Hochschule RheinMain
Fachbereich Design Informatik Medien
Studiengang Angewandte Informatik / Informatik Technische Systeme
Prof. Dr. Bernhard Geib

Security

Sommersemester 2021
(LV 4121 und 4241)

7. Aufgabenblatt

Mit den folgenden Aufgaben realisieren wir eine Krypto-Programmbibliothek, die uns für die wichtigsten kryptographischen Grundoperationen entsprechende Grundfunktionen zur Verfügung stellt. Neben der Generierung von Zufallszahlen, der Berechnung von Primzahlen sowie der Bestimmung der modularen Inversion und Exponentiation sind es auch die Basisalgorithmen zur Realisierung von unterschiedlichen Substitutionschiffren. Standardverfahren wie RSA, Diffie-Hellman oder ElGamal lassen sich auf diese Weise sehr effizient realisieren.

Aufgabe 7.1

Benutzen Sie die in der Vorlesung behandelten kryptographischen Grundfunktionen, um folgende Aufgabenstellungen zu lösen:

a) ggT(44243, 39713)

b) $\phi(78817)$

c) eEA(37486, 26319)

d) $136^{33} \bmod 257$

e) $3196^{-1} \bmod 83461$

Aufgabe 7.2

Es seien m = 259200, a = 7141 und b = 54773 die Parameter eines linearen Kongruenzengenerators.

a) Bestimmen Sie die durch $x_{n+1} = (a \cdot x_n + b) \bmod m$ definierte Pseudozufallsfolge $x_1, x_2, ..., x_{10}$ für die Startwerte: $x_0 = 0$ und $x_0 = 4711$.

b) Wie groß ist die Periodizität des Generators?

Aufgabe 7.3

a) Ermitteln Sie die Anzahl $\pi'(a, b)$ der Primzahlen im Intervall [a, b] mit $a = 10^6$ und $b = 10^9$.

Formal: $\pi'(a, b) = \#p_k$, $p_k \in \mathbf{P}$ wobei $a \leq p_k \leq b$ für $k = 1, 2, ..., \pi'(a, b)$

b) Ermitteln Sie die Anzahl der Primzahlen $\pi(n)$ kleiner gleich n und stellen Sie das Ergebnis graphisch dar.

c) Bestimmen Sie die Primzahlendichte $\pi(n) / n$ kleiner gleich n und stellen Sie auch dieses Ergebnis in einem Schaubild dar.

d) Ermitteln Sie alle Primzahlenpaare (p, q) für die gilt: $q = p + 2$ und $q < 200$. Beispiele für Primzahlenpaare sind: (3, 5), (5, 7), (11, 13) und (17, 19).

Aufgabe 7.4

Seien $k \geq 1$ und $p \in \mathbf{P}$. Zeigen Sie, dass dann für die Eulersche Phifunktion Φ gilt:

$$\Phi(p^k) = p^{k-1} (p - 1)$$