WORT $\mapsto$ 23, 15, 18, 20

$\mapsto$ $a_2\ a_3\ a_4\ a_5$

Codierung $\mapsto$ $a_0\ a_1\ a_2\ a_3\ a_4\ a_5$

mit $a_0 + a_1 + a_2 + a_3 + a_4 + a_5 \equiv 0 \mod 31$

$a_1 + 2a_2 + 3a_3 + 4a_4 + 5a_5 \equiv 0 \mod 31$

$\Rightarrow$ 01, 16, 23, 15, 18, 20

Annahme: Es gibt einen Übertragungsfehler

Empfange sind 01, 16, 23, 09, 18, 20

Ziel: erkenne, daß ein Fehler der Größe 6 passiert ist und daß er an der Stelle a_3 auftritt

Suche nach Fehler:

$$C = a_0 + a_1 \cdot 4 + \dots + a_5$$

$$= 1 + 16 + 23 + 9 + 18 + 20$$

$$= 87 \equiv 25 \mod 31$$

$$\equiv -6 \mod 31$$

$\Rightarrow$ Fehler aufgetreten

Fehler der Größe e an der Stelle x liefert in der zweiten Gleichung ein Fehler xe

$$S = 1 \cdot a_1 + 2a_2 + \dots + 5a_5$$

$$= 261 \equiv 13 \mod 31$$

also gilt: $25x \equiv 13 \mod 31$

$$5 \cdot 25 - 4 \cdot 31 = 1$$

$\Rightarrow$ $x \equiv 5 \cdot 13 \mod 31$

$$\equiv 3 \mod 3$$

$\Rightarrow$ Fehler an der Position 3

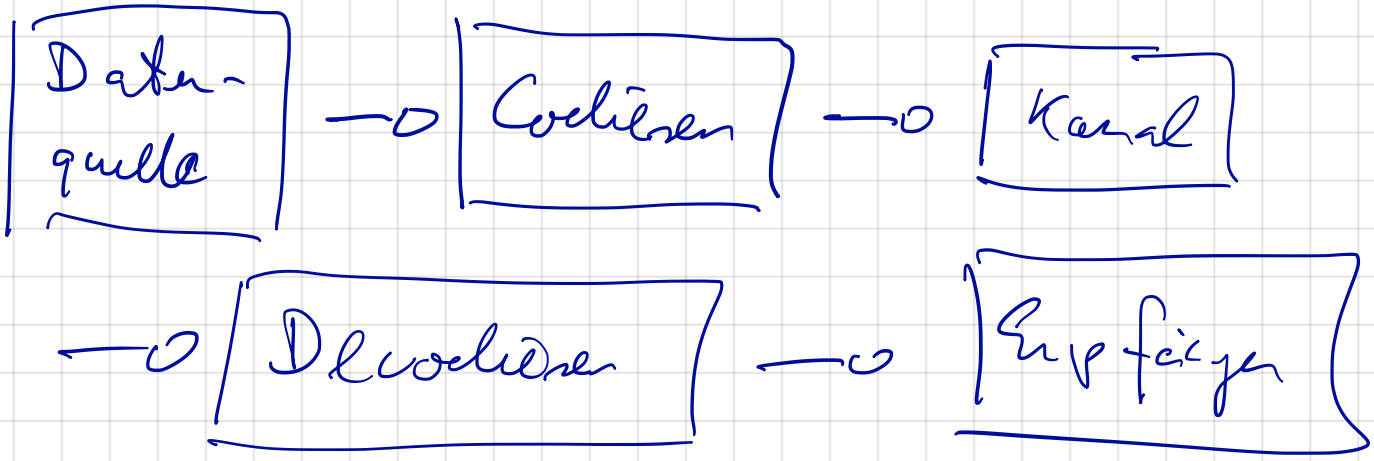
$\Rightarrow$ $q_3 = 9$ muss um 25 korrigiert werden

$\Rightarrow$ $9 - 25 \equiv 9 + 6 = 15 \mod 31$

$\Rightarrow$ richtiges Wort

01, 16, 23, 15, 18, 20

Codierungstheorie abstrakt



Alphabet: endliche Menge von Zeichen

$$\mathcal{A} = \{ z_1, z_2, \dots, z_m \}$$

Wort der Länge n: Folge von n Zeichen

Codierung: Umwandlung von einem Alphabet in ein anderes

Bsp: $A_1 = \{A, B, C, \ldots, Z\}$

$A_2 = \{01, 02, \ldots, 26\}$

Codierung: A $\rightsquigarrow$ 01, B $\rightsquigarrow$ 02, ...

Bsp: $A_1 = \{0, 1, 2, \ldots, 9\}$

$A_2 = \{0, 1, 2, 3, 4\}$

Übergang über A_1 von Zahl im 10er-System

$\longrightarrow$ A_2 $\rightsquigarrow$ $\longrightarrow$ 5er-System

Codierung $\hat{=}$ Umwandlung einer Zahl

Kryptographie

Situation: Alice und Bob wollen über einen offenen Kanal kommunizieren, Eve will sie belauschen

- Alice möchte Bob eine Nachricht schicken, nennt Klartext m
- Alice chiffriert Klartext m mit einem Schlüssel e und einer Verschlüsselungsfunktion E zum Chiffretext $c = E(e, m)$
- Alice schickt c an Bob
- Bob entschlüsselt Chiffretext c mit einem Schlüssel d und einer Entschlüsselungsfunktion D: $D(d, c)$