SHANNON'S THEORY

Shannon's theory of Communication has been the cornerstone in laying the foundations for the design of secure ciphers. It consists of three important parameters:

1. Diffusion

2. Confusion

3. Unconditional Security

In the sequel we explain in more detail these three principles.

ITERATION OF CIPHERS (DIFFUSION)

An iteration of a fixed transformation may initially display convincingly good encryption qualities, but may fail in the end to be a good encryption. This we discuss in the sequel with an example.

Consider the unit square $S = \{(x, y) : 0 \leq x, y < 1\}$ with toroidal wrap-around and the transformation $T(x, y) = (y, x')$ such that

$$y' = \begin{cases} x + y - 1 & \text{if } x + y \geq 1 \\ x + y & \text{if } 0 \leq x + y < 1 \end{cases}$$

The affine distortion of the picture is given by the matrix

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

Notice that if f_n is n-th Fibonacci number then

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^n = \begin{pmatrix} f_{n-1} & f_n \\ f_n & f_{n+1} \end{pmatrix}$$

Observe that

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^4 = \begin{pmatrix} 2 & 3 \\ 3 & 5 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} + 3 \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^8 = \begin{pmatrix} 13 & 21 \\ 21 & 34 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + 3 \begin{pmatrix} 4 & 7 \\ 7 & 11 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^{16} = \begin{pmatrix} 610 & 987 \\ 987 & 1597 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + 21 \begin{pmatrix} 29 & 47 \\ 47 & 76 \end{pmatrix}$$

This gives fixed points for the transformation T, i.e., points (x, y) such that $T(x, y) = (x, y)$. E.g., the last equation implies

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^{16} \begin{pmatrix} i/21 \\ j/21 \end{pmatrix} = \begin{pmatrix} i/21 \\ j/21 \end{pmatrix} + \begin{pmatrix} 29i + 47j \\ 47i + 76k \end{pmatrix}$$

which gives 400 fixed points for the transformation T^{16}, with coordinates $(i/21, j/21)$, $0 < i, j < 21$. (Note that the toroidal property implies that both coordinates of the rightmost vector are 0.)