Frank Klinker

Aufgaben: Zahlentheorie

Teil 3: Potenzieren und das RSA-Verfahren

Aufgabe 1. Berechnen Sie:

a) $9^{81} \mod 11$ b) $14^{722} \mod 5$ c) $(-9)^{182} \mod 7$

Aufgabe 2. Zeigen Sie mit Hilfe der Eulerschen φ-Funktion, dass

a) $632^{107} \equiv 42 \mod 53$ b) $166^{138} \equiv 4 \mod 24$ c) $208^{325} \equiv 5 \mod 7$

Aufgabe 3. a) Begründen Sie, warum es zum Bestimmen der letzten beiden Ziffern einer Zahl reicht, ihren Wert modulo 100 zu berechnen?

b) Bestimmen Sie die letzten beiden Stellen der Zahl 7^{1283}.

Aufgabe 4. $p = 31$ und $q = 37$ sind die zwei Primzahlen zum RSA-Verfahren.

a) Bestimmen Sie einen öffentlichen Schlüssel $(e; N)$ so, dass e so klein wie möglich ist.

b) Berechnen den zu $(e; N)$ aus a) gehörigen privaten Schlüssel $(d; N)$.

c) Ist 174 die Verschlüsselung von 10, wenn der öffentliche Schlüssel $(11; 1147)$ ist?

Aufgabe 5. $p = 17$ und $q = 11$ sind die zwei Primzahlen zum RSA-Verfahren.

a) Verschlüsseln Sie die Information 65 mit Hilfe des öffentlichen Schlüssels $(7; 187)$.

b) Begründen Sie, warum $(7; 187)$ der kleinstmögliche öffentliche Schlüssel ist.

c) Berechnen den zu $(7; 187)$ gehörigen privaten Schlüssel $(d; 187)$.

Adresse: Eduard-Spranger-Berufskolleg, 59067 Hamm
E-Mail: mail@frank-klinker.de
Version: 3. Juni 2024