Prof. J. Rothe Düsseldorf, 13.10.2009

Übung zur Vorlesung
Kryptologie 2

Blatt 1, Abgabe: 22.10.2009 bis 15:00 Uhr

Aufgabe 1 (10 Punkte):

(a) Zeigen Sie, dass die Kongruenz

$$n^2 \equiv 1 \bmod 8$$

für alle ungeraden, natürlichen Zahlen n gilt.

(b) Zeigen Sie, dass für alle natürlichen Zahlen a und alle Primzahlen p die Kongruenz

$$(a+1)^p \equiv a^p + 1 \bmod p$$

gilt.

Aufgabe 2 (10 Punkte):

(a) Bestimmen Sie den zum RSA-Modul $n = 91$ und öffentlichen Exponenten $e = 5$ passenden privaten Exponenten d mit dem erweiterten Algorithmus von Euklid.

(b) Bestimmen Sie alle für den RSA-Modul $n = 15$ gültigen öffentlichen Exponenten e.

(c) Bestimmen Sie im RSA-Kryptosystem die Anzahl der gültigen Exponenten e für den RSA-Modul $n = 323$.

Aufgabe 3 (freiwillig): Für das RSA-Verfahren sei der öffentliche Schlüssel $(n, e) = (1961, 5)$ gegeben. Weiterhin sei das Alphabet $\Sigma = \{\mathtt{A}, \mathtt{B}, \mathtt{C}, \ldots, \mathtt{Z}\}$ auf die übliche Art und Weise über $\mathbb{Z}_{26}$ kodiert, d.h. $\mathtt{A} \widehat{=} 0$, $\mathtt{B} \widehat{=} 1$, $\ldots$, $\mathtt{Z} \widehat{=} 25$.

(a) Bestimmen Sie die Primfaktorzerlegung von n.

(b) Bestimmen Sie den Entschlüsselungsexponenten d.

(c) Bestimmen Sie die Blocklänge von Nachrichten über Σ.

(d) Verschlüsseln Sie den Klartext $m = \mathtt{KAFFEE}$.

(e) Entschlüsseln Sie den Ciphertext $c = \mathtt{CJGAUACWQ}$.