Diskrete Mathematik ICE

5. Übungsblatt

26. April 2016

Verwenden Sie bei den Aufgaben 21 bis 23 lediglich einen Taschenrechner. Bei den Aufgaben 24 und 25 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

$$a = 7^{314159265},$$

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) $x \equiv \left(26^4\right)^{2016} \bmod 35$;

(b) $x \equiv 26^{\left(4^{2016}\right)} \bmod 35$.

23. Bei einem Diffie-Hellman-Schlüsselaustausch wurden die Werte $g = 3$, $p = 101$, $m = 65$ und $n = 66$ mitgehört. Bestimmen Sie die geheimen Parameter a und b sowie den Schlüssel $r = s$.

24. UZVJVI RSJRKQ NLIUV DZK VZEVI TRVJRI TYZWWIV DZK VZEVD MVIJTYLS MFE JZVSQVYE MVIJTYCLVJJVCK. UZVJV RIK UVI MVIJTYCLVJJVCLEX EVEEK JZTY RLTY IFK E LEU BREE JVYI CVZTYK ZD ZEKVIEVK VEKJTYCLVJJVCK NVIUVE. WLVI UVE QNVZKVE RSJRKQ NLIUVE QNVZ MVIJTYZVUVEV TRVJRI TYZWWIVJ MVINVEUVK, VZEVI WLVI UZV SLTYJKRSVE RE XVIRUVE GFJZKZFEVE LEU VZEVI WLVI UZV SLTYJKRSVE RE LEXVIRUVE GFJZKZFEVE.

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. AFBPBO XYPXQW TROAB JFQ BFKBO ZXBPXO ZEFCCOB JFQ BFKBJ SBOPZERY SLK AOBF SBOPZEIRBPPBIQ (AFBP FPQ DBILDBK). CRBO ABK WTBFQBK XYPXQW TROABK AFB YRZEPQXYBK ABP XIMEXYBQP RJPLOQFBOQ, XIIBOAFKDP KFZEQ JFQ BFKBJ HLKPQXKQBK SBOPZERY.

BVXQX ZIJ BXI KXIQYDFPXQQXFPGW GXGGJ QVYD ZPYD TSGSZFHDZAXJVQYDX QPAQJVJPJVSG. VT ZFFWXTXVGXG VQJ XVGX QSFYDX KXIQYDFPXQQXFPGW BPIYD XVGX DZXPCVWUXVJQZGZFNQX BXI APYDQJZAXG KXIWFXVYDQOXVQX FXVYDJ MP UGZYUXG. BZQ KXIOXGBXJX ZFHDZAXJ VQJ BZAXV GVYDJ PGAXBVGWJ USTHFXJJ MP XIUXGGXG, BZ GVYDJ ZFFX APYDQJZAXG KSIUSTTXG TPXQQXG.