Diese wurden - im Gegensatz zur periodischen polyalphabetischen Chiffre - tatsächlich von VIGENÈRE zuerst vorgeschlagen.

Ver- und Entschlüsselung

Das Alphabet Σ wird wieder mit einer Gruppenstruktur * versehen.

Es wird (unabhängig von der Länge des Klartextes) ein Schlüssel $k \in \Sigma^l$ aus l Buchstaben gewählt.

Um einen Klartext $a \in \Sigma^r$ der Länge r zu verschlüsseln, wird der Schlüssel durch Anhängen des Anfangsstücks von a zu einem Schlüsseltext der Länge r ergänzt.

Mit diesem Schlüsseltext wird dann eine Lauftextverschlüsselung durchgeführt:

$$\begin{array}{l} a_0\ a_1\ \ldots\ a_{l-1}\ a_l\ \ldots\ a_{r-1} \\ k_0\ k_1\ \ldots\ k_{l-1}\ a_0\ \ldots\ a_{r-l-1} \\ \hline c_0\ c_1\ \ldots\ c_{l-1}\ c_l\ \ldots\ c_{r-1} \end{array}$$

Verschlüsselt wird also nach der Formel:

$$c_i = a_i * k_i \quad \text{für } i = 1, \ldots, l\text{-}1,$$

$$c_i = a_i * a_{i-l} \quad \text{für } i = l, \ldots, r\text{-}1,$$

Beispiel: (l = 1, Schlüssel = X)

```
K L A R T E X T
X K L A R T E X
---------------
H V L R K X B Q
```

Entschlüsselt wird nach der Formel:

$$a_i = c_i * k_i^{-1} \quad \text{für } i = 1, \ldots, l\text{-}1,$$

$$a_i = c_i * a_{i-l}^{-1} \quad \text{für } i = l, \ldots, r\text{-}1,$$

Bemerkung: Selbstverständlich könnte man auch statt des Standard-Alphabets (also der TRITHEMIUS-Tafel) ein permutiertes Primäralphabet verwenden. Diese Methode wird hier nicht weiter verfolgt.

Ansätze zur Kryptoanalyse

1. Exhaustion, falls l klein.

2. Behandlung als Lauftext-Chiffre ab Stelle l oder, falls der Schlüssel als Wort oder Text der Sprache gewählt wurde, sogar ab dem Anfang des Geheimtextes:
   a. Wahrscheinliches Wort.
   b. Häufige Wörter oder Wortteile.
   c. Häufigkeitsanalyse.
   d. Häufige Buchstabenkombinationen.

   Durch die Wiederholung des Klartextes im Schlüssel ist die Situation gegenüber der eigentlichen Lauftext-Chiffre sogar deutlich vereinfacht.

3. Ähnlichkeit zur TRITHEMIUS-BELASO-Chiffre, siehe im nächsten Abschnitt.

4. Algebraische Kryptoanalyse (bei bekanntem Klartext): Gleichungen lösen. Die Methode lässt sich etwas leichter bei additiver Schreibweise der Gruppenoperation (wie bei abelschen Gruppen üblich) beschreiben:

$$
\begin{array}{lcl}
c_0 & 1\ 0\ \ldots\ 1 & k_0 \\
c_1 & \ldots\ 1\ 0\ \ldots\ 1 & | \\
| & \ldots & | \\
c_{l-1} & = \quad 1\ 0\ \ldots\ 1 & k_{l-1} \\
c_l & \ldots & a_0 \\
| & 1\ 0\ \ldots\ 1 & | \\
c_{r-1} & & | \\
 & & | \\
 & & a_{r-1}
\end{array}
$$

   mit einer $r*(r+l)$-Koeffizientenmatrix. Es handelt sich also um ein lineares Gleichungssystem in einem $\mathbf{Z}$-Modul aus r Gleichungen mit $r+l$ Unbekannten ($k \in \Sigma^l$, $a \in \Sigma^r$).

   Ein solches Gleichungssystem ist »im allgemeinen« lösbar, wenn l Unbekannte erraten sind, also Klartext der Länge l bekannt ist (nicht notwendig zusammenhängend).

   Diese Theorie wird bei den linearen Chiffren ausführlich beschrieben.

Geheimtext-Autokey

... ist eine ganz schlechte Variante. Beispiel:

```
K L A R T E X T
X H S S J C G D
---------------
H S S J C G D W
```

Die Definition dieses Verfahrens und die Kryptoanalyse darf sich der Leser selbst ausdenken.

Nicht ganz so trivial ist das Verfahren, wenn ein permutiertes Primäralphabet verwendet wird.

Autor: Klaus Pommerening, 19. Juni 2002; letzte Änderung: 25. Juni 2002

E-Mail an Pommerening@imsd.uni-mainz.de.