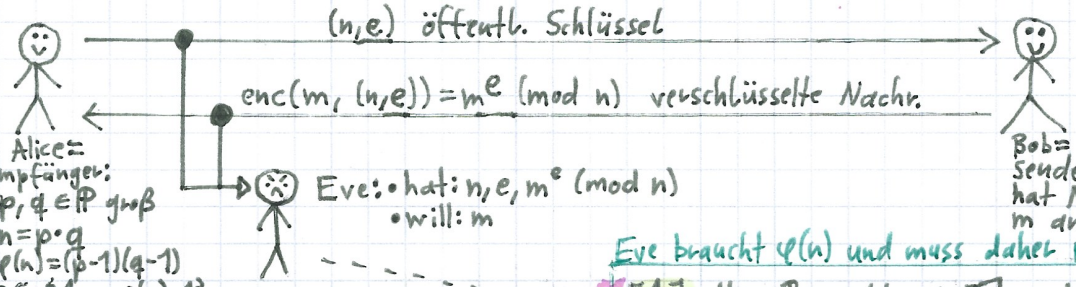
Eigenes „Gesamtbild" CRYPTO1 – „Faktorisierung I+II" (VL vom 1.6.22+15.6.) 1./2./3./4.6.22 & 16.6.

RSA (Rivest, Shamir, Adleman) zw. Alice & Bob:



Wie findet Alice große Primzahlen?:

Strategie: • Wähle $x \in_R 2\mathbb{N}+1$ zufällig & groß.
• Wende Primzahltest an (s.u.).
↳ Nein: $x \leftarrow x+2$.

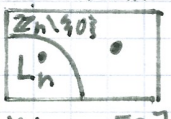
Abstrakter Primzahltest (für n):

$\mathbb{Z}_n^*$ = invertierbare Elemente in $\mathbb{Z}_n$

Idee: $\mathbb{Z}_n^* = \mathbb{Z}_n \setminus \{0\}$ gdw. n prim
↳ Beweis: $n \in \mathbb{P} \Rightarrow \mathbb{Z}_n^* = \{x \mid ggT(x,n)=1\} = \{1,\dots,n-1\}$
$n \notin \mathbb{P} \Rightarrow n = a \cdot b \equiv 0 \Rightarrow$ Nullteiler

Test: Konstruiere $L_n \subseteq \mathbb{Z}_n \setminus \{0\}$ mit Eig.:
[1] $x \in L_n$ schnell prüfbar
[2] $n \in \mathbb{P} \Rightarrow L_n = \mathbb{Z}_n^* = \mathbb{Z}_n \setminus \{0\}$
[3] $n \notin \mathbb{P} \Rightarrow \exists 0 < c < 1 : |L_n| \leq c \cdot (n-1)$

Dann: 1.) Wähle $x \in_R \mathbb{Z}_n \setminus \{0\}$ zufällig
2.) Prüfe mit [1], ob $x \in L_n$.
3.) $\}_q$: Wiederhole 1.)
Nein: $n \notin \mathbb{P}$ wegen [2]



Wegen [3] gilt für jedes x: $P[x \in L_n] = \frac{|L_n|}{n-1} \leq c$ und damit insg. $P[x_1,\dots,x_t \in L_n] \leq c^t$, d.h. mit Anzahl Schritte t groß genug ist Wk. für falsch-positive Antw. beliebig klein

Konkreter Primzahltest #1: Fermat

$L_n := \{x \in \mathbb{Z}_n \setminus \{0\} \mid x^{n-1} = 1\} \subseteq \mathbb{Z}_n^*$ (klar)
[1] ✓ wegen Square & Multiply
[2] ✓ da Element hoch Gruppenord. immer 1
[3] ↯ wenn n „eine Carmichael-Zahl", dann $|L_n| = \varphi(n) \approx n$ „zu groß" (kleinste: 561)

n ist Carm.-Zahl gdw. $a^{n-1} \equiv 1 \pmod n$ für alle a mit $ggT(n,a)=1$ (für alle a mit $ggT(n,a) \neq 1$ gilt $a^{n-1} \neq 1$ da sonst $\neq a$ invertierbar wäre!)

Element hoch Gruppenordnung = 1

Konkreter Primzahltest #2: Miller-Rabin

$L_n := \{x \in \mathbb{Z}_n \setminus \{0\} \mid x^{n-1} = 1 \wedge \forall 0 \leq j \leq h-1 : x^{2^j \cdot m} = 1 \Rightarrow x^{2^j \cdot m} = \pm 1\}$

Vor.: n ist ungerade: $n-1 = 2^h \cdot m$, m ungerade
[1] $[x^m, (x^m)^2, (x^m)^4, (x^m)^8, \dots, (x^m)^{2^h \cdot m = n-1}]$ enthält nur Einsen; od. $n-1$ als Element?!
[2] $n \in \mathbb{P}$: $x^2 \equiv 1 \pmod n \Rightarrow n \mid x^2-1 \Rightarrow x \equiv \pm 1$.
[3] $n \notin \mathbb{P}$: $|L_n| \leq \frac{1}{4}(n-1)$, d.h. $c = \frac{1}{4}$ (aufw. z.z.!)

$(n-1)^2 \equiv 1 \pmod n$

Warum gilt $dec(c,d) = c^d \pmod n = m$?:

$\Leftrightarrow m^{ed} \equiv m \pmod n$
$\Leftrightarrow m^{ed} = (m^{\varphi(n)})^k \cdot m \pmod n$
$\Leftrightarrow ed = k \cdot \varphi(n) + 1 \Leftrightarrow d = e^{-1} \pmod{\varphi(n)}$

Eve braucht φ(n) und muss daher n faktorisieren:

[1] alle Primzahlen $\leq \sqrt{N}$ probieren (trial division) $\Rightarrow O(\sqrt{N})$

[2] Pollard-ρ: Laufe mit x_i, y_i zufällig durch $\mathbb{Z}_n$ bis ne Kollision mod p, d.h. $x_i \equiv y_i \pmod p \Rightarrow p \mid x_i - y_i \Rightarrow ggT(x_i - y_i, N) = p$. ■ $\Rightarrow O(\sqrt{p}) = O(\sqrt[4]{N})$

[3] Pollard-p-1: Annahme: p-1 ist B-potenzglatt, d.h. die maximale Primzahlpotenz, die p-1 teilt, ist $\leq B$.
$M(B) := \prod_{\pi_i \in \mathbb{P}} \pi_i^{e_i}$ mit $\pi_i^{e_i} \leq B$ und e_i maximal.
Dann gilt $p-1 \mid M(B)$. Außerdem gilt für ein $a \in \mathbb{Z}_p^*$: $a^{p-1} = 1 \bmod p \Rightarrow p \mid a^{p-1}-1$
$\Rightarrow p = ggT(a^{p-1}-1, N) = ggT(a^{M(B)}-1, N)$ ■

[4] ECM/Lenstra (3. schnellste bekannte Meth.):
Wähle $E_{a,b}$ über $\mathbb{Z}_n$ u. $P_0 \in_R E_{a,b}$ zufällig.
$P_j = 2 \cdot P_{j-1}$; Punktverdopplung involviert Berechnung von $m = \frac{3x_1^2+a}{2y_1}$; irgwann „knallts" weil Nenner nicht invertierbar ist; mit allergrößter Wk. teilt dann p oder q diese Zahl
$\Rightarrow O(\exp[(\sqrt{2}+o(1))\sqrt{\ln p \ln\ln p}])$

[5] Fermat ($p \approx q$): Beob.: $p \cdot q = \frac{1}{4}[(p+q)^2 - (p-q)^2]$
$\Leftrightarrow \left(\frac{p+q}{2}\right)^2 - N = \left(\frac{p-q}{2}\right)^2 \Leftrightarrow t^2 - N = s^2$;
kombiniere mit trial division! $t_0 = \lceil\sqrt{N}\rceil$; $t_i = t_{i-1}+1$; sobald $t_i^2 - N$ Quadratzahl, faktorisiere: $N = t_i^2 - s^2 = (t_i - s)(t_i + s)$ ■

[6] Quadratisches Sieb (#2.): Durchsiebe $t_0^2 - N, \dots, t_k^2 - N$ aus Fermat nach B-glatten Zahlen: $t_i^2 - N = p_1^{e_{i1}} \cdot \dots \cdot p_s^{e_{is}}$
Löse ein LGS in $y_0, \dots, y_k$ über $\mathbb{Z}_2$, sodass:
$(t_0^2 - N)^{y_0} \cdot \dots \cdot (t_k^2 - N)^{y_k} = T^2$. $S := t_0^{y_0} \cdot \dots \cdot t_k^{y_k}$.
$S^2 = T^2 \pmod n \Rightarrow N \mid (S-T)\cdot(S+T)$
Falls $N \nmid (S-T) \wedge N \nmid (S+T)$: $ggT(N, S+T) \in \{p, q\}$ ■
$\Rightarrow O(\exp[(1+o(1))\sqrt{\ln n \ln\ln n}])$

QS = Fermat + Pollard

[7] Zahlkörpersieb (1. schnellste Meth.) → VL nur Skizze

By the way geht das Ganze auch umgekehrt: $n, \varphi(n) \Rightarrow p, q$.

$\varphi(n) = (p-1)(q-1) = pq - p - q + 1 = n - p - q + 1$
$\Rightarrow p + q = n - \varphi(n) + 1$
Damit lassen sich die Nullstellen von
$x^2 - [n - \varphi(n) + 1]x + n$
$= x^2 - (p+q)x + pq$
$= (x-p)\cdot(x-q)$
bestimmen; bei diesen handelt es sich um p & q.