Kryptologie: Übungsblatt 11, Besprechung ab dem 9.7.2018, 10:15, H20

100.) Wir betrachten den ϱ-Algorithmus von Pollard für das Faktorisieren auf einer Eingabe $n = p \cdot q$ und nehmen an, dass für $i = 5$ und $j = 9$ gilt, dass die Pseudozufallszahlen x_i und x_j kongruent sind modulo p. Wir sagen: an der Position $(i, j) = (5, 9)$ liegt ein "Treffer" vor.

Geben Sie alle weiteren Trefferpositionen mit $j \leq 20$ an. Stellen Sie diese in einem 2-dimensionalen (i, j)-Koordinatensystem dar.

Bei der Floyd'schen Cycle Detection-Methode werden die Positionen $(k, 2k)$, $k = 1, 2, 3, \ldots$, überprüft. Wann findet diese Methode hier einen Treffer? Tragen Sie diese Koordinaten ebenfalls in das Diagramm ein.

101.) Bei der Fermat-Faktorisierung startet man, bei Eingabe n, mit $x = \lceil \sqrt{n} \rceil$ und $z = x^2 - n$ und testet in jedem Schleifendurchlauf, ob z eine Quadratzahl ist, also $z = y^2$. Ansonsten wird im nächsten Durchlauf x um 1 erhöht und dementsprechend z neu berechnet.

Führen Sie diesen Algorithmus durch, um $n = 2923$ zu faktorisieren.

102.) Die Fermat-Faktorisierung ist bei Eingabe $n = p \cdot q$ dann besonders effizient, wenn die Faktoren p und q sehr nahe beieinander liegen.
Bei RSA erzeugen wir eine (z.B.) 1000-Bitzahl n mit Hilfe einer 499-Bit Primzahl p und einer 501-Bit Primzahl q. Kann man hier sagen, dass p und q "sehr nahe beieinander" liegen, so dass man mit einer schnelleren Faktorisierung (als andere Methoden) rechnen kann?

103.) Bei der Baby-Step-Giant-Step-Methode zur Bestimmung des Diskreten Logarithmus wird (bei Eingabe n, a, y) das gesuchte x mit $y = a^x \bmod n$ zerlegt in x_1, x_2 so dass $x = x_1 \cdot \lceil \sqrt{n} \rceil + x_2$. Dementsprechend muss die Gleichung $u^{x_1} = y \cdot v^{x_2}$ gelöst werden (wobei $u = a^{\lceil \sqrt{n} \rceil}$ und $v = a^{-1}$).
Hierzu werden die zwei Listen $\mathcal{L}_1 = \{(x_1, u^{x_1}) \mid x_1 = 0, 1, \ldots, \lfloor \sqrt{n} \rfloor\}$ und $\mathcal{L}_2 = \{(x_2, y \cdot v^{x_2}) \mid x_2 = 0, 1, \ldots, \lfloor \sqrt{n} \rfloor\}$ auf ein gemeinsames Element untersucht. Dieses liefert dann x_1, x_2.

Führen Sie dies durch für $n = 137$, $a = 3$ und $y = 11$ (vgl. Aufgabe 97).

104.) Wir ermitteln den diskreten Logarithmus von $y = 20$, modulo der Primzahl $n = 59$, zur Basis $a = 2$, nach der Pollard-ϱ-Methode. Die Grundmenge wird aufgeteilt in die 3 Bereiche $M_1 = \{1, \ldots, 19\}$, $M_2 = \{20, \ldots, 38\}$, $M_3 = \{39, \ldots, 58\}$. Gestartet wird mit $z = a^1 y^1 = 40$. (Alle Rechnungen sind modulo 59.) Wenn z in den Bereich M_1 fällt, so wird der Exponent bei a um 1 erhöht (d.h. z mit a multipliziert). Wenn z in den Bereich M_2 fällt, so wird der Exponent bei y um 1 erhöht (d.h. z mit y multipliziert). Wenn z in den Bereich M_3 fällt, so werden beide Exponenten verdoppelt (d.h. z quadriert). Dies wird solange durchgeführt, bis bei den auftretenden z-Werten eine Dublette vorliegt. Führen Sie dies durch.

105.) Zur Erinnerung: $\psi(n, B)$ gibt die Anzahl der Zahlen $z \leq n$ an, die B-smooth sind, die sich also in Primfaktoren $\leq B$ zerlegen lassen.
Berechne $\psi(n, B)$ für $n = 25$ und $B = 5$ (bzw. $B = 10$). Vergleiche mit der Approximationsformel $\psi(n, B) \approx n \cdot u^{-u}$ wobei $u = \log(n)/\log(B)$.

106.) Bei der Index Calculus-Methode zur Berechnung des Diskreten Logarithmus werden bei Eingabe n Zufallszahlen $z < n$ gezogen und darauf gehofft, dass z B-smooth ist, sich also ausschließlich mit Primfaktoren $\leq B$ faktorisieren lässt. Insgesamt muss man eine Menge solcher Zahlen z finden, die mit der Mächtigkeit der jeweiligen Faktorbasis übereinstimmt. Dazu ist es wichtig, den Parameter B, der die Größe der Faktorbasis bestimmt, geeignet festzulegen.

Im Folgenden legen wir $n = 137$ fest. Die Tabelle zeigt die $\psi(n-1, B)$-Werte für verschiedene B. Man finde dasjenige B, das die erwartete Suchzeit, bis die entsprechende Menge an verschiedenen z-Werten gefunden ist, minimiert.
(Hinweis: die Berechnung dieser Erwartungswerte ähnelt dem "Coupon Collector Problem".)

B	$\psi(136, B)$	Faktorbasis
2	7	$\{2\}$
3	21	$\{2, 3\}$
5	38	$\{2, 3, 5\}$
7	53	$\{2, 3, 5, 7\}$
11	65	$\{2, 3, 5, 7, 11\}$
13	75	$\{2, 3, 5, 7, 11, 13\}$

107.) Sei $n = 137$ (Primzahl) und $a = 5$ Primitivwurzel modulo n. Wir legen die Faktorbasis $\{2, 3\}$ fest. In der ersten Phase der Index Calculus-Methode werden die diskreten Logarithmen der Primzahlen in der Faktorbasis bestimmt. Nach einigen Versuchen mit zufälligen Exponenten stellen wir fest, dass

$$5^{10} \bmod 137 = 128 = 2^7 \quad \text{und} \quad 5^{13} \bmod 137 = 108 = 2^2 \cdot 3^3$$

Bestimmen Sie die diskreten Logarithmen von 2 und von 3 zur Basis 5 modulo 137.