Wiederholung

Bei der Beschreibung der PORTA-Chiffre war

$$f_{\sigma,k} = f_\sigma \circ f_{\varepsilon,k'}.$$

mit $k' = f_\sigma^{-1}(k)$.

Das wurde bei der Kryptoanalyse aber gar nicht benützt, sondern eine ähnliche Formel der Gestalt:

$$f_{\sigma,k} = g \circ f_\sigma,$$

wobei g ein Verrücken und g^{-1} das Zurechtrücken der Begleitalphabete bedeutete.

Eine mathematische Beschreibung von g ist gesucht.

Die Alphabet-Tafel war

s_0	s_1	s_2	...	s_{n-1}
t_0	t_1	t_2	...	t_{n-1}
t_1	t_2	t_3	...	t_0
.	.	.		.
t_{n-1}	t_0	t_1	...	t_{n-2}

mit $t_i = \sigma(s_i)$ für $0 \le i \le l\text{-}1$, σ die Permutation zum Primäralphabet.

Verschiebungen im Primäralphabet

Sei das Alphabet $\Sigma = \{s_0,...,s_{n-1}\}$ wieder mit $\mathbf{Z}/n\mathbf{Z}$ identifiziert. Die Indizes werden mod n addiert.

Verschiebungen im Standard- und im Primäralphabet werden dann mathematisch so beschrieben:

- τ = Verschiebung um 1 im Standardalphabet, $\tau(s_i) = s_{i+1}$.
- τ^k = Verschiebung um k im Standardalphabet, $\tau^k(s_i) = s_{i+k}$.
- $\sigma\tau\sigma^{-1}$ = Verschiebung um 1 im Primäralphabet,

$$t_i \overset{\sigma^{-1}}{\longmapsto} s_i \overset{\tau}{\longmapsto} s_{i+1} \overset{\sigma}{\longmapsto} t_{i+1}.$$

- $\sigma\tau^k\sigma^{-1} = (\sigma\tau\sigma^{-1})^k$ = Verschiebung um k im Primäralphabet.

Damit läßt sich die alte Formel in die gesuchte umrechnen, zunächst buchstabenweise:

$$f_{\sigma,k}(a_i) = \sigma\tau^{k_i'}(a_i) = (\sigma\tau^{k_i'}\sigma^{-1})(\sigma a_i)$$

Wird mit $b \in \Sigma^r$ das monoalphabetische Bild von a bezeichnet, also $b_i = \sigma(a_i)$, so sieht man, dass die gesuchte Funktion g die »Verrückung um k_i' des Primäralphabets« f_k^σ ist und die Beschreibung

$$b_i \to (\sigma\tau^{k_i'}\sigma^{-1})(b_i)$$

hat. Besser gesagt ist es eine Folge von Verrückungen des Primäralphabets.

Mit dieser Überlegung ist gezeigt:

> **Satz** (Kryptoanalyse der PORTA-Chiffre bei bekannter Periode). *Die PORTA-Chiffre $f_{\sigma,k}$ entsteht aus der monoalphabetischen Chiffre f_σ durch die Folge f_k^σ von Verrückungen des Primäralphabets.*

Zusammenfassung

Die kanonische Kryptoanalyse der PORTA-Chiffre $f_{\sigma,k}$ besteht aus den Schritten:

1. Bestimmung der Periode.
2. Zurechtrücken der Begleitalphabete - das ist möglich, ohne das Primäralphabet, also σ, zu kennen.
3. Kryptoanalyse der monoalphabetischen Substitution f_σ ohne vorherige Kenntnis von σ.

Der Aufwand für die Kryptoanalyse ist übrigens im wesentlichen von der Schlüssellänge unabhängig! Allerdings sinkt die Erfolgswahrscheinlichkeit bei längerer Periode:

- Die Wahrscheinlichkeit, nicht-zufällige Parallelstellen zu finden, sinkt.
- Die Chance, in den Kolonnen brauchbare Häufigkeitsverteilungen zu finden, sinkt.

Und als Fazit dieser Erkenntnisse für die Sicherheit polyalphabetischer Chiffren:

- Je größer die Periode, desto besser die Sicherheit.
- Die Wahl von unabhängigen Alphabeten bringt bessere Sicherheit.

Beides führt aber auch zu umständlicherer Handhabung und wurde in der Geschichte der Kryptographie daher oft vermieden.

Autor: Klaus Pommerening, 13. Februar 2000; letzte Änderung: 12. August 2002.

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