

SMS1 für MC, FHS Hagenberg
2. Übungsblatt für den 14. Oktober 2004

1. Die Nachricht XPQBO FURKA ABOHR MCBOH BPPBI wurde mit einem Caesar verschlüsselt. Dechiffrieren Sie sie.
2. Bonusbeispiel: Dechiffrieren Sie den monoalphabetisch verschlüsselten Text auf den Seiten 1 und 2 von [1].
Hinweis: Verwenden Sie die angegebene Tafel für die durchschnittliche Häufigkeit einzelner Buchstaben in deutschen Texten.
3. Lösen Sie Aufgabe 1.5 zur Playfair-Chiffre in [2] (auf dem in der Übung am 7.10. ausgeteilten Zusatzblatt).
4. Lösen Sie Aufgabe 1.7 zur deutschen ADFGVX-Verschlüsselung in [2] (auf dem in der Übung am 7.10. ausgeteilten Zusatzblatt).
5. Verwenden Sie den erweiterten Euklidischen Algorithmus um jeweils den größten gemeinsamen Teiler folgender Zahlen zu bestimmen:
 - (a) 84, 378
 - (b) 451, 178
 - (c) 84, 147, 378
 - (d) 34, 55

Literatur

- [1] Jürgen Ecker. *Automatentheorie und Kryptologie*. Computer- und Mediensicherheit, FHS Hagenberg, (<http://webster.fh-hagenberg.at/staff/ecker/MAT2CMS/skriptss04.pdf>).
- [2] Richard A. Mollin. *An introduction to cryptography*. CRC Press Series on Discrete Mathematics and its Applications. Chapman & Hall/CRC, Boca Raton, FL, 2001.