

39. Aufgabe

a) Seien $n = 1147$ und $e = 29$. Dann ist (n, e) der öffentliche Schlüssel, mit dem der Geheimtext verschlüsselt worden ist. Zum Entschlüsseln wird der geheime Schlüssel (n, d) von A benötigt.

$$\text{Es gilt: } n = 31 \cdot 37, \quad \varphi(n) = 30 \cdot 36 = 1080$$

$$\text{ggT}(e, \varphi(n)) = 1, \quad 149 \cdot e + (-4) \cdot 1080 = 1$$

Also ist $(1147, 149)$ der geheime Schlüssel von A , mit dem der Geheimtext entschlüsselt werden kann:

$$222^{149} \bmod n = 1110$$

Dies entspricht dem Text "BA" lt. Tabelle (11.4).

Berechnung von $222^{149} \bmod n$:

$$222^1 \bmod n = 222$$

$$222^2 \bmod n = 49284 \bmod n = 1110$$

$$222^3 \bmod n = (1110 \cdot 222) \bmod n = 246420 \bmod n = 962$$

$$222^4 \bmod n = (962 \cdot 222) \bmod n = 213564 \bmod n = 222$$

Damit wiederholen sich die Reste der Potenzen $222^k \bmod n$.

Im Falle $k \bmod 3 = 2$ ist $222^k \bmod n = 1110$. Wegen $149 \bmod 3 = 2$ ergibt sich

$$222^{149} \bmod n = 1110$$

b) $n = 34567891011121314168381477494337312520411$ (41 Stellen)

$$e = 56789101112147$$

Öffentlicher Schlüssel von A ist (n, e) . Damit ist der Geheimtext verschlüsselt worden, und er kann mit dem geheimen Schlüssel von A wieder entschlüsselt werden. Daher muss der geheime Schlüssel (n, d) von A mit $(e \cdot d) \bmod \varphi(n) = 1$ bestimmt werden.

Aus der PFZ von n

$$n = 100000000000000000039 \cdot 345678910111213141549 = p \cdot q \text{ lässt sich}$$

$$\varphi(n) = (p-1) \cdot (q-1) = 34567891011121314167935798584226099378824$$

berechnen. Es gilt $\text{ggT}(e, \varphi(n)) = 1$. Bestimme mit dem EEA Zahlen $d, z \in \mathbb{Z}$, so dass $e \cdot d + z \cdot \varphi(n) = 1$ und $d \in \mathcal{R}_{\varphi(n)}$ gilt.

$$\text{Es ergibt sich } d = 19513462547268140887950033703256438139395$$

$$\text{Geheimtext: } y = 31261643036571769583759745756803429217563$$

$$\text{Klartext: } y^d \bmod n = 151823102114$$

Bedeutung: F I N A L E (lt. Tabelle (11.4))

Hinweis: Es war natürlich nicht daran gedacht, dass diese Aufgabe mit einem Taschenrechner bearbeitet werden sollte!