MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

Spanish Strip Cipher – Part 1

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

84 19 24 39 53 40 21 01 81 90 46 30 91 57 80 27 63 04 55 60 66
08 23 96 35 17 39 76 43 50 44 84 48 14 41 40 66 81 42 98 51 30
29 15 90 35 97 02 27 33 14 21 43 85 04 24 57 53 08 80 69 98 65
30 55 68 84 27 47 66 35 17 01 04 99 45 43 13 84 91 66 50 26 39
19 74 08 90 03 42 30 92 27 41 60 40 32 04 08 58 57 14 53 35 29
43 80 28 07 84 97 66 89 98 50 21 44 96 71 55 81 39 30 99 40 35
42 43 65 27 78 04 91 08 02 90 30 46 84 60 57 15 27 53 14 33 04
96 01 55 80 26 98 24 74 66 81 17 64 35 45 82 90 93 20 43 91 60
18 84 54 14 19 66 65 45 08 46 35 30 19 39 50 94 43 42 40 84 96
98 27 66 81 90 53 04 03 44 57 13 14

Hints

1. The homophones were selected sequentially 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 a Spanish telegram sent during the Spanish civil war.
6. The plaintext does not contain the letter “ñ”.