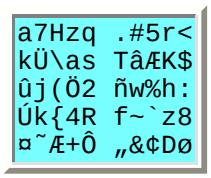
JOHANNES GUTENBERG UNIVERSITÄT MAINZ

Kryptologie

Mathematische Beschreibung der Zylinder-Chiffriergeräte



Parameter

- Zahl der Buchstaben des Alphabets = $n = \#\Sigma$.
- Zahl der Scheiben = q mit $1 \le q$;
  falls alle Scheiben *verschieden* sein sollen, ist $q \le (n\text{-}1)!$.
  [Die Erklärung, warum hier nicht etwa $n!$ steht, folgt unten.]
  - Jede Scheibe ist durch eine Permutation $\tau \in \mathbf{S}(\Sigma)$ gekennzeichnet.
  - Die Menge der Scheiben ist also als Familie (q-Tupel) $(T_1, ..., T_q) \in \mathbf{S}(\Sigma)^q$ beschreibbar.
- Zahl der ausgewählten Scheiben = l mit $1 \le l \le q$.
  - Ein Schlüssel ist also eine Folge $(\tau_0, ..., \tau_{l-1})$ aus verschiedenen Scheiben der Familie $(T_1, ..., T_q)$.
  - Es gibt dafür

    $$\#K = q \cdot (q\text{-}1) \cdots (q\text{-}l\text{+}1) = q!/(q\text{-}l)!$$

    Möglichkeiten (von denen einige identische sein können, falls es gleiche Scheiben gibt).

Beispiele

1. **JEFFERSON:** $l = q = 36$, $\#K = 36!$, effektive Schlüssellänge ≈ 138.
2. **BAZERIES:** $l = q = 20$, $\#K = 20!$, effektive Schlüssellänge ≈ 61.
3. **M-94:** $l = q = 25$, $\#K = 25!$, effektive Schlüssellänge ≈ 84.
4. **M-138-A:** $l = 30$, $q = 100$, $\#K = 100!/70!$, effektive Schlüssellänge ≈ 190.

Ver- und Entschlüsselung

Die Verschlüsselung ist polyalphabetisch mit der Periode l.

Achtung: Die Scheiben-beschreibende Permutation $\tau \in \mathbf{S}(\Sigma)$ darf nicht mit dem durch die Scheibe definierten Substitutionsalphabet $\sigma \in \mathbf{S}(\Sigma)$ verwechselt werden. Der Zusammenhang zwischen beiden wird gleich erklärt.

Ist das Standard-Alphabet Σ wie so oft mit $\mathbf{Z}/n\mathbf{Z}$ identifiziert, so sieht die Verschlüsselung eines Klartextblocks so aus (bei Verwendung der 1. Generatrix):

a_0	…	a_i	…	a_{l-1}
		$\tau_i(0)$		
		…		
Suche Eintrag x mit		$\tau_i(x) = a_i$		
		$\tau_i(x+1) = c_i$	zugehöriger Geheimtextbuchstabe	
		…		
		$\tau_i(n-1)$		

wobei die mittlere Spalte $\tau_i(0)$, …, $\tau_i(n-1)$ die Beschriftung der Scheibe Nummer i darstellt.

Also ist

$$c_i = \tau_i(x+1) = \tau_i(\tau_i^{-1} a_i + 1),$$

und die zugehörige Entschlüsselungsfunktion wird beschrieben durch

$$a_i = \tau_i(\tau_i^{-1} c_i - 1).$$

Diese Überlegungen werden zusammengefasst zu:

> **Satz** (von der Zylinder-Chiffrierung). *Der Zusammenhang zwischen der Permutation* $\tau \in \mathbf{S}(\Sigma)$, *die eine Scheibe beschreibt, und der Permutation* $\sigma \in \mathbf{S}(\Sigma)$, *die die zugehörige Substitution beschreibt, ist*
>
> $$\sigma(a) = \tau(\tau^{-1} a + 1).$$
>
> $$\sigma^{-1}(c) = \tau(\tau^{-1} c - 1).$$
>
> *Anders ausgedrückt:* σ *ist eine zyklische Permutation und* τ *ist die Zykeldarstellung von* σ.

Es gibt $(n-1)!$ verschiedene Zyklen der Länge n. Je n Scheibenbeschreibungen $\tau \in \mathbf{S}(\Sigma)$ liefern dieselbe zyklische Permutation $\sigma \in \mathbf{S}(\Sigma)$. Daher die Einschränkung $q \leq (n-1)!$ oben.

Beispiel: Sei $\Sigma = \{A,\ldots,Z\}$ und eine Scheibe beschrieben durch

τ = `QWERTZUIOPASDFGHJKLYXCVBNM`.

Dann ist σ die Permutation

```
a b c d e f g h i j k l m n o p q r s t u v w x y z
S N V F R G H J O K L Y Q M P A W T D Z I B E C X U
```

Autor: Klaus Pommerening, 3. Dezember 1999; letzte Änderung: 9. Juni 2002.

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