CONVENTIONAL ENCRYPTION TECHNIQUES: SOME MATHEMATICS

MATH 195

Some Notation

Consider the set up given in Figure 2.2 (p. 23) in the course text. We will use the following notation. Let $\mathcal{P}$ be the set from which the plaintext message is taken (e.g., the letters $\{A, \ldots, Z\}$). Let $\mathcal{C}$ be the set from which the ciphertext is taken—sometimes we will have $\mathcal{P} = \mathcal{C}$, as we shall see in the examples below, but this restriction is not necessary. Let $\mathcal{K}$ be the set of all possible keys.

Mathematically, encryption is a function (or map)

$$\begin{aligned} E : \mathcal{K} \times \mathcal{P} &\to \mathcal{C} \\ (K, X) &\mapsto E_K(X) \end{aligned}$$

The set on the right is the *Cartesian product* of the sets $\mathcal{K}$ and $\mathcal{P}$; an element of the product consists of an ordered pair of elements, one from each of the sets. Thus E eats a key K and plaintext X and spits out ciphertext $E_K(X)$.

Likewise, decryption is a map

$$\begin{aligned} D : \mathcal{K} \times \mathcal{C} &\to \mathcal{P} \\ (K, Y) &\mapsto D_K(Y) \end{aligned}$$

Now D eats a key and ciphertext and spits out plaintext.

In order for these functions E and D to make any sense, we would like decryption to return the correct plaintext. Therefore we insist that the functions D and E satisfy the following axiom:

Axiom. $\forall X \in \mathcal{P}$, $\forall K \in \mathcal{K}$, $D_K(E_K(X)) = X$. Equivalently, $\forall K \in \mathcal{K}$, $D_K \circ E_K = \mathrm{id}_{\mathcal{P}}$. □

In words, this says that for all $X \in \mathcal{P}$ and for all $K \in \mathcal{K}$, we have $D_K(E_K(X)) = X$. This says nothing than encrypting and decrypting in succession gives us the original plaintext back. The second statement says that the composition of the two maps

$$\mathcal{P} \xrightarrow{E_K} \mathcal{C} \xrightarrow{D_K} \mathcal{P}$$

is the identity map, which is exactly the statement that decrpytion undoes the encryption.

This is some of the material covered on Thursday, January 24, in Math 195: Cryptography, taught by Hendrik Lenstra, prepared by John Voight `jvoight@math.berkeley.edu`.

Caesar Cipher

The Caesar Cipher is explained in §2.3, p. 29. Here, we take $\mathcal{P} = \{\mathrm{A}, \mathrm{B}, \dots, \mathrm{Z}\}$, $\mathcal{C} = \mathcal{P}$, and $\mathcal{K} = \{0, 1, \dots, 25\}$. The encryption function we write as

$$E_K(\alpha) = \alpha + K,$$

where we think of this arithmetic modulo 26, which we write by giving $\mathcal{K}$ the ring structure $\mathcal{K} = \mathbb{Z}/26\mathbb{Z}$. For a review of modular arithmetic, you might consult §7.2 of the text. For now, it is enough to know that addition and multiplication are performed exactly the same, but we care only what remainder is left over after dividing by 26. For example,

$$17 + 18 = 35 = 26 + 9 \equiv 9 \pmod{26}$$

and

$$17 \cdot 18 = -9 \cdot -8 = 72 \equiv 20 \pmod{26}.$$

Note that in order to satisfy the axiom (that decryption is inverse to encryption), we must have $D_K = \alpha - K$, which we can also write $D_K = E_{-K}$.

Monoalphabetic Cipher

The monoalphabetic cipher is explained in §2.3, p. 31. Here, again $\mathcal{P} = \{\mathrm{A}, \mathrm{B}, \dots, \mathrm{Z}\}$ and

$$\mathcal{K} = \operatorname{Sym} \mathcal{P} = \{\sigma : \mathcal{P} \to \mathcal{P}, \sigma \text{ bijective}\}.$$

Recall: a map $f : S \to T$ is *injective* (or *one-to-one*, we write $f : S \hookrightarrow T$) if

$$\forall t \in T, \#\{s \in S : f(s) = t\} \leq 1.$$

This says that the number of preimages of every element $t \in T$ is at most one. The map f is *surjective* (or *onto*, we write $f : S \twoheadrightarrow T$) if

$$\forall t \in T, \#\{s \in S : f(s) = t\} \geq 1.$$

This means that every element of T has at least one preimage. If f is both injective and surjective, then we say that f is *bijective*. For example, the map $f : \mathbb{R} \to \mathbb{R}$ by $x \mapsto x^2$ is neither injective nor surjective; it is surjective, though, if we restrict the image set to the nonnegative real numbers.

If S and T are finite (and have the same number of elements), then a map $f : S \to T$ is injective if and only if it is surjective if and only if it is bijective. A map $f : S \to T$ is bijective if and only if there is a map $f^{-1} : T \to S$ such that $f \circ f^{-1} = \mathrm{id}_T$, $f^{-1} \circ f = \mathrm{id}_S$. In this case, $f^{-1}(t)$ is the unique $s \in S$ such that $f(s) = t$.

Therefore, $\mathcal{K}$ consists of all bijections from the finite set $\mathcal{P}$ to itself; this is a set with 26! elements, since there are 26 possibilities for the image of A, 25 for B, and so on. How large is this number? Well,

$$26! = 403291461126605635584000000 \approx 4 \times 10^{26}.$$

We can also approximate this number using *Stirling's formula*, which states that

$$n! \sim \frac{n^n}{e^n}\sqrt{2\pi n}$$

where this statement says that

$$\lim_{n \to \infty} \frac{n!}{(n^n/e^n)\sqrt{2\pi n}} = 1.$$

Returning to our cipher, we see that $E_\sigma(\alpha) = \sigma(\alpha)$, and hence $D_\sigma(\alpha) = \sigma^{-1}(\alpha)$, where σ^{-1} is the inverse map constructed above. Therefore $D_\sigma = E_{\sigma^{-1}}$.

[If you need to review the material on functions and sets, it is ordinarily covered in the Discrete Mathematics course (Math 55) at Berkeley. The text for the course this semester is Kenneth Rosen, *Discrete Mathematics and Its Applications*, and this material is treated in §1.6. Of course, any such a text will do, such as one for an introduction to higher mathematics course or the text for Abstract Algebra (Math 113), e.g. Fraleigh, *A First Course in Abstract Algebra*, covered in Chapter A. You might want to keep such a text handy throughout the semester.]