

Aufgabe 24. Berechne ohne Taschenrechner $14^{(2017^{2017})} \bmod 60$. (3P.)

Aufgabe 25. Bestimme Zahlen $a_0, a_1, a_2 \in \mathbb{Z}_3$, sodaß die Funktion

$$f : \mathbb{Z}_3 \rightarrow \mathbb{Z}_3$$

$$0 \mapsto 1$$

$$1 \mapsto 0$$

$$2 \mapsto 0$$

durch die Formel $f(x) = a_0 + a_1x + a_2x^2$ dargestellt wird.

Aufgabe 26. (a) Beschreibe und berechne einen Diffie-Hellman-Schlüsselaustausch mit den Parametern $p = 31, g = 5, a = 13, b = 11$.

(b) Zu einem Diffie-Hellman-Schlüsselaustausch seien folgende Daten bekannt:

$$g = 7$$

$$p = 29$$

$$m = 24$$

$$n = 23$$

Bestimme wenn möglich die geheimen Parameter a, b und den Schlüssel r !

(2+3P.)

Aufgabe 27. Entschlüssele den folgenden Text (Satz- und Leerzeichen sind unverschlüsselt). Die Verwendung eines Computers für statistische Analyse etc. ist erlaubt (den String gibt es auch als Textdatei auf der Internetseite¹), die Vorgangsweise muß jedoch ausführlich erläutert werden. (3P.)

BLP JKLPPHPUGW KLDWHZHPUGW LKMGLTWD EZDWOPUGWHBWD
 PHUG FAY LOUGLHPUGWZ KLDWHZHPUGWZ LKMGLTWD
 LTUBWXGHJKYZAMNOPDFS BEOUG BHW QEPLWDQKHUGWZ
 TEUGPDLTWZ C, V EZB Q. PMEHEP ULOFHKHEP OECL PAKK WP
 CWRWPWZ PWHZ, BWO BEOUG GHZQEPWDQWZ WHZWP
 BHLJOHDHPUGWZ PDOHUGWP QEY U BWZ EZDWOPUGHWP FAZ U EZB C
 WHZXEWGODW. BLP ZWEW C REOBW LZ BWO PDWKKW BWP
 WZDXLKKWZWZ Q HZ BLP LKMGLTWD WHZCWOWHGD. RWHDWOW
 FWOLWZBWOEZWZ WOCLTWZ PHUG, ZLUGBWY BLP COHWUGHPUGW
 YEDDWOKLZB EZDWORAOXWZ EZB BWY PDLLDPCWTHWD BWO
 OAWYHPUGWZ OWMETKHJ WHZCWCKHWPBOD RAOBWZ RLO EZB
 FWOPDLWOJDWO TWBLOX WZDPDLZB, COHWUGHPUGW ZLYWZ EZB
 XOWYBRAWODWO HZ KLDWHZHPUGWO PUGOHXD RHWBWOQECWTWZ.
 HY WOCWTZHP TWPDLZB BLP KLDWHZHPUGW LKMGLTWD LEP
 BOWHEZBQRLZQHC, ZLWYKHUG LTUBWXCXGHJKYZAMNOPDFSQ. BHW
 QEPLWDQKHUGWZ TEUGPDLTWZ IER REOBWZ WOPD HY
 YHDDWKLKDWO WHZCWXEWGOD.

¹<https://www.math.tugraz.at/mathc/diskmath/2017/Uebungsblaetter/aufgabe27.txt>