

**Aufgabe 1.** *Public keys* werden für Verschlüsselung, *private keys* für Entschlüsselung verwendet (Skriptum, S. 62). Ich interpretiere die Aufgabe also so, dass in (a) ein *private key*  $(m, d)$  gegeben ist und (b) die Rekonstruktion eines *public keys* zur Verschlüsselung verlangt.

- a) Es gilt  $m = 2471004485256198699723347$  und  $d = 679256688868919115503281$ . Dann gilt  $\text{mod}(x^d, m) = 282033334039281634 = \text{merryxmas}$ .
- b) Man zerlege  $m$  in die Primfaktoren  $p = 1417021450037$  und  $q = 1743801750631$ . Daraus ergibt sich weiters  $\phi = (p - 1)(q - 1) = 2471004485253037876522680$  und, nachdem  $de \equiv_\phi 1$  gelten muss,  $e = 2094576675656119524619681$  als modulares Inverses von  $d$ . Die Nachricht **happynewyear** wird zu  $x = 231631314029203840201633$  codiert, was zu

$$\text{mod}(x^e, m) = 156693474749568634695296$$

verschlüsselt werden kann.

**Aufgabe 2** Der gegebene Mechanismus erzeugt keine besonders guten Zufallsziffern nachdem Ziffern  $< 6$  bedeutend wahrscheinlicher als solche  $\geq 6$  sind. Das ist dadurch bedingt, dass der Ausdruck  $b_0 + 2b_1 + 4b_2 + 8b_3$  uniform Werte im Bereich  $[0, 15]$  erzeugt. Werte in  $[10, 15]$  werden durch den Modulo allerdings zu  $[0, 5]$  gewandelt, sie kommen also häufiger vor.

0	1	2	3	4	5	6	7	8	9
0.124757	0.124656	0.124566	0.125098	0.124697	0.125103	0.062505	0.062703	0.062811	0.063104

Tabelle 1: Relative Häufigkeit der möglichen Ziffern,  $n = 1000000$ .

Sei  $B(i)$  eine Funktion die das Zufallsbit  $b_i$  retourniert. Dann wäre ein uniformer Generator die Funktion

$$f(i) = \begin{cases} b_i + 2b_{i+1} + 4b_{i+2} + 8b_{i+3} & \text{für } b_i + 2b_{i+1} + 4b_{i+2} + 8b_{i+3} < 10 \\ f(i+4) & \text{andernfalls} \end{cases}$$

welche so lange neue Bits durchprobiert bis eine Zahl  $< 10$  das Ergebnis ist. Somit wird die Verwendung von mod und die damit einhergehenden Probleme umgangen.

### Aufgabe 3

- a)  $\{\dots, -58, -23, 12, 47, 82, \dots\}$  bzw.  $\{35y + 12 : y \in \mathbb{Z}\}$ .
- b)  $\{\dots, -43, -19, 5, 29, 53, \dots\}$  bzw.  $\{24y + 5 : y \in \mathbb{Z}\}$ .
- c)  $\{\dots, -25, -1, 23, 47, 71, \dots\}$  bzw.  $\{24y + 23 : y \in \mathbb{Z}\}$ .