

### 3. Übung zur Vorlesung Kryptographie

**Aufgabe 10:** ECB-Modus und CBC-Modus (2+4 Punkte)  
Mit Hilfe der Permutation

$$\pi: \left\{ \begin{array}{c|ccc} x & 1 & 2 & 3 \\ \pi(x) & 2 & 3 & 1 \end{array} \right\}$$

werden Bitstrings blockweise verschlüsselt.

- (a) Die Chiffre wird im ECB-Modus betrieben, der Klartext ist 111011101001. Wie lautet der Chiffretext?
- (b) Die Chiffre wird im CBC-Modus betrieben, der Chiffretext ist 111011101001. Wie lautet der Klartext?

**Aufgabe 11:** Synchrone Stromchiffre (4 Punkte)

Im ASCII-Code werden Zeichen durch 8-Bit-Wörter codiert. Beispielsweise entspricht Z dem Code dezimal 90, d.h., hexadezimal 0x5A und als 8-Bit-String 01011010. Vollständige Tabellen gibt es im WWW, z.B. unter <http://www.ascii-tabelle.de/>.

Der Chiffretext

1110010101110010

wurde aufgefangen, und man weiß, dass er von einer synchronen Stromchiffre mit Blocklänge  $m = 4$  und dem Schlüsselbildungsgesetz

$$z_{i+4} = (z_i + z_{i+1}) \bmod 2, \quad \text{für } i \geq 1$$

stammt. Von der anfänglichen Belegung  $z_1 z_2 z_3 z_4$  des Schlüsselstrings weiß man, dass darin genau zweimal die 0 und zweimal die 1 vorkommen. Welches zweibuchstabile deutsche Wort codiert der zugehörige Klartext in ASCII?

**Aufgabe 12:** Kryptanalyse einer Autokey-Chiffre (4 Punkte)

Der folgende Chiffretext wurde mit Hilfe einer Autokey-Chiffre mit Schlüsselwortlänge  $m = 1$  verschlüsselt:

PWNAULMZRTXRJEZ

Finden Sie mit Hilfe von Brute Force die Entschlüsselung.

**Aufgabe 13:** Inverse über  $\mathbb{Z}_{26}$  (2+4 Punkte)

Sind diese Matrizen über  $\mathbb{Z}_{26}$  invertierbar? Wenn ja, wie lauten ihre Inversen über  $\mathbb{Z}_{26}$ ?

$$(a): \begin{pmatrix} 2 & 5 \\ 9 & 5 \end{pmatrix} \quad (b): \begin{pmatrix} 1 & 11 & 12 \\ 4 & 23 & 2 \\ 17 & 15 & 9 \end{pmatrix}$$