Mathematik und Logik

8. Übungsaufgaben

2007-01-23

1. Berechnen Sie $2^{340} \bmod 341$. Glauben Sie, daß 341 eine Primzahl ist?
2. Wiederholen Sie das vorige Beispiel mit der Basis 3. Was stellen Sie fest?
3. Wählen Sie $p = 11$ und $q = 23$ als „große“ Primzahlen. Sei $m = pq$; bestimmen Sie φ, und wählen Sie ein e relativ prim zu φ.
4. Bestimmen Sie zu e aus dem vorigen Beispiel ein passendes d mit mit $de \equiv 1 \pmod{\varphi}$.
5. 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.
6. 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?
7. Bob hat die Nachricht empfangen; sie 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?