3 Beispiele für perfekte Sicherheit

Trivialbeispiele

Beispiel 0: $\#M_0 = 1$

Dieses Beispiel ist natürlich kryptologisch unsinnig, da der Kryptoanalytiker den einzig möglichen Klartext von vornherein kennt. Also kann er durch den Geheimtext keine zusätzliche Information über den Klartext gewinnen.

Sei $M_0 = \{a\}$. Da für alle $c \in C_1$ trivialerweise $P(a|c) = 1 = P(a)$ gilt, ist F, wie immer es auch definiert ist, perfekt sicher.

Beispiel 1: $\#M_0 = 2$

Das kleinste sinnvolle Beispiel beinhaltet zwei mögliche Klartexte. Sei (o. B. d. A.) $M_0 = M_1 = \{0,1\} = C_1 = K$. Sei f_0 die identische Abbildung auf $\{0,1\}$ und f_1 die Vertauschung von 0 und 1. Ferner seien die beiden Schlüssel 0 und 1 gleichwahrscheinlich: $P(0) = P(1) = \frac{1}{2}$.

Dann ist $K_{00} = K_{11} = \{0\}$, $K_{01} = K_{10} = \{1\}$. Daher ist F nach Satz 2 perfekt sicher.

Die Verschiebechiffre

Hier ist $M_0 = K = C_1$ eine Gruppe und $F\colon M_0 \times K \longrightarrow C_1$ die Gruppenoperation, also $f_k(a) = a * k$. Die Mengen

$$K_{ac} = \{k \in K \mid a * k = c\} = \{a^{-1} * c\}$$

sind alle einelementig. Wird wie üblich $P(k) = \frac{1}{\#K}$ für alle Schlüssel $k \in K$ angenommen, so ist F perfekt sicher.

Die Beispiele 0 und 1 oben waren die Spezialfälle der ein- und zweielementigen Gruppe. Weitere Spezialfälle folgen als Beispiele 2 und 3.

Beispiel 2: Die CAESAR-Chiffre

Das ist die Verschiebechiffre auf der zyklischen Gruppe $\Sigma = \mathbb{Z}/n\mathbb{Z}$ der Ordnung n.

Also ist die CAESAR-Chiffre perfekt sicher, *sofern nur Nachrichten der Länge 1 verschlüsselt werden und der Schlüssel für jede Nachricht zufällig neu gewählt wird.*

Beispiel 3: Die VERNAM-Chiffre

Das ist die Vereinigung der Verschiebechiffren auf den Gruppen $\Sigma^r = M_0$ mit $\Sigma = \mathbb{Z}/n\mathbb{Z}$. Nachrichten sind also jeweils Texte der Länge r, und Schlüssel sind *zufällig gewählte* Buchstabenfolge der gleichen Länge r.

Da man insbesondere den Schlüssel für jede Nachricht neu wählen muss, heisst diese Chiffre auch **One Time Pad**. Man stellt sich einen Abreisskalender vor: Jedes Blatt enthält einen zufälligen Buchstaben und wird nach Verwendung abgerissen und vernichtet.

Die VERNAM-*Chiffre ist der Prototyp einer perfekten Chiffre.*

Im Spezialfall $\Sigma = \{0,1\}$ erhält man die binäre VERNAM-Chiffre, die Bitstrom-Verschlüsselung mit völlig zufälliger Schlüsselbitfolge.

Gegenbeispiel: Die monoalphabetische Chiffre

Hier wird $M_0 = \Sigma^r$ gewählt und $K = \mathcal{S}(\Sigma)$. Etwa für $r = 5$ haben wir schon gesehen, dass

$$P(\texttt{bauer}|\texttt{XTJJA}) = 0 < q = P(\texttt{bauer}).$$

Die monoalphabetische Chiffre ist also (für $r \geq 2$ und $n \geq 2$) nicht perfekt. Für $r = 1$ ist sie dagegen nach Satz 2 (mit $s = (n-1)!$) perfekt.