

E. Best

25.06.2004

Abgabe: 02.07.2004

Freitags in der Vorlesung

10. Übung zur Vorlesung Kryptographie

Achtung: Nächste Woche gibt es 2 Übungsgruppentermine: **Montag**, 28. Juni, 10:15 wie gewohnt im HS F; **Mittwoch**, 30. Juni, 8:15 wie gewohnt in Raum A7-0-025.

Aufgabe 36: Ordnung von Restklassen (4 Punkte)
Finden Sie Restklassen zum primen Modul 2333, die die Ordnungen 22 und 53 haben.

Aufgabe 37: Erzeugung von Primitivwurzeln (4+4 Punkte)

- (a) Sei p eine Primzahl, so dass $q = (p-1)/2$ auch prim ist. Man möchte eine Primitivwurzel zum Modul p finden, zieht dazu zufällig eine Zahl aus einem Intervall $(1, \dots, p)$ (exklusive 1 und p) und testet, ob sie Primitivwurzel ist. Wie groß ist die Erfolgswahrscheinlichkeit?
- (b) Wie viele Multiplikationen in \mathbb{Z}_p benötigt man im Durchschnitt, wenn das Verfahren so lange fortgesetzt wird, bis eine Primitivwurzel gefunden ist? Für die Zwecke der Abschätzung dürfen Sie annehmen, dass die Hälfte aller Bits von q gleich 1 sind.

Aufgabe 38: Diffie-Hellmann (4 Punkte)
Alice und *Bob* vereinbaren mit Hilfe des Diffie-Hellmann-Protokolls einen symmetrischen Schlüssel K . *Oscar* fängt das Folgende ab: $p = 43$, $g = 3$, $A = 30$, $B = 24$. Wie lautet K ?
Hinweis: Legen Sie sich eine Tabelle mit $3^k \bmod 43$ für $k = 0, \dots, 41$ an. Zur Vereinfachung können Sie verwenden, dass $3^{21+k} \equiv -3^k \bmod 43$ für jedes $k \in \mathbb{Z}$ gilt.

Aufgabe 39: ElGamal (4 Punkte)
Alice erhält den ElGamal-Chiffretext $(y_1, y_2) = (24, 7)$. Wie lauten ihr privater Schlüssel und der Klartext, wenn ihr öffentlicher Schlüssel $(p, g, b) = (43, 3, 30)$ ist?
Hinweis: Man kann die vorige Aufgabe benutzen.