The two most important methods used to code a message are the transposition and the replacing methods. In the first method the letters of the original message remain intact and the order in which they appear is what changes. But in the replacing method the letters are replaced by numbers, letters or signs, while keeping the original order of the letters. This method is also known as codification. Both methods can be used in the same coding system, one or several times, in order to make it more difficult to decipher them.

In this unit we are going to learn how to use a simple method of transposition known as the "boxes method" that was used until the end of the Second World War by the Intelligence Services of different countries.

As in any other encryption system, both persons, the one sending the message and the one getting it, must know the "key".

In this method the key is a word. We are going to describe how it works using a practical example.

The first thing that we must do is to create a table and write the keyword in the first row.

Let's suppose that the secret key is "sangakoo" and that the message that we want to send is

NEXT MONDAY THERE IS A MATH EXAM

The first thing that we must do is create a table and write in the first row the keyword:

S	A	N	G	A	K	O	O

The next step is to number the letters in the order in which they appear in the alphabet

S	A	N	G	A	K	O	O
8	1	5	3	2	4	6	7

If the letter is repeated we write consecutive numbers for each one. For example, A is the first letter in alphabetical order, but as there are two A in the word SANGAKOO, we write below the first one the number 1 and number 2 below the second one. The following letter that appears in the alphabet is G (so it gets a 3), then the K and so on.

After that we write the message that we want to send, starting in the third line and without spaces.

S	A	N	G	A	K	O	O
8	1	5	3	2	4	6	7
N	E	X	T	M	O	N	D
A	Y	T	H	E	R	E	I
S	A	M	A	T	H	E	X
A	M						

Once the box is completed, the message that we are going to send is written by columns and in the order in which these are numbered: column 1 would be eyam, the following column would be met, and we keep on filling out all columns in this way. The finished coded text would be so:

eyam met tha orh xtm nee dix nasa

Let's see an example of deciphering.

Let's suppose that the message that we receive is

UORE FTWT OYA OGUL YROL

and the key word is SPACE

To decipher the first message we place the key word in the first line of the table:

S	P	A	C	E

After that we number the columns:

S	P	A	C	E
5	4	1	2	3

Then we write the groups of words following the order of the columns:

S	P	A	C	E
5	4	1	2	3
Y	O	U	F	O
R	G	O	T	Y
O	U	R	W	A
L	L	E	T	

Finally we read what it says on the lines:

YOU FORGOT YOUR WALLET

And we already have the deciphered message.