6 Cryptological Applications

The unicity distance is a very coarse measure of the quality of a cipher. In modern cryptology it is almost never used. For an attack with known plaintext it is meaningless (except for perfect ciphers where it is ∞).

A large unicity distance is achieved by:

- a large key space,
- lowering the redundancy of the plaintext language, for example by compression.

Application 1: PORTA's disk cipher is not so much stronger than the TRITHEMIUS-BELLASO cipher because the unicity distance is greater only by the constant summand 27.6. For a longer period the complication by permuting the primary alphabet effects not much additional security.

Application 2: Another application of SHANNON's theory is to running text encryption. The cryptanalysis must derive two meaningful plaintexts of total length $2r$ from a ciphertext of length r. This can work only for a language of redundancy at least 50%.

More generally consider a q-fold running text encryption with q independent keytexts. If cryptanalysis is feasible, then meaningful plaintext of total length $(q + 1) \cdot r$ is excavated from a ciphertext of length r. We conclude that the redundancy of the language is at least $\geq \frac{q}{q+1}$. Because the redundancy of German, 70%, is smaller than $\frac{3}{4}$ we conclude that a triple running text encryption is secure. For English that has somewhat less redundancy even a double running text encryption seems to be secure.

Application 3: The unicity distance may serve as an indication for how much ciphertext corresponding to a single key may be known to the enemy without being of use. Or in other words: How often the key must change.

A general short summary of SHANNON's theory consists of the rule: *A necessary condition for the solvability of a cipher is that "information content of the ciphertext + redundancy of the plaintext language" $\geq$ "information content of the plaintext + information content of the key".*