

Алгоритм (протокол) Диффи — Хеллмана.

Современные алгоритмы шифрования делятся глобально на два вида: симметричные (AES, IDEA, 3DES...) и асимметричные (RSA, ElGamal, Elliptic curve cryptosystem...). Симметричные алгоритмы используют один и тот же ключ для процесса шифрования/десифрования, асимметричным алгоритмам требуется несколько ключей. Например RSA шифрует данные при помощи открытого ключа (доступного кому-угодно), но расшифровать данные можно только с помощью второго (закрытого) ключа. У каждого из этих алгоритмов есть свои недостатки:

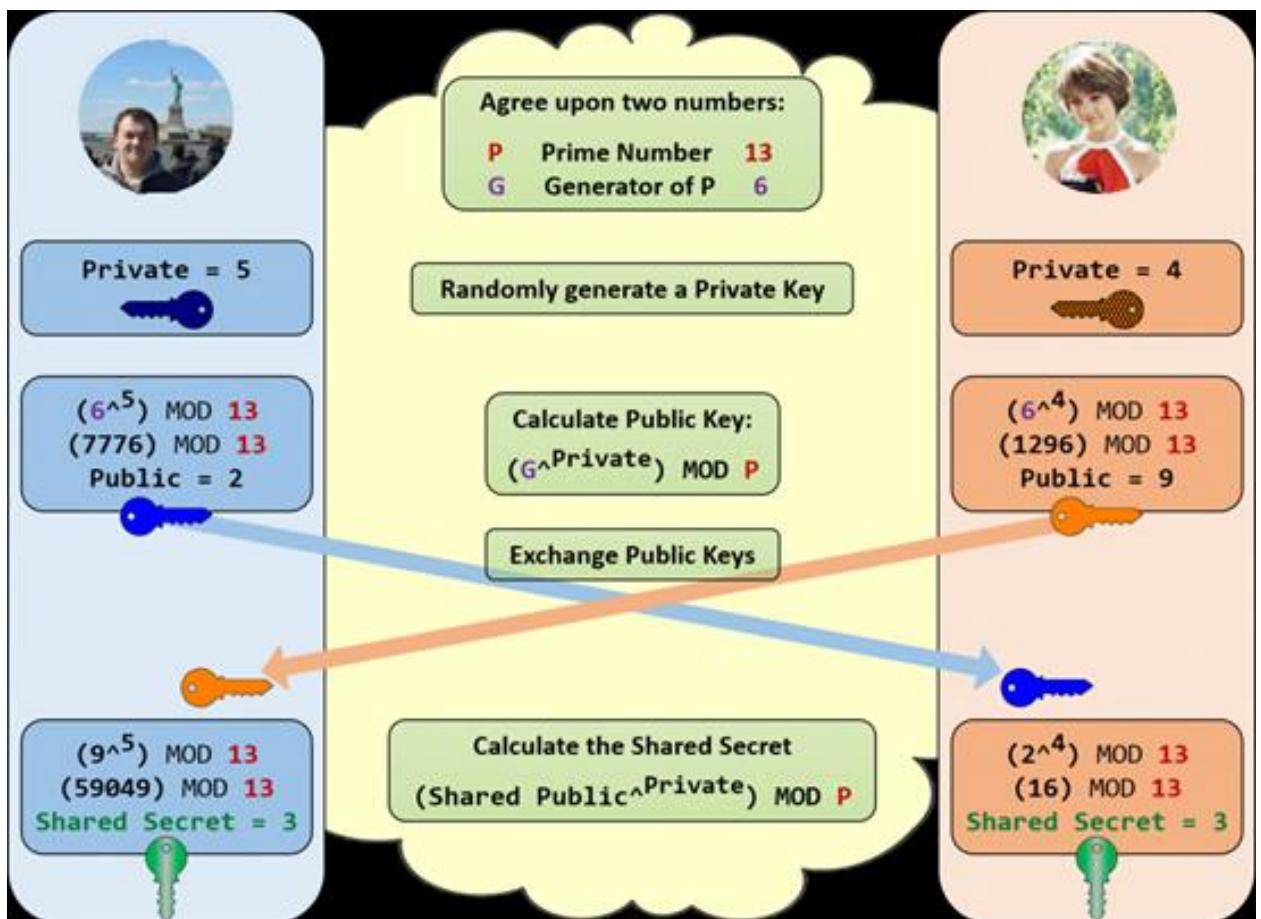
- недостаток асимметричного шифрования заключается в низкой скорости выполнения операций шифрования и расшифровки, что обусловлено необходимостью обработки ресурсоемких операций. Дополнительные проблемы возникают и при защите открытых ключей от подмены, ведь достаточно просто подменить открытый ключ легального пользователя, чтобы впоследствии легко расшифровать его своим секретным ключом.
- недостаток симметричного шифрования заключается в необходимости публичной передачи ключей – «из рук в руки». При такой системе становится практически невозможным использование симметричного шифрования с неограниченным количеством участников.

Рассмотрим безопасное общение по открытому (прослушиваемому) каналу связи. Сообщения или данные нужно зашифровывать и расшифровывать, но для этого обеим сторонам нужно иметь общий ключ. Если этот ключ передавать по тому же каналу, то прослушивающая сторона тоже получит его, и смысл шифрования исчезнет.

Алгоритм (протокол) Диффи — Хеллмана позволяет двум сторонам получить общий секретный ключ, используя незащищенный от прослушивания, но защищенный от подмены канал связи. Полученный ключ можно использовать для обмена сообщениями с помощью симметричного шифрования.

Стоит заметить, что даже перехват сессионного ключа не влечёт за собой компрометацию личного ключа участника, т.к. данные операции построены на принципах необратимых математических операций.

Предположим некий Боб, хочет обменяться сообщениями с некой Алисой, но так чтобы их переписка была зашифрована и никто другой не догадался о содержимом переписки. Как же обменяться ключом шифрования с Алисой?



Вначале вспомним математику:

простое число (prime number) это такое число, которое делится только 1 и на самого себя, например 1, 13, 17, 29

mod – это операция взятия остатка от деления.

Пример: $25 \text{ mod } 5 = 0$, $29 \text{ mod } 5 = 4$.

Пусть $P=13$. Так как это число также используется как модуль для каждого вычисления, все пространство ключей для полученного общего секрета

может быть только 0-12. Чем больше это число, тем труднее вычисление и тем большее время требуется для прямого перебора ключей. Маленькое число 13 взято для простоты вычислений и большей наглядности, в реальной жизни для Диффи-Хеллмана числа значительно больше 768, 1024 или 1536 бит. Что это значит? Например, чтобы полностью записать номер 768 бит, вам понадобится 232 десятичных разряда.

Итак:

- 1) Боб договаривается с Алисой, что в качестве простого числа (P) для своих вычислений они будут использовать 13, а в качестве примитивного корня по модулю G цифру 6. Данная информация открыта и может быть перехвачена, но это не страшно.
- 2) Каждый из участников задумывает свой приватный ключ, и держит его в строгом секрете. Боб – число 5, Алиса – число 4.
- 3) Каждый из участников вычисляет свои публичные ключи по формуле:
($G^{\text{приватный_ключ}} \bmod P$).

Боб: **$6^5 \bmod 13 = (7776) \bmod 13 = 2$**

Это публичный ключ Боба, который он отправляет так же по открытому каналу связи Алисе.

Алиса: **$(6^4) \bmod 13 = (1296) \bmod 13 = 9$**

Это публичный ключ Алисы, который она отправляет Бобу.

Вычисляем сессионный ключ, тот самый который будет использоваться в симметричном алгоритме шифрования и тот который будет неизвестен никому кроме Алисы и Боба. Вычисляем этот ключ по формуле:

(публичный_ключ_собеседника $^{\wedge}$ свой_приватный_ключ) mod P

Боб: $(9^5) \bmod 13 = (59049) \bmod 13 = 3$ (общий секрет)

Алиса: $(2^4) \bmod 13 = 16 \bmod 13 = 3$ (общий секрет)

Итог $3=3$, одинаковый ключ и у Алисы и у Боба.

Далее, используя сессионный ключ, Боб шифрует свое сообщение, например, при помощи алгоритма AES и отправляет Алисе. Алиса получает сообщение Боба и расшифровывает его.

ЗАДАНИЕ

Выберите р и q согласно варианта (номер в списке группы)

| Вариант | p | q | Вариант | p | q |
|---------|----|----|---------|----|----|
| 1 | 19 | 73 | 14 | 71 | 79 |
| 2 | 29 | 73 | 15 | 19 | 43 |
| 3 | 17 | 29 | 16 | 13 | 61 |
| 4 | 23 | 61 | 17 | 41 | 79 |
| 5 | 13 | 31 | 18 | 13 | 53 |
| 6 | 23 | 31 | 19 | 59 | 61 |
| 7 | 53 | 73 | 20 | 13 | 83 |
| 8 | 31 | 37 | 21 | 13 | 19 |
| 9 | 17 | 37 | 22 | 19 | 29 |
| 10 | 23 | 79 | 23 | 17 | 67 |
| 11 | 13 | 41 | 24 | 13 | 17 |
| 12 | 23 | 41 | 25 | 31 | 73 |
| 13 | 17 | 41 | 26 | 31 | 67 |

Вычислите закрытый сессионный ключ

С помощью полученного ключа, используя на выбор алгоритм Цезаря, AES или любой другой симметричный алгоритм шифрования, зашифруйте произвольное сообщение на стороне Боба, а затем расшифруйте это сообщение на стороне Алисы.