1 Mathematical Model of Cryptography

We want to give a formal definition of the following two concepts:

- *An encryption function transforms arbitrary character strings into other character strings.* (Where the strings are from a given alphabet.)
- *A cipher is a parametrized family of encryption functions. The parameter is called the key.* It determines the choice of a function from the family.

The purpose of this construct is that nobody can invert the encryption function except people who know the key. That is, an encrypted message (or a text, a file ...) is kept secret from third parties. These can see that there is a message, but they cannot read the contents of the message because they don't have the key and therefore don't know which of the functions from the family to invert.

Alphabets and Texts

Let Σ be a finite set, and call it **alphabet**. Call its elements **letters** (or **symbols**, or **characters**).

Examples. Here are some alphabets of cryptographic relevance:

- {A, B, ..., Z}, the standard 26 letter alphabet of classical cryptography.
- The 95 character alphabet of printable ASCII characters from "blank" to "tilde", including punctuation marks, numbers, lowercase, and uppercase letters.
- $\{0,1\} = \mathbb{F}_2$, the alphabet of bits, or the field of two elements. The earliest appearence (after Bauer[1]) is Bacon 1605.
- $\mathbb{F}_2^5$, the alphabet used for telegraphy code since Baudot (1874). It has 32 different symbols and also goes back to Bacon (after Bauer[1]).
- $\mathbb{F}_2^8$, the alphabet of bytes (correctly: octets, because in early computers bytes did not necessarily consist of exactly 8 bits). The earliest appearance seems to be at IBM around 1964.
- More generally $\mathbb{F}_2^l$, the alphabet of l-bit blocks. Often $l = 64$ (for example in DES or IDEA), or $l = 128$ (for example in AES). See Part II (on bitblock ciphers).

Often the alphabet Σ is equipped with a group structure, for example:

- $\mathcal{Z}_n$, the cyclic group of order $n = \#\Sigma$. Often we interpret the calculations in this group as arithmetic $\bmod n$, as in elementary number theory, and denote $\mathcal{Z}_n$ by $\mathbb{Z}/n\mathbb{Z}$, the residue class ring of integers $\bmod n$.

- $\mathbb{F}_2$ with the field addition $+$, as BOOLEan operator often denoted by XOR or $\oplus$. (Algebraists like to reserve the symbol $\oplus$ for direct sums. For this reason we'll rarely use it in the BOOLEan context.)

- $\mathbb{F}_2^l$ as l-dimensional vector space over $\mathbb{F}_2$ with vector addition, denoted by $+$, XOR, or $\oplus$.

For an alphabet Σ we denote by Σ^* the set of all finite sequences from Σ. These sequences are called **texts** (over Σ). A subset $M \subseteq \Sigma^*$ is called a **language** or **plaintext space**, and the texts in M are called meaningful texts or **plaintexts**.

Note that the extreme case $M = \Sigma^*$ is not excluded.

Ciphers

Let K be a set (finite or infinite), and call its elements **keys**.

Definition (i) An **encryption function** over Σ is an injective map $f : \Sigma^* \longrightarrow \Sigma^*$.

(ii) A **cipher** (also called encryption system or cryptosystem) over Σ with key space K is a family $F = (f_k)_{k \in K}$ of encryption functions over Σ.

(iii) Let F be a cipher over Σ, and $\tilde{F} = \{f_k | k \in K\} \subseteq \operatorname{Map}(\Sigma^*, \Sigma^*)$ be the corresponding set of different encryption functions. Then $\log_2(\#K)$ is called the **key length**, and $d(F) = \log_2(\#\tilde{F})$, the **effective key length** of the cipher F.

Remarks

1. This is not the most general definition of an encryption function. One could also consider non-injective functions, or even relations that are not functions, or are not defined on all of Σ^*.

2. Strictly speaking, the encryption functions need to be defined only on the plaintext space M, however we almost always consider encryption functions that are defined on all of Σ^*.

3. The encryption functions f_k, $k \in K$, need not be pairwise different. Therefore in general $\#\tilde{F} \leq \#K$, and effective key length $\leq$ key length. If K is infinite, then $\tilde{F}$ can be finite or infinite. In general the key length

is easier to determine than the effective key length, however it is less useful.

4. The elements in the ranges $f_k(M)$ depend on the key k. They are called **ciphertexts**.

5. Note that the identification of the alphabet Σ with the integers $\bmod n$, $\mathbb{Z}/n\mathbb{Z}$, also defines a linear order on Σ. We often implicitely use this order. In some cases for clarity we must make it explicit.