MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

Handycipher made in love – Part 1

Author: George Theofanidis

January 2019

Introduction (1/6)

Main characters involved – Plot:

- Bob
- Alice, who ist secretly in love with Bob
- Eve, who is jealous about this flirt and eavesdrops on their communication
- Bob and Alice intend to meet and Eve wants to be there, too, in order to spy on them.

Introduction (2/6)

What happens?

- Bob and Alice want to communicate in a more secure way and therefore use the Handycipher algorithm, described in the Handycipher challenges, Parts 1-3.
- Alice takes a Wikipedia article and adds somewhere an irrelevant sentence that describes date, time, and place of their rendezvous (see example on page 4).
- Using Handycipher, she generates a random key and uses it to encrypt the plaintext. The corresponding ciphertext can be found in the file "ciphertext.txt" in the additional zip archive. Being in love, she makes a crucial mistake that will be explained on the following paragraphs of the Introduction.

Introduction (3/6)

Example:

Wikipedia article: METEOROLOGY IS A BRANCH OF THE ATMOSPHERIC SCIENCES WHICH INCLUDES ATMOSPHERIC CHEMISTRY AND ATMOSPHERIC PHYSICS WITH A MAJOR FOCUS ON WEATHER FORECASTING THE STUDY OF METEOROLOGY DATES BACK MILLENNIA THOUGH SIGNIFICANT PROGRESS IN METEOROLOGY DID NOT OCCUR UNTIL THE 18TH CENTURY

Irrelevant sentence: BOB LETS MEET AT DATE TIME PLACE

Plaintext: METEOROLOGY IS A BRANCH OF THE ATMOSPHERIC SCIENCES WHICH INCLUDES ATMOSPHERIC CHEMISTRY AND ATMOSPHERIC PHYSICS WITH A MAJOR FOCUS ON WEATHER FORECASTING BOB LETS MEET AT DATE TIME PLACE THE STUDY OF METEOROLOGY DATES BACK MILLENNIA THOUGH SIGNIFICANT PROGRESS IN METEOROLOGY DID NOT OCCUR UNTIL THE 18TH CENTURY

Introduction (4/6)

- To understand the fault in her procedure, first the structure of a Handycipher key is explained.
- The key length of Handycipher is 41 symbols.
- The symbol "^" is deleted and then the 40 symbols are arranged according to the table at page 6.
- The table area with a white background (on the left side) contains the main symbols of the key.
- The table area with a yellow background (on the right side) contains the nulls.
- By mistake, Alice arranged the nulls not in their correct order, but as they are sorted.
- Thus, the resulting wrong key is: "2H1.OBEFSCVQ4GLR-P9U6WXZKINMT035JA^Y7D8,?", which is included in the file "wrong_key.txt" in the additional zip archive.

Introduction (5/6)

2	H	1	.	O	B	E	F
S	C	V	Q	4	G	L	R
–	P	9	U	6	W	X	Z
K	I	N	M	T	0	3	5
J	A	Y	7	D	8	,	?

Introduction (6/6)

- Alice encrypted the plaintext with the correct key. But to Bob, she sends the wrong key together with the ciphertext. In order to simplify this challenge, the decrypted ciphertext is given in the file "wrong_plaintext.txt".
- Eve manages to intercept both messages, the ciphertext and the wrong key, but she is unable to reveal the plaintext.
- On the contrary, Bob understands that the revealed plaintext is tampered and manages to find the place with the irrelevant sentence.
- After Bob and Alice email to each other, Bob says that he managed to retrieve the plaintext, not by examining all 15! possibilities of the nulls symbols, but with a bit of luck, intuition and logical assumptions.

Challenge

- Your task is to analyze and correct the given "wrong" plaintext and isolate the irrelevant sentence.
- The text is written in English.
- The solution consists of the irrelevant sentence. Please enter the solution in capital letters without any spaces.
- There is no need to either calculate all 15! possibilities of the key, nor to use the Handycipher program. Use another more clever and efficient way.

Additional Files

The additional zip archive contains the following files:

- wrong_key.txt
  - ➥ Contains the wrong key, but is not needed to solve this challenge.
- ciphertext.txt
  - ➥ Contains the ciphertext encrypted with the correct key.
- wrong_plaintext.txt
  - ➥ Contains the plaintext, decrypted with the "wrong" key. You have to retrieve the correct plaintext and the irrelevant sentence.

The MTC3 Team wishes you success!