Übungen Diskrete Mathematik, TE

4. Übungsblatt

1. April 2014

Für alle Beispiele, die dem Kapitel Kryptographie angehören, darf für die Berechnungen ein Computer verwendet werden.

19. Man bestimme, welche der folgenden Strukturen $(X, \circ)$ eine Halbgruppe/ein Monoid/eine Gruppe ist und ob die Struktur abelsch ist.

(a) Sei $X = \mathbb{N}$ und $x \circ y = \max(x, y)$.

(b) Sei $X = \mathbb{Z}$ und $x \circ y = x + y + 2014$

(c) Sei $X = \mathbb{R} \times \mathbb{R} \setminus \{(0, 0)\}$ und $(a, b) \circ (c, d) = (ac - bd, ad + bc)$

20. Man bestimme die letzten beiden Ziffern in der Dezimaldarstellung von

(a) $x = 7^{123456789}$

(b) $x = 8^{123456789}$

Hinweis: Man verwende $100 = 4 \cdot 25$ *und den chinesischen Restsatz*

21. Man bestimme $0 \leq x < m$, sodass folgende Kongruenzen gelten:

(a) $x \equiv \left(2^{2014}\right)^{2014} \mod m = 35$

(b) $x \equiv 2^{\left(2014^{2014}\right)} \mod m = 35$

22. TYUIUH JUNJ MKHTU CYJ UYDUH SQUIQHSXYVVHU CYJ UYDUC LUHISXKR LED IUSXPUXD LUHISXBKUIIUBJ. TYUIU QHJ TUH LUHISXBKUIIUBKDW DUDDJ IYSX QKSX HEJ D KDT AQDD IUXH BUYSXJ YC YDJUHDUJ UDJISXBKUIIUBJ MUHTUD.

Falls man in Wirklichkeit einen verschlüsselten Text abfängt, erfährt man auch nicht mehr. Ein kleiner zusätzlicher Hinweis hier: Leerzeichen bleiben Leerzeichen.

23. In den folgenden Text wurden vor dem Verschlüsseln Störzeichen eingebaut und alle Leerzeichen entfernt. Danach wurde der Text auf folgende Art verschlüsselt: Alle Buchstaben, die an geraden Stellen stehen wurden mit einer Caesar-Chiffre verschlüsselt, alle Buchstaben an ungeraden Stellen mit einer anderen Caesar-Chiffre.

FJBFUFXFTTEINVGTUFNVPVIJUUPBEIFFOGTBUOBPUFPCNBKTGEGBXJIOGSGCGOCO PUVOBPTNCMGSYFKTGXKSFEGSVFZUKOOFJSCQNTBXGJVFKMGHGUGJNUWVPEFFT WGSUDJOWCFFTDCFUBTDJJMGHSGNKUJUKMHFGJPFUTEINVGTUFNXQSVFUGGTVH GMGHV

24. Bei einem Diffie-Hellman-Schlüsselaustausch wurden folgende Werte erhalten: $g = 2$, $p = 101$, $m = 14$, $n = 27$. Man bestimme die geheimen Parameter a und b und den Schlüssel r.