Урок 5. Обмен ключами Диффи–Хеллмана

Криптография · ~35 минут

Представь: тебе нужно договориться с другом о секретном пароле, но единственный канал связи — открытый чат, где всё читает твоя любопытная сестра. Кажется, это невозможно? А вот и нет. В 1976 году придумали способ, и он кажется почти волшебством.

🎯 Что ты узнаешь

- В чём суть проблемы обмена ключами.
- Как двое договариваются о секрете по открытому каналу.
- Аналогию со смешиванием красок.
- Почему подслушивающий не может вычислить секрет.

📖 Разбираемся в теме

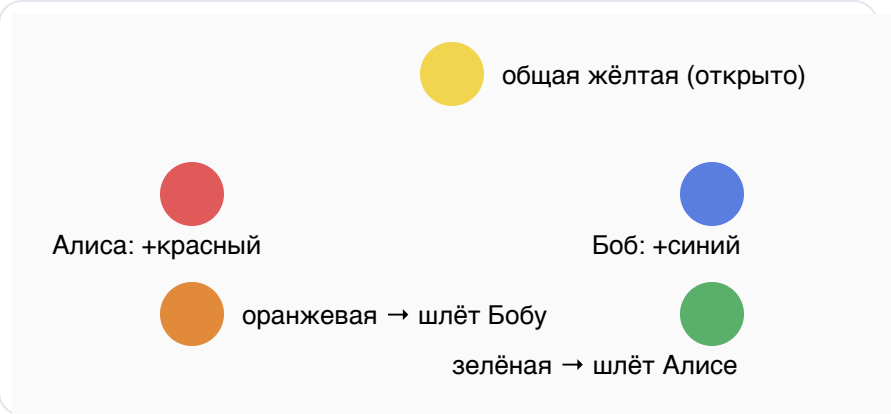
Проблема

Все шифры до этого требовали, чтобы у отправителя и получателя был **общий секретный ключ**. Но как его передать, если любой канал прослушивается? Отправить ключ по почте — его перехватят. Получается замкнутый круг.

Уитфилд Диффи и Мартин Хеллман нашли выход: секрет можно **создать совместно**, ничего секретного не пересылая.

Аналогия с красками

Представь смешивание красок. Есть важное свойство: **смешать две краски легко, а разделить смесь обратно на исходные цвета — практически невозможно**.



1. Алиса и Боб публично договариваются об **общей жёлтой краске** (её видят все).
2. Каждый добавляет к ней **свою секретную краску**: Алиса — красную, Боб — синюю. Свои секретные цвета они никому не показывают.
3. Они **обмениваются смесями** по открытому каналу: Алиса шлёт оранжевую (жёлтая+красная), Боб — зелёную (жёлтая+синяя).
4. Теперь каждый добавляет к **полученной смеси свою секретную краску**:
   - Алиса: зелёная + её красная = жёлтая+синяя+красная.
   - Боб: оранжевая + его синяя = жёлтая+красная+синяя.

У обоих получилась **одна и та же** грязно-коричневая смесь — их общий секрет! А сестра видела только жёлтую, оранжевую и зелёную. Чтобы получить секрет, ей пришлось бы «разделить» смесь на исходные краски — а это невозможно.

То же самое, но с числами

Роль «легко смешать, трудно разделить» играет **возведение в степень по модулю** (из урока 4). Обратная операция — найти показатель степени — называется **дискретным логарифмом**, и она очень трудна.

Возьмём маленькие числа. Публично известны:

- модуль (простое) $p = 23$;
- основание $g = 5$.

Секреты: Алиса задумала $a = 6$, Боб задумал $b = 15$ (никому не говорят).

Шаг 1. Каждый вычисляет свою «смесь» и посылает её открыто:

- Алиса: $A = g^a \bmod p = 5^6 \bmod 23$. Считаем: $5^2=25\equiv 2$, $5^3\equiv 2\cdot5=10$, $5^6=(5^3)^2\equiv 10^2=100\equiv 8$. Значит $A = 8$.
- Боб: $B = g^b \bmod p = 5^{15} \bmod 23 = 19$.

Шаг 2. Каждый возводит **полученное** число в свою секретную степень:

- Алиса: $s = B^a \bmod p = 19^6 \bmod 23 = 2$.
- Боб: $s = A^b \bmod p = 8^{15} \bmod 23 = 2$.

Оба получили **общий секрет 2**! 🎉

> 📌 **Запомни:** это работает, потому что $(g^a)^b = g^{ab} = (g^b)^a$. Оба в итоге вычисляют $g^{ab} \bmod p$ — просто разными путями.

Почему сестра не справится

Сестра-подслушивающий знает всё **открытое**: $p=23$, $g=5$, $A=8$, $B=19$. Чтобы найти секрет, ей нужно вычислить a или b — то есть решить, например, $5^a \equiv 8 \pmod{23}$. Это и есть задача дискретного логарифма.

Для $p=23$ её легко решить перебором. Но в реальности берут p длиной в сотни цифр — и тогда перебор невозможен даже для всех компьютеров мира, хотя сами Алиса и Боб считают свои степени за доли секунды (быстрое возведение из урока 4!).

> 🤔 **А знаешь ли ты?** Диффи и Хеллман опубликовали свою идею в статье с говорящим названием «Новые направления в криптографии». Она перевернула всё: впервые люди, никогда не встречавшиеся и не имевшие общего секрета, смогли безопасно договориться. Сегодня этот обмен происходит каждый раз, когда ты открываешь сайт по https.

✍️ Разбор примера

Задача: Алиса и Боб используют $p = 23$, $g = 5$. Секрет Алисы $a = 4$, секрет Боба $b = 3$. Найди общий секрет.

Шаг 1 — открытые числа:

- $A = 5^4 \bmod 23$. $5^2 = 25 \equiv 2$, значит $5^4 \equiv 2^2 = 4$. Итак $A = 4$.
- $B = 5^3 \bmod 23 = 125 \bmod 23$. $125 = 5\cdot 23 + 10$, значит $B = 10$.

Шаг 2 — общий секрет (каждый своим путём):

- Алиса: $B^a = 10^4 \bmod 23$. $10^2 = 100 \equiv 8$, тогда $10^4 \equiv 8^2 = 64 \equiv 18$.
- Боб: $A^b = 4^3 \bmod 23 = 64 \equiv 18$.

Оба получили **18** — совпало. ✅

📝 Задачи

1. Своими словами объясни, какое свойство красок делает аналогию с обменом ключами работающей.
2. При $p=23$, $g=5$ Алиса выбрала секрет $a=2$. Какое открытое число A она пошлёт?
3. При тех же p, g Боб выбрал $b=2$. Найди B, а затем общий секрет (учти, что у обоих секрет равен 2).
4. Что именно из перечисленного знает подслушивающий: p, g, A, B, a, b, общий секрет? Выпиши только то, что открыто.
5. Как называется трудная задача, которую пришлось бы решить подслушивающему, чтобы найти секрет?
6. Почему в настоящей системе берут очень большое простое p, а не $p=23$?
7. Объясни с помощью равенства степеней, почему Алиса и Боб гарантированно получают одно и то же число.
8. *Со звёздочкой.* Диффи–Хеллман даёт двоим общий секрет, но сам по себе **не** защищает от «человека посередине», который подменяет сообщения.

Подумай, как злоумышленник, вставший между Алисой и Бобом, мог бы обмануть обоих. (Достаточно идеи.)