Vorlesung „Kryptographie I“ (Sommersemester 2018)

10-ECTS-Klausur (28.9.2018)

Anmerkungen:

(1) Als Hilfsmittel ist nur ein Taschenrechner erlaubt.
(2) Zur Lösung einer Aufgabe gehören auch Darstellung des Lösungswegs und Begründungen.

Aufgabe 1: Der folgenden PLAYFAIR-Verschlüsselung liege das Schlüsselwort `GEBURTSTAGSFEIER` zugrunde.

(1) Stelle die zugehörige PLAYFAIR-Matrix auf.
(2) Erläutere die PLAYFAIR-Verschlüsselung anhand der Verschlüsselung von `KAFFEEUNDKUCHENSINDVORHANDEN`.
(3) Entschlüssle den Chiffretext `AMGISWFBDK`, der mit obigem Schlüsselwort PLAYFAIR-verschlüsselt wurde.

Aufgabe 2: Sei $n = 4033$.

(1) Erläutere die/eine square-and-multiply-Methode an der Berechnung von $2^{63} \bmod n$. (Lösung: 3521)
(2) Führe den Miller-Rabin-Test zur Basis 2 für n durch. Welches Ergebnis erhält man?
(3) Zeige, dass die Gleichung $109x \equiv 1 \bmod n$ nicht lösbar ist.
(4) Bestimme die Primfaktorzerlegung von n.

stark ; mit $b^{2^i} \equiv -1 \bmod n$

Aufgabe 3: $N = 66128467$ ist eine RSA-Zahl.

(1) Faktorisiere N mit der Fermatschen Faktorisierungsmethode.
(2) Bestimme die kleinste natürliche Zahl $e > 1$, sodass (N, e) ein gültiger (öffentlicher) RSA-Schlüssel ist.

Aufgabe 4: Einem Diffie-Hellman-Schlüsselaustausch liegen $p = 67$ und $g = 2$ zugrunde. Die öffentlichen Schlüssel von Ute und Vera sind $f_U = 44$ und $f_V = 55$.

(1) Zeige, dass $g = 2$ eine Primitivwurzel modulo $p = 67$ ist.
(2) Berechne den privaten Schlüssel von Ute oder Vera.
(3) Bestimme den gemeinsamen Diffie-Hellman-Schlüssel k_{UV} von Ute und Vera.

Aufgabe 5: $(p, g, e) = (2017, 5, 11)$ ist ein privater ElGamal-Signatur-Schlüssel. $g^e = f$

(1) Bestimme den zugehörigen öffentlichen Schlüssel (p, g, f).
(2) Signiere ein Dokument mit Hashwert $h = 12$ unter Verwendung der „Zufallszahl“ $z = 13$.
(3) Welche Bedingungen müssen erfüllt sein, damit ein Zahlenpaar (b, c) als gültige Signatur der Person mit dem öffentlichen ElGamal-Signatur-Schlüssel (p, g, f) für ein Dokument mit Hashwert h akzeptiert wird?

gelten: $1 \leq b < p$; $g^h \equiv f^b b^c \bmod p$

sign: $b = g^z \bmod p$; $c = \frac{1}{z}(h - b \cdot e) \bmod p-1$