Strom- und Blockchiffern

1. Der Schlüsselstrom einer Stromchiffer wird durch ein Schieberegister S_5, S_4, S_3, S_2, S_1 (Alphabet $\mathbb{Z}_{11}$) mit c_5=2, c_4=0, c_3=5, c_2=0, c_1=0 erzeugt. Die erste Belegung des Schieberegisters (eigentlicher Schlüssel) sei S_5=8, S_4=1, S_3=5, S_2=2, S_1=1. Man berechne den Anfang des Schlüsselstroms.

2. Gegeben ist eine Blockverschlüsselung durch: Blocklänge n=5, Alphabet $\mathbb{Z}_7$. Verschlüsselung:

   - Zuerst Permutation anwenden

$$\pi : \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 5 & 4 & 1 & 3 \end{pmatrix}$$

   - Dann Komponentenweise die Abbildung $\varphi(x)=3 \cdot x+2$ anwenden.

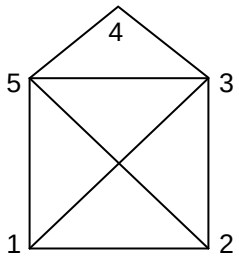
Man verschlüssle den Klartextblock m = (6, 0, 2, 2, 3) und entschlüssle den Schlüsselblock c.

3. Blockverschlüsselung in CFB-Mode. Alphabet: $\mathbb{Z}_{11}$.
Blockverschlüsselung für Blocklänge n = 5:
Addiere (Komponentenweise) (8, 1, 3, 3, 1)
Klartextblöcke der Länge r = 3
Invertiere JV = (3, 3, 1, 8, 10)
Man verschlüssle m_1 = (5, 1, 5), m_2 = (3, 8, 7), m_3 = (1, 1, 9).
Man entschlüssle den Schlüsseltext c_1, c_2, c_3.

4. Es sei G ein zusammenhängender Graph mit genau zwei Ecken A und B, die ungeraden Grad haben. Dann hat G eine eulersche Linie. Zum Zeichnen der Linie beginnen wir bei A, das Ende wird dann B. Ergibt sich die Linie bei Zeichnen „von selbst“ oder muss man sie konstruieren?

5. **Das Haus des Nikolaus**

Seit Generationen zeichnen die Kinder (und auch manche Erwachsene) das Haus des Nikolaus. Ohne mit dem Stift



abzusetzen und ohne eine Linie zweimal zu durchlaufen, muss das Haus gemalt werden. Nur wenn man in einer unteren Ecke des Hauses beginnt, gelingt es.

Sie sollen das Haus mit einem Programm bauen, das alle Möglichkeiten ausgibt, wenn man in der unteren linken Ecke anfängt. Die Ecken werden wie in der nebenstehenden Figur nummeriert. Eine mögliche Ausgabe wie „153125432” bedeutet, dass man in der Ecke 1 beginnt, einen Strich zu Ecke 5 zieht, dann zu Ecke 3 ...

Die *Ausgabe* der lexikographisch sortierten und nummerierten Lösungen erfolgt in die Datei *nikolaus.out*. Beispiel:

nikolaus.out
Loesung 1: 1 2 3 1 5 3 4 5 2 ..... Loesung 26: 1 3 5 2 3 4 5 1 2 ..... Loesung 44: 1 5 4 3 5 2 3 1 2

Literatur

1. Albrecht Beutelspacher, Marc-Alexander Zschiegner, *Diskrete Mathematik für Einsteiger. Mit Anwendungen in Technik und Informatik*, 3. Auflage, Vieweg Verlag, 2007.

2. Doina Logofătu, *Algorithmen und Problemlösungen mit C++*, Vieweg+Tebuner Verlag, 2010.