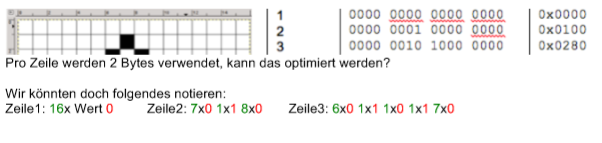
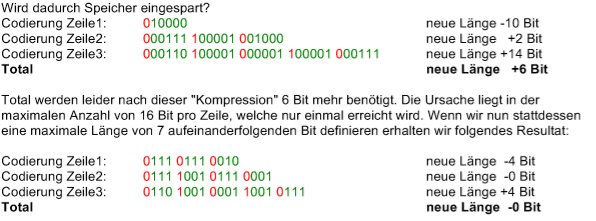
Spicker Modul 114 Olivier Winkler 11.06.18

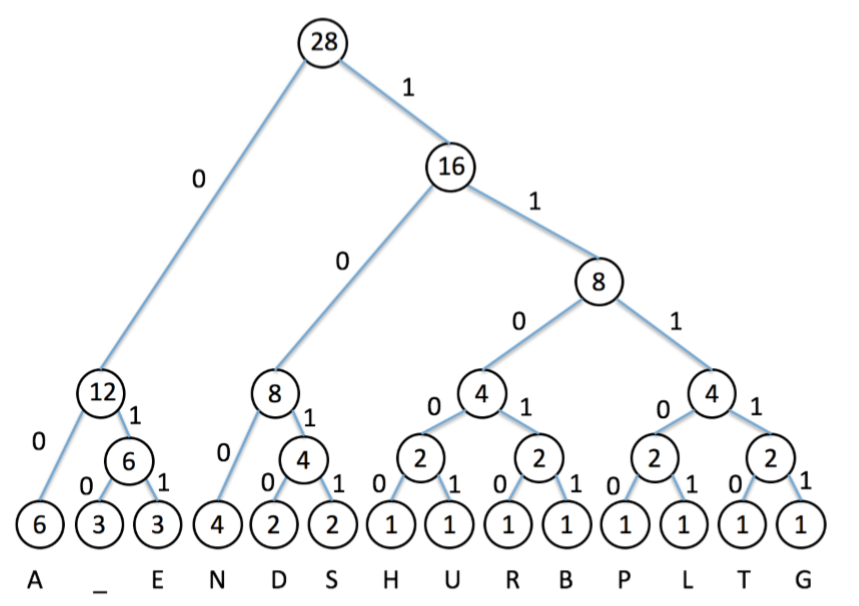
Kompression:

Verlustfrei 🡪 Daten verkleinern, keine Verluste, wenig Speicher

Verlustbehaftet 🡪 Menschliche Sinne bearbeiten, Daten verändern ohne dass wir es merken.

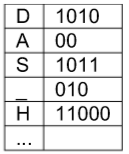
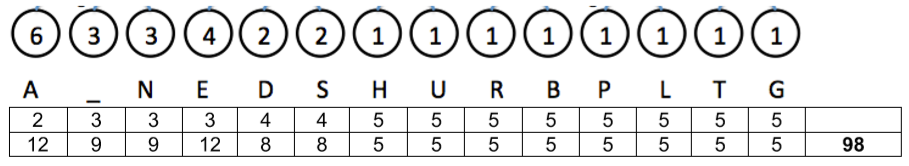
**Lauflängencodierung:**

1111 1110 0000 1000 0001 1111 🡪 7 5 1 6 5 🡪 111 101 001 110 101 (Von 24 Bits auf 15 Bits reduziert).

**Huffman Code**

Daten „Das Haus“ 🡪 Zählen von Buchstaben (D:1, A:2, S:2, H:1, U:1, Leerzeichen (\_): 1) Danach Anzahl Vorkommen (8) mit Daten (8) vergleichen um sicherzugehen. Als nächstes wird Baum gebaut:

Danach hat jeder Buchstabe seine Bitfolge:

Errechnung von benötigtem Speicher:

Kompressionsrate (sagt um wie viel Mal grösser die Originaldatei war.) Immer x:1

Menge komprimiert = Menge unkomprimiert / Kompressionsrate

Kompressionsrate = Menge unkomprimiert / Menge komprimiert (800 / 200 🡪 4:1)

Kompressionsfaktor (sagt um wie viel Mal kleiner die komprimierte Datei ist.) Immer 1:x

Menge komprimiert = Menge unkomprimiert \* Kompressionsfaktor

Kompressionsfaktor = Menge komprimiert / Menge unkomprimiert (200 / 800 🡪 1:4v)

**Cäsar Verschlüsselung**

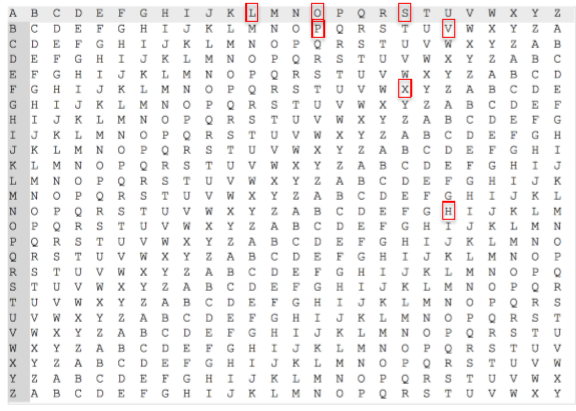
Klartext = Hallo Schlüssel = C Tabelle: Geheimtext = KCNNQ

ABCDEFGHIJKLMNOPQRSTUVWXYZ

CDEFGHIJKLMNOPQRSTUVWXYZAB

**Vigenere Chiffre**

Klartext = ABBAFAN Schlüssel = SOUL Geheimtext = SPVLXOH

Linke Spalte ist für Klartext und die Spalte oben ist für Schlüssel

XOR

x y

0 0 0

0 1 1

1 0 1

1 1 0

Kryptografie 🡪 Lehre der Verschlüsselung

Kryptoanalyse 🡪 Inhalt ohne Schlüssel zu entschlüsseln.

Kryptologie 🡪 Beide Begriffe zusammen.

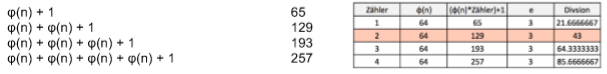
**RSA Verfahren: (Beispiel)**

1. Primzahlen p & q (p = 5, q = 17)
2. Modulzahl errechnen (n) n = p \* q (5 \* 17 = 85)
3. Geheime Modulzahl errechnen Phi(n) = (p-1) \* (q-1) ((5-1)\*(17-1) = 64)
4. Teilerfremde Zahl suchen (Zahle welche bei beiden nicht teilbar ist) e (e = 3)

Öffentlicher Schlüssel Privater Schlüssel

n = 85 e = 3 n = 85 d = 43

d herausfinden:

Nachricht versenden

Klartext m, Geheimtext c = m^e (mod n) (m = 2, c = 2^3 (mod 85) = 8)

Nachricht entschlüsseln

Geheimtext c, Klartext m = c^d (mod n) (c = 8, m = 8^43 (mod 85) = 2)