**Теоретические сведения**

1. Протокол Диффи-Хеллмана - это криптографический протокол, который позволяет двум сторонам (называемым Алисой и Бобом) безопасно обмениваться секретными данными через незащищенный канал связи.

Протокол Диффи-Хеллмана основан на математической задаче дискретного логарифмирования в конечных полях. Эта задача является вычислительно сложной и не имеет известного эффективного алгоритма решения.

Протокол использует математическую операцию возведения в степень по модулю, которая обеспечивает свойство диффузии, то есть небольшие изменения во входных данных приводят к большим изменениям в выходных данных.

Протокол состоит из следующих шагов:

- Алиса и Боб выбирают общее простое число `P` и примитивный элемент `g`, которые являются общими для обоих сторон.

- Алиса выбирает случайное число `a` в качестве своего приватного ключа и вычисляет публичный ключ `A` как `g^a mod P`.

- Боб выбирает случайное число `b` в качестве своего приватного ключа и вычисляет публичный ключ `B` как `g^b mod P`.

- Алиса и Боб обмениваются публичными ключами `A` и `B` через незащищенный канал связи.

- Алиса вычисляет общий секретный ключ `K` как `B^a mod P`.

- Боб вычисляет общий секретный ключ `K` как `A^b mod P`.

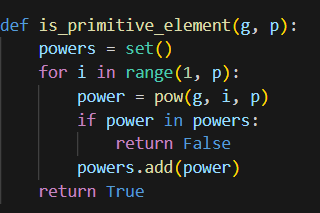
- Оба участника получают одинаковый общий секретный ключ `K`, который может использоваться для дальнейшего обмена секретными сообщениями.

Однако протокол Диффи-Хеллмана не обеспечивает аутентификацию сторон. Это значит, что стороны не могут быть уверены в том, что они обмениваются ключами с именно тем, с кем они думают. Для обеспечения аутентификации сторон протокол Диффи-Хеллмана может быть комбинирован с другими протоколами, такими как протоколы аутентификации или цифровые подписи.

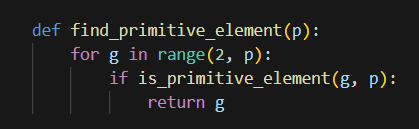
Протокол Диффи-Хеллмана широко используется в современных системах криптографии, включая протоколы SSL/TLS, VPN и аутентификацию в беспроводных сетях.

Безопасность протокола Диффи-Хеллмана зависит от выбора безопасных параметров и правильной реализации протокола. При разработке и использовании протокола Диффи-Хеллмана необходимо учитывать современные атаки и рекомендации по безопасности.

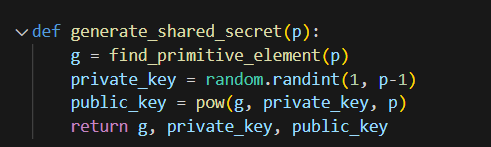
**Реализация протокола Диффи Хелмана**



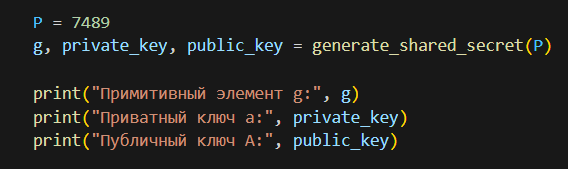
Функция is\_primitive\_element проверяет, является ли число g примитивным элементом поля GF(P).



Функция find\_primitive\_element находит примитивный элемент для заданного простого числа P.



Функция generate\_shared\_secret генерирует приватный и публичный ключи для каждого из участников и возвращает их.



Описание шагов для вычисления общего секрета Алисой и Бобом:

Алиса и Боб выбирают одно и то же простое число P=7489.

Алиса генерирует случайное число private\_key от 1 до P-1.

Алиса вычисляет public\_key = g^private\_key mod P, где g - примитивный элемент поля GF(P).

Боб генерирует случайное число private\_key от 1 до P-1.

Боб вычисляет public\_key = g^private\_key mod P.

Алиса и Боб обмениваются значениями public\_key.

Алиса вычисляет общий секретный ключ K = public\_key^private\_key mod P.

Боб вычисляет общий секретный ключ K = public\_key^private\_key mod P.

Алиса и Боб получают одинаковое значение общего секретного ключа K.

Выводы:  
а) Длина ключа зависит от выбранного простого числа P, в данном случае P=7489. Длина ключа равна длине представления числа P в битах.  
б) Возможные угрозы протоколу включают атаки на основе перебора значений private\_key, атаки посредника, подмены значения public\_key. Для защиты от таких угроз можно использовать дополнительные алгоритмы аутентификации, шифрования и проверку целостности данных. Также важно выбирать достаточно длинные простые числа P для обеспечения безопасности протокола.