3. War, finance and arithmetic

Cryptography is the practice and study of techniques for sending a message from a *sender* to a *receiver* across a *public communications channel* in such a way that if the message is intercepted by a third party as it passes through the channel then that third party will not be able to read the message in any meaningful way. For centuries the subject was mainly of interest as a military tool. However, its application domain has now broadened to include e-commerce and e-finance.

A classic example is the Enigma machine, which was the mainstream German cipher machine before and during the second world war. A military version is shown in Figure 3.1. An improved

Figure 3.1: Military Enigma machine, model "Enigma I", photographed in the Museo della Scienza e della Tecnologia "Leonardo da Vinci"by Alessandro Nassiri. CC BY-SA 4.0 International

naval version was issued to U-boats. Messages could be typed into the machine at Naval Headquarters in order to produce a scrambled version for transmission to U-boats. The U-boats also carried Enigma machines which they used to unsscramble the messages. The machines could also be used to send messages from boats to Headquarters. The scrambled messages were routinely intercepted by Allied Forces who had difficulty unscrambling them. The Enigma machine had rotors (the machine of Figure 3.1 has three rotors but the improved naval version had four rotors) which could be initialized in many different positions. The initial position of the rotors influenced the scrambling. The initial rotor settings were varied on a regular basis known to both Headqurters and U-boats. This meant that if the Allies succeeded in unscambling messages on a certain day by 'breaking the code', they'd need to break the code again as soon as the initial rotor settings changed.

3.1 Basic assumptions

A sketch of the fundamental idea of cryptography is shown in Figure 3.2. We make the following assumptions.

1. Enciphering and deciphering machines are public knowledge.
2. The enciphering machine requires an *enciphering key* known only to the sender, and the deciphering machine (which is usually the same as the enciphering machine) needs a *deciphering key* known only to the receiver.
3. Enciphered messages will be intercepted.

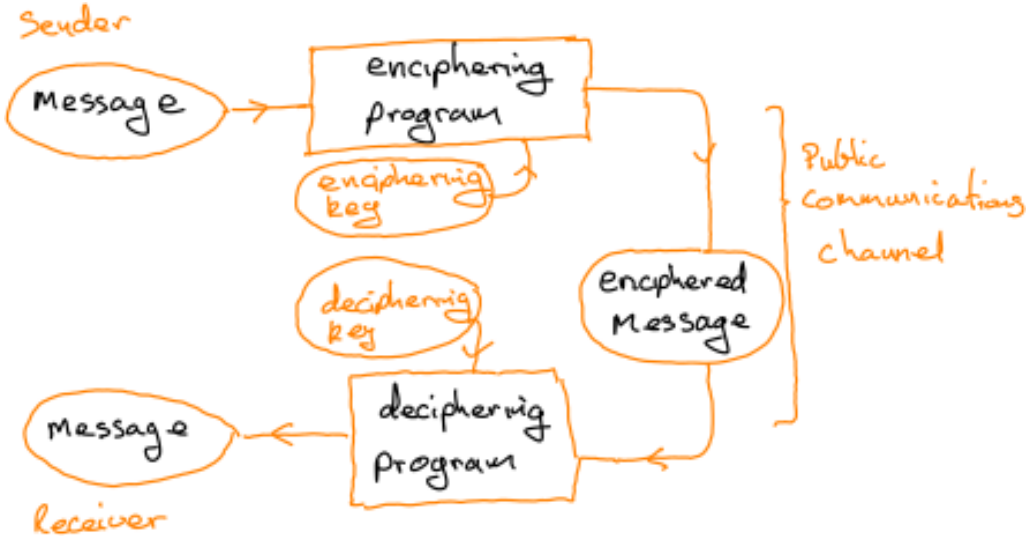

Figure 3.2: Overview of cryptography

In the case of the naval Enigma machine, assumption (1) was met in 1941 when British destroyers captured a German submarine, U-110, south of Iceland. Assumption (2) was met by the list of initial rotor positions to be used on given dates. Assumption (3) was met through the interception of German radio messeages by Allied radio operators.

There are more modern examples of cryptography. Every day, encryption is used to protect the content of web transactions, email, newsgroups, chat, web conferencing, and telephone calls as they are sent over the Internet. More will be said about the mathematics underlying this.

3.2 A first mathematical example

Suppose that a sender wants to send a secret message via email to a friend, knowing that emails are easily intercepted at various points in their journey. To keep things simple, we suppose that the

message is sent using an alphabet of just 26 letters A, B, C, ..., Z, all upper case and no spaces or punctuation allowed. The message to be sent, which we refer to as the *plaintext*, is in this example the single word:

HELLO

It is convenient to index the letters by integers.

$$A \leftrightarrow 1, B \leftrightarrow 2, C \leftrightarrow 3, \ldots, Z \leftrightarrow 26$$

It is even more convenient to calculate with these integers module 26. Since

$$26 \equiv 0 \mod 26 \tag{3.1}$$

we get the correspondence $Z \leftrightarrow 0$. To denote the collection of 26 numbers on a 26-hour clock we use the symbols $\mathbb{Z}_{26}$, and refer to $\mathbb{Z}_{26}$ as the *integers modulo 26*.

For illustrative purposes we use a very simple *enciphering function* and *enciphering key*. Caveat: its simplicity means that it is extremely easy to 'break the code', and so this method should never be used in practice. We use the enciphering function

$$f_E \colon \mathbb{Z}_{26} \to \mathbb{Z}_{26}, n \mapsto an + b \tag{3.2}$$

with encipering key a suitable pair of integers $E = (a,b)$. For instance , using $E = (3,4)$ the enciphering function becomes $f(n) = 3n+4 \mod 26$ and our plaintext is enciphered as follows.

$$H \;\; E \;\; L \;\; L \;\; O \tag{3.3}$$
$$\leftrightarrow 8 \;\; 5 \;\; 12 \;\; 12 \;\; 15 \tag{3.4}$$
$$\to f_E(8) \;\; f_E(5) \;\; f_E(12) \;\; f_E(12) \;\; f_E(15) \tag{3.5}$$
$$\to 2 \;\; 19 \;\; 14 \;\; 14 \;\; 23 \tag{3.6}$$
$$\leftrightarrow B \;\; S \;\; N \;\; N \;\; W \tag{3.7}$$

The *ciphertext*

BSNNW

is then emailed to the friend. To decipher the message the friend uses the deciphering function

$$f_D \colon \mathbb{Z}_{26} \to \mathbb{Z}_{26}, n \mapsto \alpha n + \beta \tag{3.8}$$

with an appropriate deciphering key $D = (\alpha, \beta)$. The deciphering function and key should yield the original plaintext message. So we need the equation

$$f_D(f_E(n)) \equiv n \mod 26 \tag{3.9}$$

to hold. In other words, we want:

$$f_D(an+b) = \alpha(an+b) + \beta \tag{3.10}$$
$$= \alpha(an) + (\alpha b + \beta) \tag{3.11}$$
$$\equiv n \mod 26 \tag{3.12}$$

Thus:

$$\alpha \equiv a^{-1} \mod 16 \tag{3.13}$$
$$\beta \equiv -\alpha b \mod 26 \tag{3.14}$$

For $E = (3,4)$ the formulae (3.13) and (3.14) give $D = (9,16)$. It is a worthwhile exercise to check that the deciphering function f_D applied with this key to the cipertext BSNNW yields the plaintext HELLO .