

MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

HUTTON CIPHER – PART 1

Author: Eric Bond Hutton

May 2023

Introduction

Hutton cipher is a pen-and-paper cipher invented by Eric Bond Hutton in 2018.

A tweak made to it by Girkov Arpa later the same year allowed for a letter to be encrypted as itself, possibly making it more resistant to statistical analysis.

As far as is known only one ciphertext encrypted with the Hutton cipher (in version 1) has been cracked to date. [4]

Interestingly, this was done by means of a brute-force attack, other methods having failed.

Encryption Procedure (1/3)

- Below your plaintext write a keyword repeatedly: the first letter of the keyword below the first letter of the plaintext, the second below the second and so on till the number of letters matches the number in the plaintext.
- Spaces may be retained, omitted or replaced with the word *space*. Punctuation marks may be retained, omitted or spelled out. Numerals may be retained or spelled out.

Encryption Procedure (2/3)

- Write down another keyword, stripped of any duplicate letters, and append to it the remaining letters of the alphabet in order. This is your initial cipher alphabet. It will get scrambled a little almost every time you encrypt a letter.
- Sum the numerical values connoted by their respective positions in the regular alphabet of the first letter of the first keyword and the current first letter of the cipher alphabet.

Encryption Procedure (3/3)

- Locate the first letter of the plaintext in the cipher alphabet and swap it with the letter this number of places to its right, wrapping round to the left if necessary. The letter thus swapped becomes the first letter of the ciphertext.
- In the same manner encrypt the second letter of the plaintext with the second letter of the first keyword and the current first letter of the cipher alphabet, the third with the third letter of the first keyword and the current first letter of the cipher alphabet and so on.

Decryption Procedure

To decrypt, apply the encryption procedure, except the addition steps are replaced with subtraction, and if one ends up with a negative number, 26 is to be repeatedly added to it until it's positive.

Example (1/2)

In the following example the plaintext is "Meet me at the Green Man at three".

The first keyword is "fedora", the second "Jupiter".

Plaintext: MEETMEATTHEGREENMANATTHREE

Repeated first keyword: FEDORAFEDORAFEDORAFEDORAFE

Cipher alphabet: JUPITERABCDEFGHIJKLMNOQSVWXYZ

6 (F) + 10 (J) = 16. Therefore, M swaps with R, which becomes the first letter of the ciphertext.

The cipher alphabet is now: JUPIT**E**MABCDEFGHIKL**R**NOQSVWXYZ

Example (2/2)

5 (E) + 10 (J) = 15. Therefore, E swaps with S, which becomes the second letter of the ciphertext.

The cipher alphabet is now: JUPITSMABCDFGHKLRNOQEVWXYZ

Continuing in this manner, one obtains the following ciphertext:

RSBIENXONGQYTMWQVWXWIOKXKU

Challenge

The challenge is to decrypt the ciphertext given in `hutton_ciphertext_1.txt`.

- The plaintext is in contemporary English and includes no numerals.
- Spaces and punctuation marks were removed before encryption.
- The keywords, both short, can be found in concise English-language dictionaries.

This is the first challenge in a series of three challenges about the Hutton cipher.

In the next parts it gets more difficult: keywords have to be reconstructed and different strategies for obtaining the plaintexts have to be developed.

Resources

1. Original cipher description:
en.wikipedia.org/w/?title=User:Eric_Bond_Hutton&oldid=840686562
2. Encryption and decryption tool created by Girkov Arpa:
hutton-cipher.netlify.app
3. Reddit thread:
reddit.com/r/codes/comments/ar1lbd
Issued in 2019, this challenge remains open as of 2023. The 169,081-letter ciphertext involved having so far resisted all attacks.
4. Only known cracked ciphertext (version 1):
reddit.com/r/codes/comments/ffgpef

Additional Files

→ `hutton_ciphertext_1.txt`: The ciphertext to be decrypted.