

Вот пример одного из ассиметричного алгоритма (диффи-хеллмана) для обмена симметричным ключом. Все чудо заключается в математике.

Представьте, что Алиса и Боб хотят обменяться секретными сообщениями. Но у них нет возможности передать секретный ключ так, чтобы никто их не подслушал. Они решают использовать алгоритм Диффи-Хеллмана для безопасного обмена секретным ключом. Вот как они это делают:

1. Алиса и Боб договариваются о большом числе, скажем, 99, и меньшем числе — 2. Эти числа не являются секретными и могут быть переданы кому угодно.
2. Алиса задумывает своё секретное число — 11. С помощью математики вычисляет результат, используя общеизвестные числа и свое секретное число (то есть 99, 2 и 11). В результате магии математики получается 68. Алиса посылает это число Бобу.
3. Боб думает о своем личном секретном числе — 13 и вычисляет результат тем же математическим способом, но с помощью своих чисел (открытые 99, 2 и свое 13). В результате получается 74. Боб отправляет этот результат Алисе.
4. Алиса берет результат Боба (74) и с помощью математики вычисляет общее секретное число = 41.
5. Аналогично, Боб берет результат Алисы (68) и с помощью математики вычисляет общее секретное число, которое за счет магии получается таким же = 41.
6. Алиса и Боб имеют одно и то же число 41 в качестве общего секретного ключа, который могут использовать для симметричного шифрования. Любой, кто подслушивал их разговор, знает только открытые числа (99 и 2) и результаты, которые Алиса и Боб послали друг другу в процессе (68 и 74). Никто не может разгадать их секретный ключ, не зная их секретных чисел.