Kryptologie: Übungsblatt 10, Besprechung ab dem 2.7.2018, 10:15, H20

92.) Wir definieren hier eine Einwegfunktion als eine bijektive Funktion $f : \{0,1\}^* \to \{0,1\}^*$, $|f(x)| = |x|$, so dass $f \in P$ und $f^{-1} \notin P$.

Zeige: Wenn eine derartige Einwegfunktion existiert, dann folgt P $\neq$ NP.

(Beweisidee: Nimm an, dass eine solche Einwegfunktion f existiert. Konstruiere ein geeignetes Entscheidungsproblem A_f in NP. Unter der indirekten Beweis-Annahme P $=$ NP folgt dann $A_f \in$ P. Mit Hilfe dieser Tatsache konstruiere einen polynomialen Algorithmus, der f^{-1} berechnet. Dies ist dann ein Widerspruch, der beweist, dass P $\neq$ NP.)

93.) Teste mit dem Solovay-Strassen-Primzahltest, ob 561 eine Primzahl ist. (Bemerkung: dies ist keine Primzahl, sondern eine Carmichaelzahl.)
Verwende hierzu die Basiszahl 5. Das heißt, teste ob

$$\left(\frac{5}{561}\right) \equiv 5^{(561-1)/2} \pmod{561}$$

Für die linke Seite benötigt man die Prozedur *Jacobi*, für die rechte Seite die modulare Exponentiation.

94.) Wir wollen die Quadratwurzeln von 11 modulo der Primzahl 37 berechnen. Tatsächlich ist 11 ein quadratischer Rest, denn $11^{36/2} \equiv 1 \pmod{37}$.
Wir vermerken für spätere Verwendung, dass $b = 2$ kein quadratischer Rest ist, denn $2^{36/2} \equiv -1 \pmod{37}$.
Außerdem hat die Primzahl 37 die Form $37 \equiv 1 \pmod 4$. Dies ist der schwierigere der beiden Fälle bei der Quadratwurzelberechnung modulo einer Primzahl.
Wir wünschen uns einen ungeraden Exponenten bei der 11, daher berechnen wir nun $11^{36/4} = 11^9 \equiv -1 \pmod{37}$.
Da diese Berechnung nicht 1 ergibt, sondern -1, kommen wir so nicht weiter; wir müssen nun $b = 2$ ins Spiel bringen. Führen Sie dies aus.

95.) Gegeben sei $n = p \cdot q$ mit $n = 437$, $p = 19$, $q = 23$. Bestimmen Sie a und b in $\mathbb{Z}_n^*$ mit

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{a}{q}\right) = 1 \cdot 1 = 1 \quad \text{und} \quad \left(\frac{b}{n}\right) = \left(\frac{b}{p}\right) \cdot \left(\frac{b}{q}\right) = (-1) \cdot (-1) = 1$$

96.) Geben Sie alle quadratischen Reste in $\mathbb{Z}_{45}^*$ an! Sie dürfen hierzu folgende Tabelle verwenden, die den Isomorphismus zwischen $\mathbb{Z}_5^* \times \mathbb{Z}_9^*$ und $\mathbb{Z}_{45}^*$ gemäß des Chinesischen Restsatzes wiedergibt. Es genügt, die quadratischen Reste in der Tabelle zu kennzeichnen.

	1	2	4	5	7	8
1	1	11	31	41	16	26
2	37	2	22	32	7	17
3	28	38	13	23	43	8
4	19	29	4	14	34	44

97.) Angenommen, Sie wissen, dass $3^6 \equiv 44$ (mod 137) und $3^{10} \equiv 2$ (mod 137).

Finde eine Zahl $x \in \{0, 1, \ldots, 135\}$ so dass $3^x \equiv 11$ (mod 137).

98.) Der $(p-1)$-Algorithmus von Pollard startet mit (z.B.) $a = 2$ und berechnet in jedem Schritt a neu zu a^i mod n, wobei i in jedem Schritt um 1 erhöht wird. Dabei wird jedesmal getestet, ob $ggT(a-1, n)$ einen nicht-trivialen Teiler von n ergibt.

Führen Sie dies durch mit $a = 2$ und $n = 24823$.

Es gilt $24823 = 103 \cdot 241$. Sagen Sie voraus, welcher der beiden Faktoren hierbei zuerst gefunden wird.

99.) Der ϱ-Algorithmus von Pollard soll die Zahl 1219 faktorisieren. Man startet mit einer beliebigen Zahl, zum Beispiel $x_1 = 20$ und berechnet die Nachfolgerzahlen mittels $x_{i+1} = ((x_i)^2 + 1)$ mod 1219. Man testet dabei, ob $ggT(x_k - x_{2k}, n)$ für $k = 1, 2, 3, \ldots$ einen nicht-trivialen Teiler von $n = 1219$ ergibt. Führen Sie dies durch.