PROBEKlausur zur Spezielle Aspekte: Kryptographie

SoSe 2011

Vorname und Name (bitte leserlich !):

Matrikelnummer:

Bitte beachten Sie:

- Jedes abgegebene Blatt mit Namen und Matrikelnummer versehen! Namen bitte leserlich in BLOCKSCHRIFT!
- (Teil-)Lösungen werden nur mit vollständigem (Teil-)Lösungsweg anerkannt.
- Erlaubte Hilfsmittel sind ein einseitig handgeschriebenes DIN A4 Blatt.
- Es dürfen nur die Algorthimen aus der Vorlesung verwendet werden.
- Jede Aufgabe zählt 12 Punkte. Sie können sich 4 Aufgaben heraussuchen. Die Klausur ist mit 24 Punkten bestanden.

Aufgabe 1

(a) Berechnen Sie das Inverse zu 71 in $\mathbb{Z}_{341}^*$. (10 Punkte)

(b) Es ist $341 = 11 \cdot 31$. Bestimmen Sie die Ordnung $|\mathbb{Z}_{341}^*|$. (2 Punkte)

Aufgabe 2

(a) Geben Sie die Definition eines Kryptosystems. (6 Punkte)

(b) Geben Sie ein Beispiel für ein symmetrisches Kryptosystem und begründen Sie, warum es ein solches Beispiel ist. (6 Punkte)

Aufgabe 3 Seien $r, n \in \mathbb{N}$ und $a, b, c \in \mathbb{Z}$ so, dass $a \equiv b \bmod n$ gilt. Zeigen Sie

(a) $ac \equiv bc \bmod n$ (6 Punkte)

(b) $a^r \equiv b^r \bmod n$ (6 Punkte)

Aufgabe 4 (a) Formulieren Sie den kleinen Satz von Fermat. (4 Punkte)

(b) Beweisen Sie diesen Satz. (8 Punkte)

Aufgabe 5 Alice will das ElGamal Verfahren anwenden. Sie wählt $p = 37, \alpha = 2$ und $a = 3$.

(a) (1) Geben Sie den öffentlichen Schlüssel und den privaten Schlüssel von Alice an. (1 Punkt)

(2) Bob will $x = 27$ mit $k = 2$ verschlüsseln. Was sendet er? (3 Punkte)

(b) (1) Wie entschlüsselt Alice die Nachricht von Bob? (Hinweis: $27^{-1} = 11$ in $\mathbb{Z}_{37}^*$) (2 Punkte)

(2) Beweisen Sie, dass Alice als Ergebniss der Entschlüsselung des Chiffretextes immer wieder den ursprünglich von Bob gesendeten Text erhält.

Aufgabe 6 (a) Erklären Sie, wie der Miller-Rabin Test funktioniert. (6 Punkte)

(b) Überprüfen Sie mit dem Miller-Rabin Test, ob 177 eine Primzahl ist. (6 Punkte)
Beachten Sie: $2^{10} \equiv 139 \bmod 177$, $2^{11} \equiv 101 \bmod 177$, $2^{15} \equiv 23 \bmod 177$, $2^{22} \equiv 112 \bmod 177$, $2^{33} \equiv 161 \bmod 177$, $2^{44} \equiv 154 \bmod 177$, $2^{88} \equiv 175 \bmod 177$.