

E. Best

19.04.2004

Abgabe: 26.04.2004

Montags in der Übungsstunde

1. Übung zur Vorlesung Kryptographie

Die Abgabe von Aufgaben darf in Gruppen von maximal drei Personen erfolgen. Unleserliche, kopierte, abgeschriebene oder zu spät abgegebene Aufgaben werden nicht gewertet. Rechenwege gehören generell zur Lösung und sollen mit abgegeben werden. Falls Sie Google / das WWW benutzt haben, müssen die Quellen vollständig angegeben werden.

Die Übungsaufgaben gehen mit einem Anteil von 25% in die Modulnote ein, ebenfalls zu 25% wird die aktive Beteiligung an der Übung gewertet. Die übrigen 50% der Modulnote ergeben sich aus einer abschließenden Prüfung am Ende der Vorlesungsperiode. Als Termin der Abschlussklausur ist der 20. Juli 2004 vorgesehen.

Aufgabe 1: Affin-lineare Chiffrierung (4 Punkte)

Benutzen Sie die affin-lineare Chiffre mit Schlüssel $(a, b) = (3, 3)$, um den Klartext

`dieaxtimhauserspartdenzimmermann`

zu verschlüsseln.

Aufgabe 2: Kryptanalyse (4 Punkte)

Welches Wortspiel hat Groucho Marx hier gemacht?

`GRNVUORVHORPVZMZIILDUIFRGUORVHORPVZYZMZMZ`

Beschreiben Sie kurz, wie Sie die Lösung gefunden haben!

Aufgabe 3: Distributivgesetz in \mathbb{Z}_m (4 Punkte)

Sei $m \in \mathbb{N} \setminus \{0\}$. Verifizieren Sie die erste Hälfte des Distributivgesetzes in $(\mathbb{Z}_m, +, \cdot)$, indem Sie (für beliebige $a, b, c \in \mathbb{Z}$) ausführlich

$$x \in ([a]_m \cdot ([b]_m + [c]_m)) \Leftrightarrow x \in (([a]_m \cdot [b]_m) + ([a]_m \cdot [c]_m))$$

beweisen.

Aufgabe 4: Der größte gemeinsame Teiler (4 Punkte)

Sind diese beiden Aussagen richtig oder falsch?

- Wenn für drei ganze Zahlen a, b, c $ggT(a, b, c) = 1$ gilt, dann gilt auch $ggT(a, b) = 1 \wedge ggT(a, c) = 1 \wedge ggT(b, c) = 1$.
- Wenn für drei ganze Zahlen a, b, c $ggT(a, b) = 1 \vee ggT(a, c) = 1 \vee ggT(b, c) = 1$ gilt, dann gilt auch $ggT(a, b, c) = 1$.

Geben Sie jeweils entweder Begründung oder Gegenbeispiel an.

Aufgabe 5: Gruppentafeln (4 Punkte)

Stellen Sie die Gruppentafeln von $(\mathbb{Z}_6, +)$ und von (\mathbb{Z}_6^*, \cdot) auf.