Простые числа

1 Проверка на простоту

N - простое?

$2 \dots \sqrt{N}$ - проверить

$|N| = \log N = n$

Нужно перебрать $2^{\log \sqrt{N}} = 2^{n/2}$ чисел.

$N = a \cdot b$ $\quad$ a или $b \le \sqrt{N}$

2. Малая т. Ферма

$a^{p-1} \equiv 1 \pmod p$, p - простое, НОД$(a,p) = 1$

3. Тест Ферма

N - простое? $\quad a^{N-1} \equiv 1 \pmod N$ → ДА (простое?) / → НЕТ (составное)

возьмем $a < N$

∃ числа для кот. тест Ферма всегда ошиб. $\quad$ ‖ Числа Кармайкла ‖ $\quad$ для a вз. прост. с N

Утв: ∃ N - составное и $a^{N-1} \not\equiv 1 \pmod N$

НОД$(a, N) = 1$

$\Rightarrow \ge 1/2$ всех $a < N$ не проходят тест.

▷ Возьмём b: $\underline{b}^{N-1} \equiv 1 \mod N$

$\leftarrow$ $\underline{c = (a \cdot b)}$ $\quad \underline{c}^{N-1} = a^{N-1} \cdot b^{N-1} \equiv a^{N-1} \not\equiv 1 \pmod N$

$\forall$ b - плохого $\exists$ c - хорошее.

$\{b\} \longleftrightarrow \{c\}$ — биекция

$b \to c = a \cdot b$

$c \to b = a^{-1} \cdot c$

$\Rightarrow$ # b - проход тест $\leq 1/2$ $\triangleleft$

Следствие:

$P[$Ферма тест. ошибётся на $N \mid N$ - не число Карм.$] \leq \frac{1}{2}$

Если повторить 10 раз $\Rightarrow$ $P[\dots] \leq \frac{1}{2^{10}} < 0.001$

Пример:

$N \in [1 \dots 2.5 \cdot 10^9]$

$a = 2$

Тест Ферма для $\forall N$

ошибок $\approx 2 \cdot 10^4$ $\Rightarrow$ $P[\dots] = 10^{-5}$

$\equiv$ Индустриальные простые числа

Числа Кармайкла

$561 = 3 \cdot 11 \cdot 17$

$a^{560} \equiv 1 \pmod{561}$ $\forall a$: НОД$(a, 561) = 1$

Тест Рабина-Миллера

Ферма тест + доп. проверка

$N - 1 = 2^t u$, u - нечётное

Проверим все: $a^u, a^{2u}, a^{4u}, \dots, a^{2^t u}$

Если среди них есть числа отличные от ± 1

$\Rightarrow$ мы найдём нетривиальный корень из 1

$\Rightarrow N$ – составное

Вероятность ошибки $\leq \frac{1}{4}$

Детерминированный алг-м проверки простоты

Как генерировать простые числа?

$\pi(N)$ – # простых $< N$

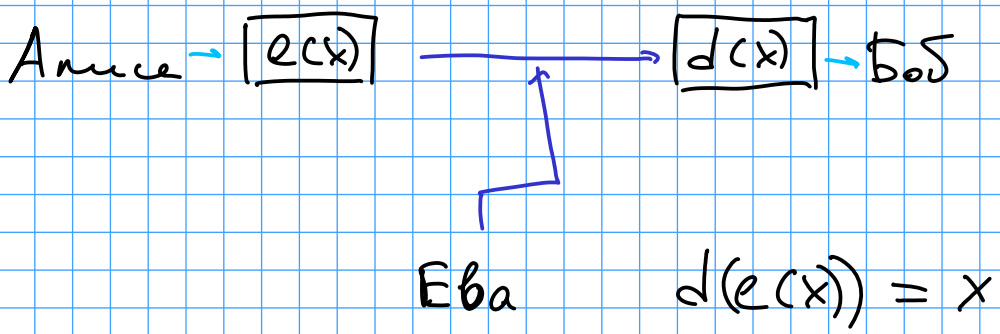
$\pi(N) \approx N / \ln N$

Следствие: Случайное и битовое число будет простым с вер-тью $\sim 1/n$

Повторим n раз $\Rightarrow$ вер-ть не найти простое

$\sim \left(1 - \frac{1}{n}\right)^n \sim \frac{1}{e}$

RSA



1. One-time pad

В блокноте – случайные биты

$P_2[x \oplus_2 = 1] = \frac{1}{2} p + \frac{1}{2}(1-p)$

$x \oplus r \longrightarrow c$ – случайная

↑ случайная

$((x \oplus r) \oplus r) \longrightarrow x$

* 2 сообщ. с одним блокнотом

$(x \oplus 2) \oplus (y \oplus 2) \rightarrow x \oplus y$

2. Secret Key

Алиса и Боб знают секретный ключ K

Они используют нек-ую функцию f для генерации псев-ти бит, похожую на случайную (AES).

m - сообщ. разбивают на блоки фикс. длины (например, 128, 192, 256 бит)

$m = (m_1, m_2, m_3, \dots, m_l)$

$e(m) = (f(k,1) \oplus m_1), (f(k,2) \oplus m_2), \dots,$

Функция f сложно обратима

3. Public Key

Алиса $\rightarrow$ [e(x, k'p)] ——— [d(c, ks)] $\rightarrow$ Боб

(k_p, k_s) (k'_p, k'_s)

публичный; знает только Алиса; Ева

c, k_p, k'_p

RSA $N = p \cdot q$, p, q - простые

e - вз. прост. с $(p-1)(q-1)$

d: $e \cdot d = 1 \mod (p-1)(q-1)$

$k_p = (N, e)$ $k_s = (N, d)$

$e(x, k_p) = x^e \pmod N$ $\quad e = 65537$

$d(c, k_s) = c^d \pmod N$

$d(e(x, k_p), k_s) = x^{ed} \equiv x \pmod N$

Задача ЕВСИ: $(N, k_p, x^e) \xrightarrow{\text{сложно}} x$

Утв:

$x^{ed} \equiv x \pmod N$

$ed \equiv 1 \pmod{(p-1)(q-1)}$

$ed = k(p-1)(q-1) + 1, \quad k \in \mathbb{Z}$

$x^{ed} \equiv x \pmod N \iff x^{ed} - x \vdots N$

$x^{k(p-1)(q-1)+1} - x \vdots N$

$x\left(x^{k(p-1)(q-1)} - 1\right)$

По м.т. Ферма $\begin{matrix} \vdots p \\ \vdots q \end{matrix} \Rightarrow \vdots p \cdot q$