MysteryTwister C3
THE CRYPTO CHALLENGE CONTEST

Spanish Strip Cipher – Part 3

Author: Luis Alberto Benthin Sanguino

February 2014

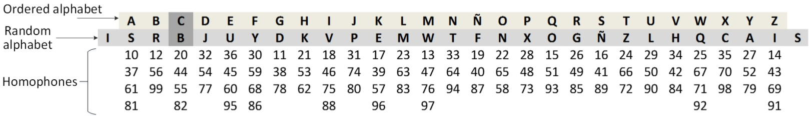
Introduction

The Spanish Strip Cipher (SSC) is a homophonic substitution cipher, in which a plaintext letter not only maps to one ciphertext character (as in monoalphabetic substitution ciphers), but it can map to different ones. In this kind of ciphers, the ciphertext characters are called homophones, which are arranged in a table, where each column is mapped by one letter of the plaintext alphabet. During the Spanish civil war (1936-1939) this method was widely adopted by both sides, Republicans and Nationalists.

Normally, the number of homophones in a column is related with the frequency of a plaintext letter. For example, in a Spanish text, the letter E occurs with a frequency of 13.68% approximately. On the other hand, the letter N approximately occurs with a frequency of 6.71%. Thus, the column assigned to the letter E should contain more homophones than the column assigned to the letter N. In this way, frequency analysis attacks become more difficult.
Contradictorily, in the original variant of SSC a column contains 3 or 4 homophones, regardless of the letters frequency.

In addition to the homophones table, the SSC encompasses three more elements (see Figure 1): A random alphabet, a keyword, which is used to generate the random alphabet, and an initial position that is used to shift the random alphabet.

Keyword: cryptool
Initial position: B in C



Ordered alphabet		A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	
Random alphabet	I	S	R	B	J	U	Y	D	K	V	P	E	M	W	T	F	N	X	O	G	Ñ	Z	L	H	Q	C	A	I	S
Homophones		10	12	20	32	36	30	11	21	18	31	17	23	13	33	19	22	28	15	26	16	24	29	34	25	35	27	14	
		37	56	44	54	45	59	38	53	46	74	39	63	47	64	40	65	48	51	49	41	66	50	42	67	70	52	43	
		61	99	55	77	60	68	78	62	75	80	57	83	76	94	87	58	73	93	85	89	72	90	84	71	98	79	69	
		81		82		95	86			88		96		97											92			91	

Encryption

In order to encrypt a plaintext, sender and receiver agree on a key which consists of three elements: a keyword, a homophones table, and an initial position. After generating and shifting the random alphabet, the encryption can begin. For each plaintext letter:

1. We look for the same letter in the random alphabet.
2. We substitute the plaintext letter by one the homophones of the same column of the random-alphabet letter.

For instance, the plaintext letter A can be replaced by the homophones 27, 52 and 79. The selection of one of these homophones can be performed either sequentially or randomly.

Encryption – Example

A plaintext is encrypted using the key from Figure 1.

Plaintext	U	N	I	V	E	R	S	I	D	A	D
Ciphertext	36	22	14	18	17	12	10	43	11	27	38

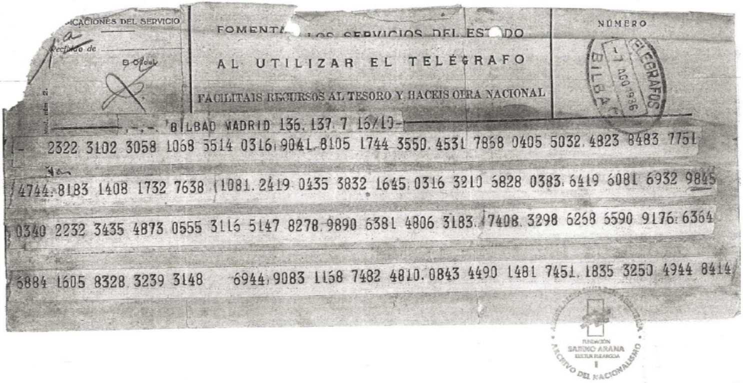
Decryption

The decryption is a straightforward process, in which each ciphertext homophone is replaced by its corresponding letter of the random alphabet.

Example: A ciphertext is decrypted using the key shown in Figure 1.

Ciphertext	10	17	35	12	39	33
Plaintext	S	E	C	R	E	T

Challenge



ICACIONES DEL SERVICIO

Recibido de

El Oficial

Mod. núm. 2.

FOMENTA LOS SERVICIOS DEL EST DO

AL UTILIZAR EL TELÉGRAFO

FACILITAIS RECURSOS AL TESORO Y HACEIS OBRA NACIONAL

NÚMERO

TELÉGRAFOS 7 AGO 1936 BILBAO

BILBAO MADRID 136. 137 7 16/10-

2322 3102 3058 1068 5514 0316 9041.8105 1744 3550.4531 7868 0405 5032.4823 8483 7751

4744.8183 1408 1732 7638 1081.2419 0435 3832 1645.0316 3210 6828 0383.6419 6081 6932 9845

0340 2232 3435 4873 0555 3116 5147 8278.9890 6381 4806 3183.7408.3298 6268 6590 9176.6364

6884 1605 8328.3239 3148 6944.9083 1158 7482 4810.0843 4490 1481 7451.1835 3250 4944 8414

FUNDACIÓN SABINO ARANA KULTUR ELKARGOA

ARCHIVO DEL NACIONALISMO

Please find the corresponding plaintext!

Challenge – Transcript

```
23 22 31 02 30 58 10 68 55 14 03 16 90 41 81 05 17 44 35 50 45
31 78 68 04 05 50 32 48 23 84 83 77 51 47 44 81 83 14 08 17 32
76 38 10 81 24 19 04 35 38 32 16 45 03 16 32 10 68 28 03 83 64
19 60 81 69 32 98 45 03 40 22 32 34 35 48 73 05 55 31 16 51 47
82 78 98 90 63 81 48 06 31 83 74 08 32 98 62 68 65 90 91 76 63
64 68 84 16 05 83 28 32 39 31 48 69 44 90 83 11 68 74 82 48 10
08 43 44 90 14 81 74 51 18 35 32 50 49 44 84 14
```

Hints

1. This telegram was sent during the Spanish civil war (Summer/ Fall 1936). It is most likely to be a Spanish text. However, it can also be a text written in Basque.
2. It is likely that this telegram was encrypted with the SSC. Nonetheless, some variants should be considered:
   - The columns may content between 3 and 5 homophones.
   - The ordered alphabet can include the digraphs "LL" and "CH", or also can exclude the letter "W".