диффи и Мартином Хеллманом и стал основой для многих современных протоколов шифрования.

Цель протокола Диффи-Хеллмана — позволить двум сторонам (например, Алисе и Бобу) безопасно обменяться общим секретным ключом, даже если их общение может прослушиваться третьей стороной (например, злоумышленником Джо). Этот общий ключ затем может быть использован для симметричного шифрования сообщений.

*Алгоритм протокола:*

1. Выбор публичных параметров.

Выбирается большое простое число 𝑃 (модуль) и базовое число 𝑔 (также известное как "примитивный корень"), которое является примитивным корнем по модулю. Эти числа 𝑃 и 𝑔 не являются секретными, их могут знать все участники, включая злоумышленников.

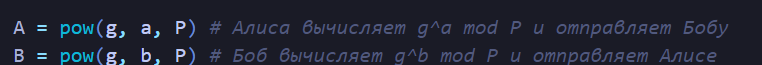


2. Генерация приватных чисел.

Алиса выбирает случайное приватное число 𝑎, которое никому не сообщает. Боб выбирает своё приватное число 𝑏, также не делясь им с кем-либо.

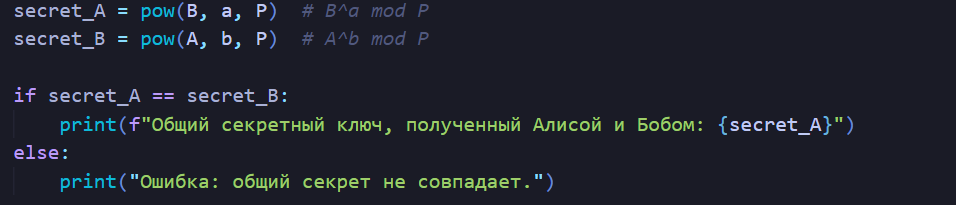
3. Вычисление публичных значений.

Алиса вычисляет значение A=g^a modP и отправляет его Бобу. Боб вычисляет значение B=g^b modP и отправляет его Алисе.



4. Генерация общего секрета:

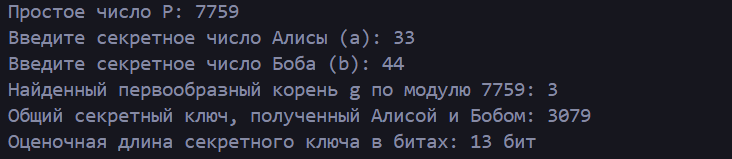
После получения 𝐵 от Боба, Алиса вычисляет общий секретный ключ как K = 𝐵^𝑎 mod𝑃. Боб, получив 𝐴 от Алисы, вычисляет тот же секретный ключ как K=𝐴^𝑏 mod𝑃.



Таким образом, общий секретный ключ K вычисляется и у Алисы, и у Боба, и его значение совпадает, поскольку 𝐵^𝑎 mod = 𝐴^𝑏 mod𝑃 = 𝑔^(𝑎𝑏)mod𝑃.

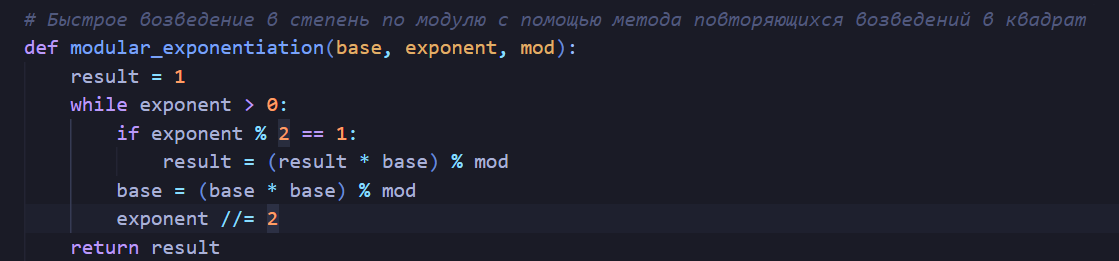
*Преимущество Диффи-Хеллмана*

Протокол позволяет двум сторонам создать общий секретный ключ по незащищённому каналу, не передавая сам ключ напрямую. Даже если злоумышленник перехватит значения 𝐴 и 𝐵, ему будет чрезвычайно сложно вычислить общий секрет, так как для этого требуется решить задачу вычисления дискретного логарифма, которая сложна и занимает много времени при больших значениях 𝑃.

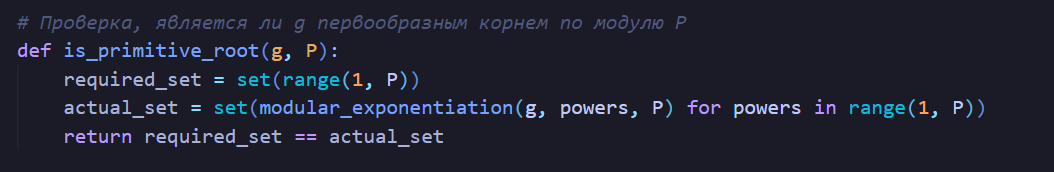


*Дополнительные функции для работы программы*

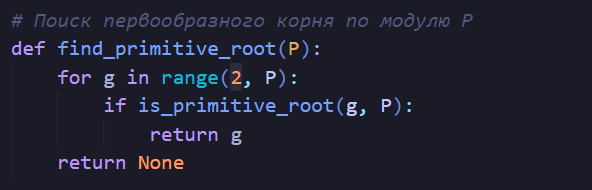
Функция *modular\_exponentiation(base, exponent, mod)* выполняет быстрое возведение числа в степень по модулю, используя метод повторяющегося возведения в квадрат. Этот метод существенно сокращает количество необходимых операций по сравнению с обычным возведением в степень.



Функция *is\_primitive\_root(g, P)* проверяет, является ли число g первообразным корнем по модулю простого числа P, то есть создаёт все возможные остатки от деления чисел от 1 до P−1.

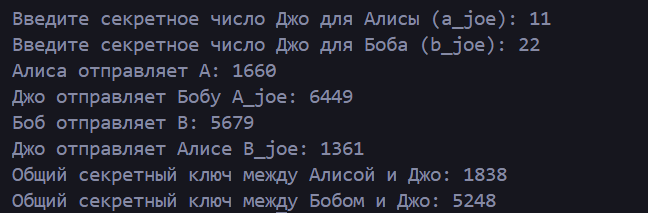


Функция *find\_primitive\_root(P*) ищет первообразный корень по модулю простого числа 𝑃. Как только найден первый кандидат, который является первообразным корнем, функция возвращает его значение.



*Уязвимость протокола*

Атака "человек посередине" (MITM, от англ. Man-in-the-Middle) — это тип атаки, при котором злоумышленник перехватывает и, возможно, изменяет сообщения, которыми обмениваются две стороны (Алиса и Боб). В атаке MITM злоумышленник "встаёт" между участниками так, чтобы оба считали, что общаются напрямую друг с другом, тогда как на самом деле вся информация проходит через злоумышленника, который может читать, подменять или искажать данные. В контексте протокола Диффи-Хеллмана MITM позволяет злоумышленнику, перехватив значения, подменить их своими и создать два независимых "секретных ключа" с каждым из участников.



Для защиты от атак типа "человек посередине" (MITM), как в примере с Джо, используются протоколы аутентификации сторон. Эти протоколы позволяют участникам обмена убедиться в личности друг друга перед началом сеанса, чтобы гарантировать, что данные передаются именно тому, кому они предназначены, и не были перехвачены или изменены злоумышленником.

Основные методы аутентификации:

* Цифровые сертификаты и инфраструктура открытых ключей (PKI).

Цифровой сертификат — это электронный документ, который содержит публичный ключ участника и подписан центром сертификации (CA), что подтверждает подлинность владельца ключа.

* Электронные подписи

Электронная подпись создаётся с использованием закрытого ключа отправителя и добавляется к передаваемым данным, например, к значениям 𝐴 и 𝐵. Подлинный владелец закрытого ключа может создать действительную подпись, которую затем можно проверить с помощью открытого ключа.

* Многофакторная аутентификация

Этот метод добавляет дополнительные уровни аутентификации, требуя от пользователей предоставить несколько подтверждений личности (например, пароль, токен или биометрический параметр).