

9. Übung zur Vorlesung Kryptographie

Achtung: Nächste Woche gibt es **NUR EINEN** Übungsgruppentermin: **Montag**, 21. Juni, 10:15 wie gewohnt im HS F; der Zusatztermin **Mittwoch**, 23. Juni, 8:15 **FÄLLT AUS** bzw. kann für Interessenten während meiner Sprechstunde am Montag, 28. Juni, 14 Uhr, nachgeholt werden.

Aufgabe 33: Geburtstags-Paradox **(2+2 Punkte)**

Ein Computersystem benutzt Passwörter, die genau 5 Zeichen lang sind und für jeden Nutzer zufällig generiert werden. Ab welcher Nutzerzahl ist die Wahrscheinlichkeit, dass zwei Nutzer das gleiche Passwort zugeteilt bekommen, größer als $1/100$, falls

- (a) nur Großbuchstaben verwendet werden,
- (b) unter Einbeziehung von Sonderzeichen insgesamt 94 Zeichen zugelassen sind?

Aufgabe 34: RSA-Entschlüsselung **(4+3+3 Punkte)**

Die RSA-Entschlüsselung (mit $n = p \cdot q$) kann beschleunigt werden. *Alice* möchte den Schlüsseltext y entschlüsseln. Ihr privater Schlüssel ist d . Sie berechnet

$$x_p = y^d \bmod p \quad , \quad x_q = y^d \bmod q$$

und löst dann die simultane Kongruenz

$$x \equiv x_p \pmod{p} \quad , \quad x \equiv x_q \pmod{q}. \tag{1}$$

Dann ist x der ursprüngliche Klartext. Um (1) zu lösen, berechnet *Alice* mit *extended_euclid* zwei Zahlen X_p, X_q mit $X_p \cdot p + X_q \cdot q = 1$ und setzt

$$x = (x_p \cdot X_q \cdot q + x_q \cdot X_p \cdot p) \bmod n.$$

- (a) Sie haben den privaten Schlüssel $p = 8999$, $q = 9001$ und $d = 80964007$. Entschlüsseln Sie die Nachricht $y = 16777216$ unter Zuhilfenahme dieser Methode.
- (b) Argumentieren Sie, dass dieses Verfahren korrekt ist.
- (c) Schätzen Sie ab (in %), wie viel Rechenzeit durch diese Methode gewonnen wird.

Aufgabe 35: Sicherheit des geheimen Schlüssels in RSA **(6 Punkte)**

Sie haben zu dem öffentlichen Schlüssel $(n, e) = (49601, 515)$ den geheimen Exponenten $d = 14507$ ausgespäht. Faktorisieren Sie n .