Vorlesung „Kryptographie I“ (Sommersemester 2018)

Klausur (18.7.2018, 10:00-12:00, Hörsaal H11)

Anmerkungen:

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

Aufgabe 1: Ein Text wurde unter Verwendung der Schlüsselwörter `JULI2018` und `MITTWOCH` zu

`AADXA FADAD AVDAD DGDAA`

ADFGVX-chiffriert. Entschlüssle den Text und erläutere dabei die ADFGVX-Verschlüsselung.

Aufgabe 2: Sei $n = 2^{256} + 1$. Es ist

$$n = 115792089237316195423570985008687907853269984665640564039457584007913129639 9 * *,$$

wobei die letzten beiden Dezimalstellen „verlorengegangen“ sind.

(1) Was besagt der Satz von Euler über die Eulersche φ-Funktion?
(2) Bestimme n mod 4.
(3) Bestimme n mod 25.
(4) Bestimme die letzten beiden Dezimalstellen von n. (Hinweis: Was ist n mod 100?)

Aufgabe 3: $N = 18386939$ 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 $p = 61$ und $g = 2$ zugrunde. Die öffentlichen Schlüssel von Ulrike und Veronika sind $f_U = 3$ und $f_V = 6$.

(1) Zeige, dass $g = 2$ eine Primitivwurzel modulo $p = 61$ ist.
(2) Berechne den privaten Schlüssel von Ulrike oder Veronika.
(3) Bestimme den gemeinsamen Diffie-Hellman-Schlüssel k_{UV} von Ulrike und Veronika.

Aufgabe 5: $(p, g, e) = (1999, 3, 17)$ ist ein privater ElGamal-Signatur-Schlüssel.

(1) Bestimme den zugehörigen öffentlichen Schlüssel (p, g, f).
(2) Signiere ein Dokument mit Hashwert $h = 18$ unter Verwendung der „Zufallszahl“ $z = 19$.
(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?