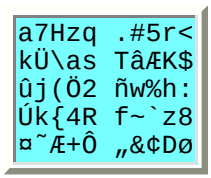
Kryptologie

Mathematische Beschreibung der periodischen polyalphabetischen Substitution



Der allgemeine Fall

Allgemein ist bei einer **polyalphabetischen Chiffre der Periode** l der Schlüsselraum

$$K \subseteq \mathbf{S}(\Sigma)^l$$

eine Menge von Folgen der Länge l von Permutationen des Alphabets Σ. Die Verschlüsselungsfunktion

$$f_k: \Sigma^r \to \Sigma^r$$

zum Schlüssel $k = (\sigma_0,...,\sigma_{l-1})$ sieht so aus:

$$\begin{array}{cccccccc} a_0 & a_1 & \dots & a_{l-1} & a_l & \dots & a_i & \dots\ a_{r-1} \\ \downarrow & \downarrow & & \downarrow & \downarrow & & \downarrow & \\ \sigma_0 a_0 & \sigma_1 a_1 & \dots & \sigma_{l-1} a_{l-1} & \sigma_0 a_l & \dots & \sigma_{i \bmod l} a_i & \dots \end{array}$$

Verschlüsselt wird für $c = f_k(a) \in \Sigma^r$ also nach der Formel

$$c_i = \sigma_{i \bmod l}(a_i),$$

und entschlüsselt nach der Formel

$$a_i = (\sigma_{i \bmod l})^{-1}(c_i).$$

Effektive Schlüssellängen

a) Die BELASO-Chiffre

Hier ist das Primäralphabet das Standard-Alphabet und als bekannt anzunehmen. Der Schlüssel wird als Wort (oder Text) $\in \Sigma^l$ gewählt. Also ist

$$\#K = n^l,$$
$$d(F) = l \cdot {}^2\log(n).$$

Für $n = 26$ ist das $\approx 4.70 \cdot l$.

b) Die PORTA-Chiffre

Hier wird als Schlüssel eine Permutation $\in \mathbf{S}(\Sigma)$ und unabhängig davon ein Schlüsselwort $\in \Sigma^l$ gewählt. Also ist

$$\#K = n! \cdot n^l,$$
$$d(F) = l \cdot {}^2\log(n) + {}^2\log(n!) \approx (n+l) \cdot {}^2\log(n).$$

Für $n = 26$ ist das $\approx 4.70 \cdot l + 88.38$.

(Ist dem Gegner das Primäralphabet allerdings bekannt, etwa durch Eroberung einer Drehscheibe, reduziert sich die effektive Schlüssellänge auf die der BELASO-Chiffre.)

c) Der allgemeine Fall

... der periodischen polyalphabetischen Substitution mit l unabhängigen Alphabeten:

$$K = \mathbf{S}(\Sigma)^l,$$
$$d(F) = {}^2\log((n!)^l) \approx ln \cdot {}^2\log(n).$$

Für $n = 26$ ist das $\approx 122.2 \cdot l$.

Eine andere Sicht

Eine l-periodische polyalphabetische Substitution ist eine l-graphische Substitution (oder Blockchiffre der Länge l), beschrieben durch die Produktabbildung

$$(\sigma_0,...,\sigma_{l-1}): \Sigma^l = \Sigma \times ... \times \Sigma \to \Sigma \times ... \times \Sigma = \Sigma^l,$$

also eine monoalphabetische Substitution über dem Alphabet Σ^l.

Speziell ist die BELASO-Chiffre einfach die Verschiebechiffre über Σ^l, identifiziert mit $(\mathbf{Z}/n\mathbf{Z})^l$.

Ist $\Sigma = \mathbf{F}_2$, so wird die BELASO-Chiffre zum schlichten XOR auf $\mathbf{F}_2{}^l$.

Autor: Klaus Pommerening, 12. November 1999; letzte Änderung: 13. Februar 2000.

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