Kryptologie

Algorithmische Bescheibung der Drehscheiben-Chiffre

```
a7Hzq .#5r<
kÜ\as TâÆK$
ûj(Ö2 ñw%h:
Úk{4R f~`z8
¤˜Æ+Ô „&¢Dø
```

Bezeichnungen

Sei $\Sigma = \{s_0,...,s_{n-1}\}$ das Alphabet, das mit der Gruppenstruktur als $\mathbf{Z}/n\mathbf{Z}$ interpretiert (»codiert«) wird.

Der Schlüssel $(\sigma,k) \in \mathbf{S}(\Sigma) \times \Sigma^l$ besteht aus einem (mit σ permutierten) Primäralphabet und einem Kennwort $k = (k_0,...,k_{l-1}) \in \Sigma^l$.

Die Verschlüsselungsfunktion wird so bezeichnet:

$$f_{\sigma,k}: \Sigma^* \to \Sigma^*$$

Spezialfall

$f_{\varepsilon,k}$ ist die BELASO-Chiffre mit Schlüssel k, wenn mit $\varepsilon \in \mathbf{S}(\Sigma)$ die identische Permutation bezeichnet wird.

Die Alphabet-Tafel

... hat dann die Gestalt

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 $0 \le i \le l-1$.

Die Verschlüsselungsfunktion

Wie wird ein Text $a = (a_0,a_1,a_2,...) \in \Sigma^r$ verschlüsselt?`

Sei

$$a_i = s_q \quad \text{und} \quad k_i = t_p.$$

Dann muss man den Geheimtextbuchstaben c_i in Zeile p und Spalte q ablesen, also:

$$c_i = t_{p+q} = \sigma(s_{p+q}) = \sigma(s_p + s_q) \qquad \text{[Summe in } \mathbf{Z}/n\mathbf{Z}\text{]}.$$

Da

$$k_i = t_p = \sigma(s_p), \quad \text{ist} \quad s_p = \sigma^{-1}(k_i),$$

also

$$c_i = \sigma(a_i + \sigma^{-1}(k_i)),$$

wobei die Summe in $\mathbf{Z}/n\mathbf{Z}$ zu bilden ist.

Mit dieser Überlegung ist gezeigt, wobei f_σ die monoalphabetische Verschlüsselung zu σ bezeichnet:

> **Satz.** *Die Drehscheiben-Chiffre $f_{\sigma,k}$ ist die Komposition (»Überchiffrierung«) der BELASO-Verschlüsselung $f_{\varepsilon,k'}$ - wobei $k' = f_\sigma^{-1}(k)$ - mit der monoalphabetischen Verschlüsselung f_σ,* also
>
> $$f_{\sigma,k} = f_\sigma \circ f_{\varepsilon,k'}.$$

Algorithmus

Daraus ergibt sich der folgende Algorithmus:

1. Bilde $k' = f_\sigma^{-1}(k)$, also $k_i' = \sigma^{-1}(k_i)$ für $0 \le i < l$.
2. Addiere a mit dem periodisch verlängerten k' in $\mathbf{Z}/n\mathbf{Z}$, Ergebnis $b \in \Sigma^r$; also $b_j = a_j + k'_j \bmod l$.
3. Bilde $c = f_\sigma(b) \in \Sigma^r$; also $c_j = \sigma(b_j)$.

Das entsprechende Perl-Programm steht hier, das passende zur Entschlüsselung hier. Online kann man hier verschlüssseln und hier entschlüsseln.

Übungsaufgabe. Verschlüssele und entschlüssele einige Texte mit Hilfe des Web-Dienstes, u. a. auch den bisher manuell behandelten. Wie gibt man das Standard-Alphabet (für die BELASO-Chiffre) als ersten Schlüssel ein?

Autor: Klaus Pommerening, 13. November 1999; letzte Änderung: 4. November 2007.
E-Mail an `Pommerening »AT« imbei.uni-mainz.de`.