3 Examples of Perfect Security

Trivial Examples

Example 0: $\#M_0 = 1$. This example is cryptological nonsense since the cryptanalyst knows the only possible plaintext a priori. Hence she cannot gain any additional information on the plaintext by knowing the ciphertext.

Let $M_0 = \{a\}$. For all $c \in C_0$ trivially $P(a|c) = 1 = P(a)$. Hence F is perfectly secure, no matter how it is defined.

Example 1: $\#M_0 = 2$. The smallest nontrivial example involves two possible plaintexts. Without restriction we may assume that $M_0 = \{0, 1\} = C_0 = K$. Let f_0 be the identity map on $\{0, 1\}$, and f_1, the transposition of 0 and 1. Furthermore let the two keys 0 and 1 have the same probability: $P(0) = P(1) = \frac{1}{2}$.

Then $K_{00} = K_{11} = \{0\}$, $K_{01} = K_{10} = \{1\}$. Theorem 2 tells us that F is perfectly secure.

The Shift Cipher

We provide $M_0 = K = C_0$ with a group structure, and let $F\colon M_0 \times K \longrightarrow C_0$ be the group composition, hence $f_k(a) = a * k$. The sets

$$K_{ac} = \{k \in K \mid a * k = c\} = \{a^{-1} * c\}$$

each consist of one element only. We let $P(k) = \frac{1}{\#K}$ for all keys $k \in K$. Then F is perfectly secure.

The Examples 0 and 1 are the special cases of the one- or two-element group. Also Examples 2 and 3 will be special cases.

Example 2: The CAESAR Cipher. This is the shift cipher on the cyclic group $\Sigma = \mathbb{Z}/n\mathbb{Z}$ of order n.

Hence the CAESAR cipher is perfecly secure, *if we encrypt messages of length 1 only and randomly choose an independent new key for each message.*

Example 3: The One-Time Pad. This is the collection of the shift ciphers on the groups $\Sigma^r = M_0$ where $\Sigma = \mathbb{Z}/n\mathbb{Z}$. Messages are texts of length r, and keys are *independently and randomly chosen* letter sequences of the same length r.

Because one has to choose a new key for each message this cipher has its name **One-Time Pad**. Imagine a tear-off calendar where each sheet contains a random letter. After use it is torn off and destroyed.

The One-Time Pad is the prototype of a perfect cipher.

The special case $\Sigma = \{0,1\}$ gives the binary VERNAM/MAUBORGNE cipher, that is the bitstram encryption with a completely random sequence of key bits.

Counterexample: The Monoalphabetic Substitution. Set $M_0 = \Sigma^r$ and $K = \mathcal{S}(\Sigma)$. For $r = 5$ we saw already that

$$P(\texttt{fruit}|\texttt{XTJJA}) = 0 < q = P(\texttt{fruit}).$$

Therefore the monoalphabetic substitution is not perfect (for $r \geq 2$ and $n \geq 2$). For $r = 1$ it is perfect by Theorem 2 (with $s = (n-1)!$).