Diskrete Mathematik ICE

5. Übungsblatt

24. April 2018

Verwenden Sie bei den Aufgaben 21 bis 23 und 25 lediglich einen Taschenrechner. Bei der Aufgaben 24 sind sämtliche Hilfsmittel (Computer, Internet, ...) zulässig, um den Text zu entschlüsseln. Sie sollten jedoch an der Tafel erzählen können, wie Sie bei der Entschlüsselung vorgegangen sind. Ein kleiner Hinweis: Leer- und Satzzeichen bleiben durch die jeweilige Verschlüsselung unverändert.

21. Bestimmen Sie die letzten beiden Ziffern in der Dezimaldarstellung von

$$a = 7^{20180424},$$

indem Sie den Satz von Euler-Fermat

(a) für $m = 100$ anwenden,

(b) für $m_1 = 4$ und $m_2 = 25$ anwenden und danach den chinesischen Restsatz benutzen.

22. Ermitteln Sie x mit $0 \leq x < 35$, so dass

(a) $x \equiv \left(22^{3141}\right)^{272} \bmod 35$;

(b) $x \equiv 22^{\left(3141^{272}\right)} \bmod 35$.

23. Bei einem Diffie-Hellman-Schlüsselaustausch wurden die Werte $g = 5$, $p = 97$, $m = 29$ und $n = 30$ mitgehört. Bestimmen Sie die geheimen Parameter a und b sowie den Schlüssel $r = s$.

24. `MRNBNA JKBJCI FDAMN VRC NRWNA LJNBJA LQROOAN VRC NRWNV ENABLQDK EXW WNDW ENABLQUDNBBNUC. MRNBN JAC MNA ENABLQUDNBBNUDWP WNWWC BRLQ JDLQ AXC W DWM TJWW BNQA UNRLQC RV RWCNAWNC NWCBLQUDNBBNUC FNAMNW. ODNA MNW IFNRCNW JKBJCI FDAMNW IFNR ENABLQRNMNWN LJNBJA LQROOANB ENAFNWMNC, NRWNA ODNA MRN KDLQBCJKNW JW PNAJMNW YXBRCRXWNW DWM NRWNA ODNA MRN KDLQBCJKNW JW DWPNAJMNW YXBRCRXWNW.`

`GUHEH MUF GQU HHDVOKXXQVEHXXZJ ZHZQF VUFT YUJQQQUQ FTLRIDH. UP MOXJQPQLZHZ ZQUPHZ EQL QLZHD YUJQQQUQ FTLRIDH YHTU MOE CIHU FMHEDD FTLRIDHE YQUIHZGQW, IHXFTH PXDFT HUQ ORPHIRDW PDDJQVFHXOF ZQUPHZ. KUHDEQL EWQKF D RXQU WHUQQQ HHDVOKGE, N IGHD YQUEFTXN XY HUQE XZG ER IHUWQU.`

25. Die Zahlenfolge $(451, 50, 398, 373)$ wurde mit dem RSA-Algorithmus mit dem öffentlichen Schlüssel $m = 667$ und $r = 117$ verschlüsselt. Ermitteln Sie den privaten Schlüssel s und entschlüsseln Sie die Nachricht.