Vorlesung „Kryptographie I“ (Sommersemester 2018)

5-ECTS-Klausur (28.9.2018)

Anmerkungen:

(1) Als Hilfsmittel ist nur ein Taschenrechner und das ausgeteilte Blatt „Hilfen zur VIGENERE-Verschlüsselung“ erlaubt.

(2) Zur Lösung einer Aufgabe gehören auch Darstellung des Lösungswegs und Begründungen.

Aufgabe 1: Maximilian schickt an Johannes folgende VIGENERE-chiffrierte Nachricht:

```
OECMG CBLBRYLW,
RN KTZWUER DMCM AVU QJX PPR GBSK SVFYYKIE NAM QIN VLK DLN OTYFFVWH JRIJXA.
AFRY KY QFAM HRE PFZX YBKM, NYDL XPXQVXTUVFR, XLPUF VBPL FMYMETI.
YKHWT, QLEMDJDBNR
```

(1) Bestimme das zugehörige VIGENERE-Schlüsselwort.

(2) Entschlüssle das 15. Wort (OTYFFVWH) der Nachricht.

Aufgabe 2:

(1) Bestimme die kleinste natürliche Zahl, die das folgende Kongruenzgleichungssystem löst:

$$x \equiv 3 \bmod 37, \quad x \equiv 7 \bmod 73.$$

(2) Warum besitzt das folgende Kongruenzgleichungssystem keine Lösung?

$$x \equiv 3 \bmod 36, \quad x \equiv 6 \bmod 63.$$

Aufgabe 3:

(1) Erläutere die/eine square-and-multiply-Methode an der Berechnung von

$$19^{18} \bmod 100.$$

(2) Berechne $\varphi(100)$.

(3) Was besagt das Satz von Euler über die Eulersche φ-Funktion?

(4) Berechne

$$19^{2018} \bmod 100.$$

Aufgabe 4: Für $n = 123456687$ gilt $5^{\frac{n-1}{2}} \equiv 5 \bmod n$.

(1) Beschreibe den Miller-Rabin-Test zur Basis 5. Welche Ergebnisse sind möglich?

(2) Besteht n den Miller-Rabin-Test zur Basis 5?

(3) Besteht n den Fermat-Test zur Basis 5?

Aufgabe 5: $N = 66080761$ ist eine RSA-Zahl.

(1) Faktorisiere N mit der Fermatschen Faktorisierungsmethode.

(2) Bestimme die kleinste natürliche Zahl $e > 1$, sodass (N, e) ein öffentlicher RSA-Schlüssel ist.

(3) Bestimme ein $d > 1$, sodass (N, d) ein zu (N, e) passender privater RSA-Schlüssel ist.