SMS1 für MC, FHS Hagenberg
2. Übungsblatt für den 20. Oktober 2005

1. Wir codieren jedes Wort $(x_1, x_2, x_3, x_4) \in {\mathbb{Z}_2}^4$ als

$$K((x_1, x_2, x_3, x_4)) := (x_1, x_2, x_3, x_4) \cdot \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

   Bem.: Mit Elementen aus $\mathbb{Z}_2 = \{0, 1\}$ rechnet man so:
   $0 + 0 = 1 + 1 = 0$, $1 + 0 = 0 + 1 = 1$, $0 * 0 = 0 * 1 = 1 * 0 = 0$, $1 * 1 = 1$.

   (a) Wieviele verschiedene Codewörter (Elemente im Bildbereich von K) gibt es?

   (b) Begründen Sie, dass sich zwei Codewörter stets an mindestens 3 Stellen unterscheiden.

   (c) Wieviele Fehler dürfen bei der Übertragung eines Codeworts höchstens passieren, damit Sie das ursprünglich ausgesandte Codewort korrekt rekonstruieren können?

2. Fortsetzung von Aufgabe 1:

   (a) Welche der folgenden Wörter sind Codewörter? Was ist das am wahrscheinlichsten ausgesandte jeweilige Codewort?
   $a = (0, 1, 0, 1, 0, 1, 0), b = (1, 0, 1, 1, 0, 1, 0), c = (1, 0, 0, 1, 0, 0, 1)$

   (b) Zeigen Sie, dass für jedes Wort v in ${\mathbb{Z}_2}^7$ ein Codewort existiert, von dem sich v in höchstens einer Stelle unterscheidet.

   Hinweis: Zählen Sie die Wörter, die sich von einem Codewort an höchstens einer Stelle unterscheiden.

3. Die Nachricht BNQIX HMBJN SEZRK WZJMX YZJHP wurde mit einem Caesar verschlüsselt. D.h. jeder Buchstabe wurde durch den im Alphabet um n Stellen weitergeshifteten Buchstaben ersetzt (etwa $A \mapsto D$, $B \mapsto E$, $\ldots$, $Z \mapsto C$)

   Dechiffrieren Sie obige Nachricht.

Die Sicherheit moderner Kryptosysteme ist davon abhängig, dass sich gewisse mathematische Probleme nur sehr aufwändig lösen lassen.

4. Vergleichen Sie den Aufwand beim Faktorisieren versus dem beim Berechnen des ggT ohne Verwendung des Computers:

   (a) Bestimmen Sie alle Teiler von 1073.

   (b) Bestimmen Sie den ggT von 1073 und 1189.