Dr. D. Frettlöh 22.6.2016

Übungen zur Vorlesung Panorama der Mathematik und Informatik

Blatt 10

Aufgabe 28: (Erweiterter euklidischer Algorithmus)
Bestimmen Sie ggT$(1058, 1472)$ und ggT$(89, 233)$. Finden Sie $a, b, c, d \in \mathbb{Z}$, so dass gilt

$$a \cdot 1058 + b \cdot 1472 = \text{ggt}(1058, 1472) \quad \text{und} \quad c \cdot 89 + d \cdot 233 = \text{ggt}(89, 233)$$

Aufgabe 29: (RSA)
Folgende Botschaft ist mit dem RSA-Verfahren verschlüsselt: 239845 075302 198960. Der öffentliche Schlüssel ist $N = pq = 262699$, $e = 207099$. Entschlüsseln Sie die Botschaft.

Jeder Block steht für drei Buchstaben. Wie so oft bedeutet 01: A, 02: B, ..., 26: Z, sowie diesmal ausnahmsweise 00: ! (Ausrufezeichen).

Aufgabe 30: (PGP)
Schicken Sie mir (Dirk Frettlöh) eine mit PGP (oder gpg) verschlüsselte Email, mit meinem Public Key codiert und mit Ihrer Signatur. Der Text soll Ihren Vor- und Nachnamen enthalten.

Rätsel der Woche: (3D-Tic-Tac-Toe mit drei Spielern)
Gegeben sind 27 Würfel der Kantanlänge 1, die in einer 3-mal-3-mal-3 Anordnung zu einem Würfel der Kantenlänge 3 zusammengesetzt sind. Färben Sie die 27 kleinen Würfel so mit drei Farben (etwa weiß, rot und blau), dass keine einfarbige Dreierreihe entsteht. Als "Dreierreihe" zählt hier jede waagerechte oder senkrechte Reihe von drei Würfeln, sowie Diagonalen (etwa vorne-oben-rechts nach vorne-unten-links) und auch Raumdiagonalen (etwa vorne-oben-rechts nach hinten-unten-links).

Abgabe: Donnerstag 29.6.2017 bis 12 Uhr per Email an die Tutoren.

Dorian Drost ddrost@techfak.uni-bielefeld.de Mi 16-18 T2-233
Dustin Matzel dmatzel@techfak.uni-bielefeld.de Fr 14-16 V2-200