1.5 Kaskaden verschiedener Chiffren

Beispiele

1. Monoalphabetische Substitutionen und Transpositionen sind vertauschbar. Eine Komposition von mehr als jeweils einer solchen Operation bringt also nichts, da sie einzeln für sich je eine Gruppe bilden. Eine Komposition aus einer monoalphabetischen Substitution und einer Transposition ist noch ziemlich leicht sogar ohne bekannten Klartext zu brechen, da die wichtigsten Buchstaben aufgrund ihrer Häufigkeiten erkannt werden.

2. Auch für periodische polyalphabetische Chiffren und Transpositionen gilt diese Bemerkung – solange die Periodenlänge nicht nach jedem Schritt geändert wird. Hier kann man schon recht komplizierte Chiffren erzeugen.

3. Die Enigma führte die Komposition aus einer monoalphabetischen, einigen polyalphabetischen verschiedener Periode und nochmal einer monoalphabetischen Substitution aus. Das ganze war zusammengenommen auch wieder nur eine polyalphabetische Substitution sehr langer Periode.

4. Die ADFGVX-Chiffre der deutschen Wehrmacht im 1. Weltkrieg bestand aus einer Substitution gefolgt von einer Spaltentransposition; die Substitution wurde ausgeführt, indem die 26 Buchstaben und 10 Ziffern in ein 6-mal-6-Quadrat nach Vorgabe eines Schlüssels geschrieben wurden und jedes Zeichen durch seine Koordinaten in diesem Quadrat ersetzt wurde, welche mit A, D, F, G, V, X bezeichnet waren. Es gelang den Franzosen (Painvin und Givierge) zum Teil, diese Chiffre zu brechen.

5. Die Komposition von monoalphabetischer Chiffre und einer Autokey-Chiffre werden wir bald als „Betriebsmodus bei Blockverschlüsselung“ kennen lernen. Die Autokey-Chiffre erschwert einige Angriffe, erhöht aber insgesamt die Sicherheit nur unwesentlich.

6. Ferner sei noch einmal daran erinnert, dass die Drehscheiben-Chiffre nach Porta sich als Komposition einer monoalphabetischen Substitution und einer Belaso-Chiffre darstellen ließ – sogar in beiden möglichen Reihenfolgen.

Insgesamt kann man sagen, dass Kaskaden verschiedener Chiffren oft zu Verbesserungen der Sicherheit führen, aber durchaus nicht immer. Es ist in jedem Fall eine sorgfältige Analyse der entstehenden Produkt-Chiffre nötig, bevor man ihr vertraut.