MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

Hutton cipher – Part 5

Author: Eric Bond Hutton

October 2023

Introduction (1/2)

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, thereby making statistical attacks more difficult.
As far as is known only one ciphertext encrypted in it – in the original, untweaked version – had been cracked till recently. [4]
Interestingly, this was done by means of a brute-force attack, other methods having failed.

Introduction (2/2)

In 2023 ciphertexts encrypted with the improved version were cracked using brute force and known-plaintext attacks. [5]
In this fifth part, you need to recover a plaintext from a ciphertext.
The keywords might be challenging to find...

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 to the ciphertext but count to the left, wrapping round to the right if necessary.

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: JUPITERABCDFGHKLMNOQSVWXYZ

6 (F) + 10 (J) = 16. Therefore, M swaps with R, which becomes the first letter of the ciphertext.
The cipher alphabet is now: JUPITE**M**ABCDFGHKL**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 (1/2)

The challenge is to decrypt the attached ciphertext.

- The plaintext is in contemporary English and numerals have been spelled out individually
- Spaces and punctuation marks were removed before encryption.
- The keywords are both under ten letters long and are randomly generated strings.

Challenge (2/2)

Please hand in a decrypted plaintext.
The plaintext includes only uppercased letters.
This is the fifth in a series of five challenges involving Hutton cipher. It is a bit more difficult than the earlier ones.

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 remained open till 2023, when the 169,081-letter ciphertext involved was finally cracked by means of a known-plaintext attack.
4. First known cracked ciphertext (version 1):
   reddit.com/r/codes/comments/ffgpef
5. Paper about breaking Hutton cipher (version 2) (2023):
   eprint.iacr.org/2023/1113

Additional Files

→ `hutton_ciphertext_5.txt`: The ciphertext.