9.6 Kryptologische Anwendungen

Die Eindeutigkeitsdistanz ist ein sehr grobes Maß für die Qualität einer Chiffre. Sie wird in der modernen Kryptologie praktisch nicht verwendet. Unter der Annahme von bekanntem Klartext verliert sie ihre Bedeutung (außer für perfekte Chiffren, da bleibt sie ∞).

Eine große Eindeutigkeitsdistanz erreicht man durch:

- einen großen Schlüsselraum,
- Minderung der Redundanz der Sprache, z. B. durch vorherige Kompression.

Anwendung 1. Die PORTA-Drehscheiben-Chiffre ist nur unwesentlich stärker als die TRITHEMIUS-BELASO-Chiffre, da die Eindeutigkeitsdistanz nur um den konstanten Summanden 26.8 erhöht wird. Das bedeutet, dass bei langer Periode die Komplikation durch das permutierte Primäralphabet kaum zusätzliche Sicherheit bringt.

Anwendung 2. Eine weitere Anwendung der SHANNONschen Theorie betrifft die Lauftextverschlüsselung: Die Kryptoanalyse gewinnt ja aus einem Geheimtext der Länge r zwei sinnvolle Klartexte der Gesamtlänge $2r$. Damit das klappt, muss die Redundanz der Sprache mindestens 50% sein.

Stellen wir uns allgemeiner eine q-fache Lauftextverschlüsselung mit q unabhängigen Schlüsseltexten vor. Wenn die Kryptoanalyse möglich ist, ist aus einem Geheimtext der Länge r sinnvoller Text der Gesamtlänge $(q+1) \cdot r$ rekonstruierbar, die Redundanz der Sprache also $\geq \frac{q}{q+1}$. Da die Redundanz von Deutsch mit 70% kleiner als $\frac{3}{4}$ ist, kann man daraus schließen, dass eine *dreifache Lauftextverschlüsselung sicher* ist. Für Englisch mit seiner etwas geringeren Redundanz könnte sogar eine zweifache Lauftextverschlüsselung schon sicher sein.

Anwendung 3. Die Eindeutigkeitsdistanz wird auch als Anhaltspunkt dafür genommen, wieviel Geheimtext mit dem gleichen Schlüssel dem Gegner in die Hände fallen darf, ohne dass er etwas damit anfangen kann; d. h., wie häufig Schlüsselwechsel nötig sind.

Allgemein kann man die SHANNONsche Theorie zusammenfassen zu der Regel: *Eine notwendige Bedingung für die Lösung einer Chiffre ist, dass „Information im Geheimtext + Redundanz der Sprache“ ≥ „Information im Klartext + Information im Schlüssel“.*