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

Security

Sommersemester 2022
(LV 4120 und 7240)

6. Aufgabenblatt

Ziel des folgenden Aufgabenblatts ist es, den erforderlichen Rechenaufwand bei anspruchsvollen kryptographischen Berechnungen abschätzen zu können. Dazu beschäftigen wir uns zunächst mit der simultanen Lösung von Kongruenzgleichungen sowie der Berechnung der modularen Quadratwurzel. Anschließend entziffern wir eine Blockchiffre der Länge 2, deren Chiffretext bekannt ist.

Aufgabe 6.1

Es sei $x \in \mathbf{N}$ (Menge der natürlichen Zahlen).

a) Die Zahl x sei kongruent 1 modulo 3 und kongruent 2 modulo 5, d. h.

$$x \equiv 1 \pmod 3 \quad \text{und} \quad x \equiv 2 \pmod 5$$

Wie lautet die Zahl x? (Bitte den Berechnungsweg vollständig angeben!)

b) Gesucht ist die simultane Lösung der beiden Kongruenzen

$$2 \equiv x \pmod 3 \quad \text{und} \quad 1 \equiv x \pmod 5$$

Wie lautet die positive ganze Zahl x? (Bitte den Berechnungsweg vollständig angeben!)

c) Wann hat die Kongruenz

$$a \cdot x \equiv c \pmod m$$

eine Lösung x? (Die Frage ist nur zu beantworten!)

Aufgabe 6.2

Eine Lösung x der quadratischen Gleichung

$$x^2 = a$$

in der Ringstruktur $\mathbf{Z}_n$ nennen wir eine modulare Quadratwurzel und bezeichnen sie mit

$$x = a^{1/2} \bmod n.$$

Zahlen, welche eine modulare Quadratwurzel besitzen, nennen wir auch quadratische Reste (sonst quadratische Nichtreste).

a) Ermitteln Sie die beiden modularen Quadratwurzeln der Gleichung

$$x = 19^{1/2} \bmod 67.$$

b) Wieso treten die Lösungen von modularen Wurzelgleichungen immer paarweise auf?

c) Wann besitzt eine modulare Wurzelgleichung keine Quadratwurzeln?

Aufgabe 6.3

Bei der folgenden Blockchiffre der Länge 2 werde jeder Klartextblock **M** in einen entsprechenden Chiffreblock **C** gemäß der Vorschrift:

$$\mathbf{C} = \mathbf{K} \cdot \mathbf{M} \bmod n$$

transformiert, wobei der Schlüssel **K** aus einer 2x2-Matrix der Gestalt:

$$\mathbf{K} = \begin{pmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{pmatrix}$$

besteht. Für die Codierung der Zeichen a, b, c, ..., z und | des zugrunde liegenden Alphabets werden die Nummern 0, 1, 2, ..., 26 benutzt. Alle, sich bei der Transformation ergebenden Additionen und Multiplikationen werden modulo 27 berechnet.

a) Finden Sie die Schlüsselmatrix **K**, wenn sich als Chiffretext zu „`turing`“ die Zeichenfolge „`UBIXGT`“ ergibt.

b) Entschlüsseln Sie den restlichen Geheimtext „`ENERHLNHAHRM`“.

c) Warum wurde hier das Alphabet künstlich um das Zeichen „|“ erweitert, so dass es 27 statt 26 Buchstaben umfasst?

d) Warum ist 27 auch keine optimale Wahl? Geben Sie einen besseren Wert an.

Aufgabe 6.4

Berechnen Sie die modulare Exponentiation $2^{19487190} \bmod 19487191$ im Restklassenring $\mathbf{Z}_{19487191}$ unter Verwendung des

a) kleinen Satzes von Fermat

b) Entwicklungssatzes

c) Square-and-Multiply-Algorithmus