Mathematik und Logik

6. Übungsaufgaben

2006-01-17

1. Berechnen Sie für das Konto 204938716 bei der Bank mit der Bankleitzahl 54000 den IBAN. Das Verfahren ist z.B. auf `http://de.wikipedia.org/wiki/International_Bank_Account_Number` beschrieben. Wie hilft dabei modulare Arithmetik? Wiederholen Sie dies für Ihr eigenes Konto, und verwenden Sie `www.iban-rechner.de` oder ähnliche Tools nur zum Überprüfen.

2. Berechnen Sie $2^{340} \bmod 341$. Glauben Sie, daß 341 eine Primzahl ist?

3. Wiederholen Sie das vorige Beispiel mit der Basis 3. Was stellen Sie fest?

4. Wählen Sie $p = 11$ und $q = 23$ als „große" Primzahlen. Sei $m = pq$; bestimmen Sie $\varphi(m)$, und wählen Sie ein e relativ prim zu $\varphi(m)$.

5. Bestimmen Sie zu e aus dem vorigen Beispiel ein passendes d mit mit $de \equiv 1 \pmod{\varphi(m)}$.

6. Wählen Sie ein $x\colon \mathbb{Z}_m$, bestimmen Sie $y = x^e$ und rechnen Sie nach, ob $y^d = x$ ist. Wiederholen Sie das Beispiel für mehrere x.

7. Alice verwendet den/die Schlüssel aus den obigen Beispielen. Der öffentliche Schlüssel von Bob sei $m = 323$, $e = 5$. Alice will Bob die geheime Nachricht 16 mitteilen. Was muß sie versenden?

8. Bob hat die Nachricht empfangen; diese überrascht ihn aber, und er hat Zweifel, ob sie tatsächlich von Alice stammt. Er bittet sie daher, ihre Nachricht zusätzlich zu signieren. Was muß Alice nun schicken?

9. Alice erfährt, daß Bob ein Verhältnis mit Carol hat, was ihr überhaupt nicht paßt. Sie will daher eine gefälschte von Bob signierte Nachricht (die Zahl 66 bedeute: „ich will nichts mehr mit dir zu tun haben") an Carol schicken. Was muß sie tun?

10. Schreiben Sie ein kurzes rekursives Programm, welches $x^e \bmod m$ für beliebige ganze Zahlen x, e, m effizient berechnet.

11. Dasselbe für den (erweiterten) Euklidischen Algorithmus. (Input: (m, n), Output: (d, x, y), sodaß $d = m \cdot x + n \cdot y$)

12. Verwenden Sie diese Programme, um die vorigen Beispiele mit zumindest 4-stelligen Zahlen zu berechen. Noch besser arbeiten Sie mit 100-stelligen Zahlen, falls ihr Programm das unterstützt.

13. Wieviele Leute kennen sich mit Hexadezimalzahlen aus, wenn nur Sie und fade Leute sich damit auskennen?

    Hinweis: Hexadezimalzahlen sind wie Dezimalzahlen, aber zur Basis 16 (statt 10). Für die über 9 hinausgehenden Ziffern verwendet man dann meist die Buchstaben A bis F (auch als Kleinbuchstaben).