1.1 Multiple Ciphers and Group Structures

Multiple Ciphers

Let $F = (f_k)_{k\in K}$ be a cipher over the alphabet Σ, where $f_k\colon \Sigma^* \longrightarrow \Sigma^*$ is the encryption function corresponding to the key $k \in K$. The set of all of encryption functions is denoted by

$$\tilde{F} = \{f_k \mid k \in K\} \subseteq \mathrm{Map}(\Sigma^*, \Sigma^*).$$

By forming the **double cipher**

$$F^{(2)} = (f_h \circ f_k)_{h,k\in K}$$

the key space is significantly enlarged from K to $K \times K$. In the same way we can construct the triple cipher $F^{(3)}$, ..., the n-fold cipher $F^{(n)}$. All this makes sense only when

(A) $\tilde{F}$ is not a semigroup.

If $\tilde{F}$ *is* a semigroup, then for each pair of keys $h, k \in K$ there exists a key $x \in K$ such that $f_h \circ f_k = f_x$, and we don't get any new encryption functions by this kind of composition—a typical case of an "illusory complication", the effective keysize didn't increase at all!

We observe an even better effect when

(B) $\tilde{F}$ generates a subsemigroup of $\mathrm{Map}(\Sigma^*, \Sigma^*)$ of large size.

And the best we can hope for is:

(C) The map $K \times K \longrightarrow \widetilde{F^{(2)}} \subseteq \mathrm{Map}(\Sigma^*, \Sigma^*)$ is injective.

For a finite key space K we can express this also in the form:

(C') $\#\widetilde{F^{(2)}} = \#\{f_h \circ f_k \mid h, k \in K\} = (\#K)^2$.

The Group Property of a Block Cipher

A block cipher is uniquely characterized by its effect on Σ^r for a given exponent r, the blocksize. (For the moment we don't care about continuing it to strings of arbitrary lengths or about "padding" shorter strings to full blocklength.)

A block cipher **preserves lengths** if it transforms Σ^r to itself. Then in a canonical way $\tilde{F}$ is a subset of the symmetric group $\mathcal{S}(\Sigma^r)$, hence finite, and without restriction we may assume that also the keyspace K is finite. For such block ciphers the semigroup property (the converse of (A) above) is equivalent with the group property. This follows from the well-known simple lemma:

Lemma 1 *Let G be a finite group, $H \leq G$ a subsemigroup, that is $H \neq \emptyset$ and $HH \subseteq H$. Then H is a group, in particular $\mathbf{1} \in H$.*

Proof. Each $g \in G$ has finite order, $g^m = \mathbf{1}$ for some m. If $g \in H$, then $\mathbf{1} = g^m \in H$, and $g^{-1} = g^{m-1} \in H$. $\diamond$

This proves:

Proposition 1 *Let F be a length preserving block cipher over a finite alphabet. Then the following statements are equivalent:*

(i) *For any two keys $h, k \in K$ there exists an $x \in K$ such that $f_h \circ f_k = f_x$.*

(ii) *The set $\tilde{F}$ of encryption functions is a group.*

Remark

The probability that two random elements of the symmetric group $\mathcal{S}_n$ generate the whole group $\mathcal{S}_n$ or at least the alternating group $\mathcal{A}_n$ is

$$> 1 - \frac{2}{(\ln \ln n)^2} \quad \text{for large } n.$$

Source: John Dixon, *The probability of generating the symmetric group.* Mathematische Zeitschrift 110 (1969), 199–205.

For $n = 2^{64}$, a typical size for a block cipher, this lower bound is $\approx$ 0.86. With high probability it should generate the full or at least the “half” permutation group on the blocks. The concrete proof however might be difficult. One would try to determine the order of some concrete encryption functions by their effect on certain concrete messages, and then take the lowest common multiple as a lower bound for the group order.

In any case it seems that in general a multiple cipher is stronger than the underlying simple cipher. We’ll discuss this again in Sections 1.3 and 1.4.