Vorlesung "Kryptographie I" (Wintersemester 2019/2020)
Klausur (18.12.2019, 14:15-15:45, Hörsaal HG)

Anmerkungen:

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

Aufgabe 1:

1. Erläutere die TRANSSPA-Verschlüsselung anhand der Verschlüsselung von
   DAS JAHR GEHT BALD ZU ENDE
   mit dem Schlüsselwort DEZEMBER
2. Entschlüssle den mit dem Schlüssel DEZEMBER verschlüsselten TRANSSPA-Chiffretext
   RVREZBNRASATTMKDIKDAEIZNBEEVNNEETLDEAR

Aufgabe 2: Untersuche, ob das Kongruenzgleichungssystem

$$x \equiv 24 \pmod{247},\ x \equiv 7 \pmod{742}$$

lösbar ist. Wenn ja, bestimme die kleinste natürliche Zahl, die das Kongruenzgleichungssystem löst.

Aufgabe 3: Sei $n = 2^{126}(2^{127} - 1)$. Es ist
$n = 144740111546645244279463731260859884815736774914748358890663543491311991521 * *$,
wobei die letzten beiden Dezimalstellen "verlorengegangen" sind.

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

Aufgabe 4: Sei $n = 8321$

1. Erläutere die/eine square-and-multiply-Methode anhand der Berechnung von $2^{65} \pmod{n}$ (Ergebnis: 8192)
2. Führe den Miller-Rabin-Test zur Basis 2 für n durch. Was weiß man jetzt über n?
3. Zeige, dass die Gleichung $157x \equiv 1 \pmod{n}$ nicht lösbar ist.
4. Bestimme die Primfaktorzerlegung von n.

Aufgabe 5: $N = 93172369$ 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.