MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

Spanish Strip Cipher – Part 2

Author: Luis Alberto Benthin Sanguino

March 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

Decrypt the ciphertext on the next slide and use the plaintext in capital letters and without any blanks as your solution.

Challenge – Ciphertext

14 05 28 63 15 40 82 71 92 23 71 42 85 87 57 30 42 77 45 83 07
14 43 59 67 83 99 97 51 28 92 93 91 60 45 05 55 39 36 21 04 66
74 72 88 78 28 67 06 87 28 30 45 64 28 36 07 74 95 19 06 99 42
75 55 67 97 06 44 93 96 83 57 51 55 71 45 91 83 77 45 71 16 62
42 77 05 42 06 46 57 34 39 36 19 71 63 15 57 49 95 49 15 11 93
11 36 25 14 88 07 22 64 05 28 07 74 45 05 83 65 15 50 33 42 92
28 41 36 67 68 42 63 39 88 41 16 28 49 77 15 30 75 68 61 74 60
43 47 47 74 85 95 15 63 39 74 39 98 97 62 14 03 74 34 62 97 07
83 31 98 83 99 14 48 91 98 14 88 95 71 20 62 68 05 55 15 28 85
88 92 15 98 14 42 25 15 17 28 63 72 97 92 55 83 85 42 63 62 36
87 97 71 50 91 50 74 67 07 91 99 74 85 78 57 95 74 71 06 75 55
53 27 20 15 42 63 57 92 13 96 42 41 14 33 57 99 42 51 55 71 72
42 78 55 92 93 96 55 80 88 63 23 97 93 97 91 92 21 20 55 93 98
99 12 30 43 38 14 33 28 12 42 63 10 19 11 87 71 93 28 07 42 15
17 77 93 61 71 93 64 42 17 62 39 74 28 41 59 62 91 22 83 23 97
63 46 43 93 05 87 91 23 74 20 21

Hints

1. The homophones were selected randomly during the encryption.
2. The homophones table contains 99 numbers in the range of 01-99 that have been randomly entered in the table.
3. Each column of the table contains 3 or 4 homophones.
4. The ordered alphabet is the same as that shown in Figure 1.
5. The plaintext is an English telegram sent during the Spanish civil war.
6. The plaintext does not contain the letter “ñ”.