XOR-Verschlüsselung mit Pseudozufallszahlen

Author: Philipp G. Freimann (BBW (Berufsbildungsschule Winterthur) https://www.bbw.ch)

Schreiben Sie ein zweites Programm (siehe vorangehende Aufgabe), das ebenfalls eine Datei mit dem XOR-Verfahren verschlüsselt. Diesmal soll jedoch nicht eine Schlüsseldatei verwendet werden, um die Bytes zu chiffrieren. Stattdessen werden diesmal die codeBytes mit einem Pseudozufallsgereratoren erzeugt. Pseudozufallszahlen können mit einem Initialwert (seed) gestartet werden und produzieren für einen Startwert immer exakt die selbe Folge von Zufallszahlen. Diesen Effekt machen wir uns zu Nutze, indem wir diesmal als Code eine Folge von (Pseudo)Zufalls-Bytes benutzen:

```
import java.util.Random;
…
Random rnd = new Random(4453); // Geheimzahl
…
byte codeByte = (byte) rnd.nextInt();
```

Vorab im Geheimen wird nun nicht die Schlüsseldatei, sondern lediglich der "seed" als Schlüssel ausgetauscht.

Bemerkung: Das Verfahren ist nun mathematisch nicht mehr absolut sicher, denn ein Spion (Angreifer) muss nun lediglich alle Initialwerte (seed) ausprobieren.