# 1 Running-Text Ciphers

## Method

Assume we have a plaintext of length $r$. We could encrypt it with the Bellaso cipher (and the Trithemius table). But instead of choosing a keyword and periodically repeating this keyword we use a keytext of the same length $r$ as the plaintext. Then we add plaintext and keytext letter for letter (using the table).

The abstract mathematical description uses a group structure on the alphabet $\Sigma$ with group operation $*$. For a plaintext $a \in M_r = M \cap \Sigma^r$ we choose a key $k \in \Sigma^r$ and calculate

$$c_i = a_i * k_i \quad \text{for } 0 \le i \le r-1.$$

We may interpret this as shift cipher on $\Sigma^r$. The formula for decryption is

$$a_i = c_i * k_i^{-1} \quad \text{for } 0 \le i \le r-1.$$

If the key itself is a meaningful text $k \in M_r$ in the plaintext language, say a section from a book, then we call this a **running-text cipher**.

## Example

Equip $\Sigma = \{\mathtt{A}, \ldots, \mathtt{Z}\}$ with the group structure as additive group of integers mod 26.

```
Plaintext:  i a r r i v e t o m o r r o w a t t e n o c l o c k
Keytext:    I F Y O U C A N K E E P Y O U R H E A D W H E N A L
            ---------------------------------------------------
Ciphertext: Q F P F C X E G Y Q S G P C Q R A X E Q K J P B C V
```

A Perl program is `runkey.pl` in the web directory `http://www.staff.uni-mainz.de/pommeren/Cryptology/Classic/Perl/`.

## Practical Background

To avoid a period in a polyalphabetic substitution we choose a key that is (at least) as long as the plaintext. On the other hand we need a key that is easily remembered or transferred to a communication partner.

A common method of defining such a key is taking a book and beginning at a certain position. The effective key is the number triple (page, line, letter). This kind of encryption is sometimes called a **book cipher**. Historically the first known reference for this method seems to be

> Arthur Hermann: *Nouveau système de correspondence secrète. Méthode pour chiffrer et déchiffrer les dépêches secrètes.* Paris 1892.

But note that there are also other ways to use a book for encryption, see `http://www.staff.uni-mainz.de/pommeren/Cryptology/Classic/1_Monoalph/Variants.html`.

A modern version could use the contents of a CD beginning with a certain position.

**Exercise:** How large is the keyspace of this cipher, when the attacker knows which CD was used?