B.5 Basic Cryptographic Functions

Now the theoretic basis suffices for an exact definition of one-way functions and strong symmetric ciphers. Note that the "functions" or "maps" in these definitions are infinite families with growing input size. There is no mathematically sound definition of one-way or hash functions, or of strong symmetric ciphers, for a fixed input size, as we assumed in treating these concepts in a naive way in Section 4.1 and Chapters 5 and 6.

Definition 5 Let $f: L \longrightarrow \mathbb{F}_2^*$ be as in (2). A right inverse of f is a map $g\colon f(L) \longrightarrow L \subseteq \mathbb{F}_2^*$ with $f(g(y)) = y$ for all $y \in f(L)$. In other words g finds pre-images of f. We call f a **one-way function** if each right inverse of f is hard.

Adapting this definition the conjecture that the discrete exponential function in finite prime fields is hard makes sense.

Now for the definition of a strong cipher. An "ordinary" block cipher is a map

$$F\colon \mathbb{F}_2^r \times \mathbb{F}_2^q \longrightarrow \mathbb{F}_2^r.$$

The corresponding decryption function is a map

$$G\colon \mathbb{F}_2^r \times \mathbb{F}_2^q \longrightarrow \mathbb{F}_2^r$$

with $G(F(x,k),k) = x$ for all $x \in F_2^r$ and $k \in F_2^q$.

An attack with known plaintext finds a key $k \in F_2^q$ with $F(x,k) = y$, given $x, y \in \mathbb{F}_2^r$. We formalize this by a map

$$H\colon \mathbb{F}_2^r \times \mathbb{F}_2^r \longrightarrow \mathbb{F}_2^q$$

with $F(x, H(x,y)) = y$ for all $x, y \in \mathbb{F}_2^r$ with $y \in F(x, \mathbb{F}_2^q)$ ("possible pairs" (x,y)).

Exercise Give an exact definition of a possible pair.

A more general attack uses several, say s, plaintext blocks. So it defines a map

$$H\colon \mathbb{F}_2^{rs} \times \mathbb{F}_2^{rs} \longrightarrow \mathbb{F}_2^q$$

with $F(x_i, H(x_i, y_i)) = y_i$ for $i = 1, \dots s$ for all possible $x, y \in \mathbb{F}_2^{rs}$.

Now we give a definition in terms of complexity theory.

Definition 6 A **symmetric cipher** is a family $F = (F_n)_{n\in\mathbb{N}}$ of block ciphers

$$F_n\colon \mathbb{F}_2^{r(n)} \times \mathbb{F}_2^{q(n)} \longrightarrow \mathbb{F}_2^{r(n)}$$

with strictly monotonically increasing functions r and q, such that $F_n(\bullet, k)$ is bijective for each $k \in \mathbb{F}_2^{q(n)}$, and

- F is efficiently computable,
- there is an efficiently computable family $G = (G_n)_{n\in\mathbb{N}}$ of corresponding decryption functions.

Definition 7 An **known plaintext attack** on a symmetric cipher F is a family $H = (H_n)_{n\in\mathbb{N}}$ of maps

$$H_n \colon \mathbb{F}_2^{r(n)s(n)} \times \mathbb{F}_2^{r(n)s(n)} \longrightarrow \mathbb{F}_2^{q(n)}$$

with

$$F_n(x_i, H_n(x_i, y_i)) = y_i \quad \text{for } i = 1, \ldots, s(n)$$

for all possible pairs $x, y \in \mathbb{F}_2^{r(n)s(n)}$.

F is called a **strong symmetric cipher** if each known plaintext attack on F is hard.

Defining a hash function is even more tricky. We omit it.