MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

Hill Cipher with Sudoku key

Author: Emmanouil Doulgerakis

August 2013

Returning home you find on your brother's desk a note saying "I will be at the library until noon". Next to the note you can also see an unsolved Sudoku puzzle and a piece of paper full of strange characters.

					6		5	
	8		2			3		
3	2	6		8			4	
7	6	2	8					
					1	6	7	8
	9			6		4	1	3
		1			8		6	
	3		9					

Author: Emmanouil Doulgerakis

You are curious to find out the topic that your brother is searching about so you decide to decrypt the page with the strange characters. You know that your brother likes to use the Hill cipher so you decide that this is probably the solution to the problem. But what about the key?

And then you come up with an idea: Your brother has probably hidden the key in the Sudoku. Can you solve it?
Find the key and decrypt the message as to find out the topic that your brother is searching for.

The solution to the challenge is the second and the third word of the plaintext in capital letters and with a space separating them. You will find the ciphertext in the additional file hill.txt. The example of the hill cipher on the following slides will help you with this challenge.

Example – Encryption

We map the English alphabet A,B,C,...,Z to the numbers 0,1,2,...,25 and we set a matrix A:

$$\begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix}$$

All of the following calculations are done modulo 26.

Let's assume that we want to encrypt the message "BEEN". The numerical value is (1,4,4,13) which is split into two groups of two letters since the dimension of the matrix is 2x2. Then we multiply the matrix A by each group separately and receive two new blocks of two numbers that form the ciphertext.

Example – Encryption

For the first group in the example we calculate

$$\begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix} \times \begin{pmatrix} 1 \\ 4 \end{pmatrix} = \begin{pmatrix} 14 \\ 13 \end{pmatrix}$$

and for the second one:

$$\begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix} \times \begin{pmatrix} 4 \\ 13 \end{pmatrix} = \begin{pmatrix} 21 \\ 2 \end{pmatrix}$$

That means that from the first group we get the ciphertext (14,13) = ON and from the second one (21,2) = VC, thus the ciphertext is "ONVC".

Example – Decryption

In order to decrypt the message the procedure is inverted. At first, we calculate the inverse matrix B of A:

$$\begin{pmatrix} 14 & 11 \\ 17 & 10 \end{pmatrix}$$

Now we accomplish the following multiplications:

$$\begin{pmatrix} 14 & 11 \\ 17 & 10 \end{pmatrix} \times \begin{pmatrix} 14 \\ 13 \end{pmatrix} = \begin{pmatrix} 1 \\ 4 \end{pmatrix}$$

$$\begin{pmatrix} 14 & 11 \\ 17 & 10 \end{pmatrix} \times \begin{pmatrix} 21 \\ 2 \end{pmatrix} = \begin{pmatrix} 4 \\ 13 \end{pmatrix}$$

Finally, we get the blocks (1,4) = BE and (4,13) = EN that means that the plaintext is “BEEN“ – as we have already expected.

Hint 1/2

It might be helpful to use CrypTool 1.4.30 for the decrypting procedure as the used alphabet has 92 characters:
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstu
vwxyz 0123456789.,:;!?()-+*/[]{}@_><#˜=\"&%$§
Since copying special characters from PDFs can lead to incorrect symbols, you can also copy the alphabet from the additional file mtc3-doulgerakis-01-alphabet.txt.

Set the text options to the following:
Distinguish between uppercase and lowercase; alphabet order: uppercase letters, lowercase letters, space, numerals, special characters; and set the first character value to 0.

ATTENTION: The settings must be modified in the exact order mentioned above otherwise the parts of the alphabet will be permuted.

Hint 2/2

The length of the given ciphertext fits to the size of the sought-after key matrix. The plaintext was encrypted without padding.