8.5 Homophone Verschlüsselung

ZUSATZ

> ZUSATZ
>
> Die Abschnitte 8.5 und 8.6 stehen in keinem der beiden Lehrpläne. Sie schließen aber die Lücke zwischen Vigenère und den modernen Verfahren: erst die Statistik verwischen, dann die Wiederholung des Schlüssels abschaffen.

Ein anderer Weg, die Statistik zu verwischen: Jedem Klartextbuchstaben wird nicht ein Zeichen zugeordnet, sondern eine *Menge* von Zeichen – und zwar so viele, wie es seiner Häufigkeit entspricht. Beim Verschlüsseln wählt man daraus zufällig aus.

```
A: 10, 21, 52, 59, 71, 84
B: 20, 34
C: 06, 28, 80
E: 09, 18, 33, 38, 40, 42, 53, 54, 55, 60, 66, 75, 85, 86, 92, 93, 99
```

Weil dem E siebzehn Zeichen zur Verfügung stehen, dem B nur zwei, kommt am Ende jedes Zeichen etwa gleich oft vor: Die Häufigkeitsanalyse läuft ins Leere. Der Preis ist ein längerer Geheimtext und eine große Tabelle als Schlüssel. Sicher ist auch dieses Verfahren nicht – Bigramme und Wortstrukturen bleiben erhalten und wurden historisch erfolgreich ausgenutzt.

Gymnasium Ottweiler