Урок 6. Идея RSA

Криптография · ~35 минут

Диффи–Хеллман позволяет договориться о секрете. А RSA идёт дальше: он даёт каждому **два ключа** — один открытый, чтобы тебе писали, и один закрытый, чтобы читать мог только ты. Именно на RSA (и его родственниках) держатся банки, мессенджеры и электронные подписи. Сегодня ты соберёшь работающий RSA из маленьких чисел своими руками.

🎯 Что ты узнаешь

- Почему перемножить два простых легко, а разложить обратно — трудно.
- Что такое открытый и закрытый ключи.
- Как устроено шифрование и дешифрование в RSA.
- Соберёшь маленький, но настоящий пример и проверишь его.

📖 Разбираемся в теме

Односторонняя дверь

Перемножить два простых числа проще простого: $3 \cdot 11 = 33$. А теперь наоборот — тебе дали число 33 и просят найти множители. Для 33 легко. Но если дать произведение двух **200-значных** простых, то разложить его обратно не сможет ни один суперкомпьютер за время жизни Вселенной.

> 📌 **Запомни:** RSA стоит на асимметрии: **умножать простые легко, а раскладывать произведение (факторизовать) — трудно**. Это «односторонняя дверь»: пройти в одну сторону просто, обратно — почти нельзя.

Открытый и закрытый ключ

У каждого человека есть **пара ключей**:

- **Открытый ключ** — его можно публиковать где угодно. Им шифруют сообщения тебе.
- **Закрытый ключ** — только твой, хранится в тайне. Только им можно расшифровать.

Это как почтовый ящик: щель для писем видна всем (открытый ключ, любой бросит письмо), а ключ от дверцы — только у тебя (закрытый ключ).

Как строят ключи

1. Берут два простых p и q, считают $n = p\cdot q$.
2. Считают $\varphi = (p-1)(q-1)$ (это «функция Эйлера» от n; для нас — просто число).
3. Выбирают открытую экспоненту e, взаимно простую с φ.
4. Находят закрытую экспоненту d — обратный к e по модулю φ (из урока 4!): $e\cdot d \equiv 1 \pmod{\varphi}$.

- **Открытый ключ:** пара (n, e).
- **Закрытый ключ:** число d.

Шифрование и дешифрование

Сообщение — это число m (меньше n). Тогда:

$$\text{шифр: } c = m^e \bmod n, \qquad \text{расшифровка: } m = c^d \bmod n.$$

Магия в том, что возведение сначала в степень e, а потом в степень d **возвращает исходное число** — потому что e и d подобраны как взаимно обратные по модулю φ.

Собираем настоящий пример

Возьмём совсем маленькие простые:

- $p = 3$, $q = 11$ → $n = 33$.
- $\varphi = (3-1)(11-1) = 2 \cdot 10 = 20$.

- Выберем $e = 7$. Проверим: $\gcd(7, 20) = 1$ — годится.
- Найдём d: нужно $7d \equiv 1 \pmod{20}$. Перебираем: $7\cdot 3 = 21 \equiv 1 \pmod{20}$. Значит $d = 3$.

Итак: **открытый ключ $(n,e) = (33, 7)$**, **закрытый ключ $d = 3$**.

Зашифруем число $m = 2$: $$c = 2^7 \bmod 33 = 128 \bmod 33.$$ $128 = 3\cdot 33 + 29$, значит $c = 29$.

Расшифруем $c = 29$: $$m = 29^3 \bmod 33.$$ Считаем по шагам (с остатками): $29^2 = 841$, а $841 = 25\cdot 33 + 16$, значит $29^2 \equiv 16$. Тогда $29^3 \equiv 16 \cdot 29 = 464$, и $464 = 14\cdot 33 + 2$, то есть $29^3 \equiv 2 \pmod{33}$.

Получили обратно **2** — исходное сообщение! ✅ RSA работает.

> 💡 Проверим шифр ещё на паре чисел (открытый ключ (33,7), закрытый d=3):
>
> - $m=5$: $c = 5^7 \bmod 33 = 14$, обратно $14^3 \bmod 33 = 5$. ✅
> - $m=9$: $c = 9^7 \bmod 33 = 15$, обратно $15^3 \bmod 33 = 9$. ✅

Зачем это в интернете

Когда ты заходишь на сайт банка, он присылает тебе свой **открытый ключ**. Твой браузер шифрует им секрет — и расшифровать его сможет только банк своим закрытым ключом. Никто по дороге, даже провайдер, прочитать не может. Так работает защищённое соединение (https), в котором RSA и его родня играют главную роль.

> 🤔 **А знаешь ли ты?** Буквы RSA — это фамилии трёх учёных: Ривест, Шамир и Адлеман, опубликовавших схему в 1977 году. Позже выяснилось, что похожую идею несколькими годами раньше придумал британский математик Клиффорд Кокс, но его работа была засекречена разведкой и вышла на свет лишь в 1997-м.

⚠️ Наш пример с $n=33$ ломается мгновенно: любой сразу увидит, что $33 = 3\cdot 11$, и вычислит d. Безопасность появляется только при огромных p и q. Маленькие числа мы взяли, чтобы всё можно было посчитать на бумаге.

✍️ Разбор примера

Задача: с открытым ключом $(n,e) = (33, 7)$ и закрытым $d = 3$ зашифруй число $m = 4$ и расшифруй результат обратно.

Шифрование: $c = 4^7 \bmod 33$.

- $4^2 = 16$
- $4^4 = 16^2 = 256 \equiv 25 \pmod{33}$ (256 = 7·33 + 25)
- $4^7 = 4^4 \cdot 4^2 \cdot 4^1 \equiv 25 \cdot 16 \cdot 4$.
- $25\cdot 16 = 400 \equiv 4 \pmod{33}$ (400 = 12·33 + 4), затем $4\cdot 4 = 16$.

Значит $c = 16$.

Дешифрование: $m = 16^3 \bmod 33$.

- $16^2 = 256 \equiv 25$, затем $25 \cdot 16 = 400 \equiv 4 \pmod{33}$.

Получили **4** — исходное число. ✅

📝 Задачи

Во всех задачах, где не сказано иное, используй ключи из урока: $n = 33$, $e = 7$, $d = 3$.

1. Чему равны n и φ, если $p = 3$, $q = 11$? Покажи вычисление.
2. Проверь, что $e = 7$ и $d = 3$ действительно взаимно обратны по модулю $\varphi = 20$ (то есть $7\cdot 3 \equiv 1$).
3. Зашифруй число $m = 8$ открытым ключом $(33, 7)$.

4. Расшифруй результат из задачи 3 закрытым ключом $d=3$ и убедись, что получил обратно 8.
5. Зашифруй число $m = 10$. (Тут будет забавный результат — приглядись к нему.)
6. Возьми другие простые: $p = 5$, $q = 11$. Найди n и φ.
7. Почему сообщение m обязательно должно быть **меньше** n?
8. *Со звёздочкой.* Объясни своими словами, что именно делает RSA безопасным: почему, зная открытый ключ (n, e), злоумышленник всё равно не может найти d?