MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

Wheatstone Cryptograph – Part 1

Author: madness

April 2021

Introduction (1/2)

The Wheatstone Cryptograph is a simple device invented by Charles Wheatstone in the late 1800s. Variants of it were used until World War II. The device resembles a clock with two hands. For each hand there is a ring of symbols. The longer hand points to the outer ring, which holds the plaintext symbols. The plaintext alphabet consists of the 26 letters of the English alphabet and the space character. The shorter hand points to the inner ring, which holds the ciphertext symbols. The ciphertext alphabet is the key of the device and is a permutation of the 26 English letters; it does not include the space character.
For futher information on the Wheatstone Cryptograph see the references on page 12.

Introduction (2/2)

The hands are geared so that they always move by the same number of symbols on their respective rings in the clockwise sense, but not by the same angle. The short hand moves through an angle that is 27/26 times the angle moved by the long hand.

Figure: https://www.shutterstock.com/image-vector/cipher-algorithm-performing-encryption-decryption-less-1394832830

Generating a key (1/3)

The key, which is the mixed ciphertext alphabet on the inner ring of the Cryptograph, can be generated from a keyword. Here is an example how this is done: Suppose the keyword is SECRETKEY. First, we write down the keyword:

SECRETKEY

Next, consider the set of ciphertext symbols, which is the alphabet:

ABCDEFGHIJKLMNOPQRSTUVWXYZ

From the alphabet, cross out the letters that appear in the keyword:

A B ~~C~~ D ~~E~~ F G H I J K L M N O P Q ~~R~~ ~~S~~ ~~T~~ U V W X Y Z

ABDFGHIJLMNOPQUVWXZ

Generating a key (2/3)

Write the remaining letters under the keyword:

```
SECRETKEY
ABDFGHIJL
MNOPQUVWX
Z
```

Remove duplicate letters in the keyword (but keep the first occurrence of each):

```
SECR TK Y
ABDFGHIJL
MNOPQUVWX
Z
```

Generating a key (3/3)

Read off the key in columns:

```
SAMZ EBN CDO RFP GQ THU KIV JW YLX
```

```
SAMZEBNCDORFPGQTHUKIVJWYLX
```

The key is then written clockwise onto the inner ring of the Cryptograph so that its first letter is coradial (just under) the space character of the outer ring.

Method of Encryption (1/4)

Before encrypting, double letters are removed from the plaintext; the second of each double letter is replaced with Q. As a check, a space character can optionally be added to the end of the plaintext. The plaintext can contain only letters and spaces.

The hands of the device are placed in the 12 o'clock position, so that the long hand points to the space character and the short hand points to the first letter of the key. For each character in the plaintext, the hands revolve until the long hand points to that character. The short hand moves the same number of steps on the inner ring. The character to which the short hand points is the corresponding ciphertext character.

Method of Encryption (2/4)

Let's work through a short example. Suppose the plaintext is

MEET AT DAWN

and the key is the one above, SAMZEBNCDORFPGQTHUKIVJWYLX. First, we must prepare the plaintext by hiding the second E and (optionally) adding a space to the end of the message.

MEQT_AT_DAWN_

The Cryptograph begins with both hands pointing upward. To make this exposition easier, we will unwind the rings of the device and write each ring repeatedly. The initial position is this:

```
_ABCDEFGHIJKLMNOPQRSTUVWXYZ_ABCDEFGHIJKLMNOPQRSTUVWXYZ...
SAMZEBNCDORFPGQTHUKIVJWYLXSAMZEBNCDORFPGQTHUKIVJWYLXSA...
^
```

Method of Encryption (3/4)

To encrypt the first letter, we move until the long hand points to M. The short hand point to G.

```
_ABCDEFGHIJKLMNOPQRSTUVWXYZ_ABCDEFGHIJKLMNOPQRSTUVWXYZ...
SAMZEBNCDORFPGQTHUKIVJWYLXSAMZEBNCDORFPGQTHUKIVJWYLXSA...
                ^
```

We continue clockwise (rightward in the unwound view) to the second letter, E. Its encryption is N.

```
_ABCDEFGHIJKLMNOPQRSTUVWXYZ_ABCDEFGHIJKLMNOPQRSTUVWXYZ...
SAMZEBNCDORFPGQTHUKIVJWYLXSAMZEBNCDORFPGQTHUKIVJWYLXSA...
                                  ^
```

Method of Encryption (4/4)

Then onward to Q.

```
_ABCDEFGHIJKLMNOPQRSTUVWXYZ_ABCDEFGHIJKLMNOPQRSTUVWXYZ...
SAMZEBNCDORFPGQTHUKIVJWYLXSAMZEBNCDORFPGQTHUKIVJWYLXSA...
                                                    ^
```

We continue in this manner to get the full ciphertext:

GNKJMZWZCBAIN

Challenge

Here is a ciphertext that has been encrypted with the Wheatstone Cryptograph.

```
YIMUNIKCAQEIAAMLLRFDNONGGYXCKEWDZQMVLSDGRNV
WOEUYFHNTSENGWGMERYOVMJLJQLIWRZDGLAPCUTQKAD
UMILCCTOLUQMSKFDXWBADHACPTPIVC
```

The first half of the plaintext is

```
CHARLES WHEATSTONE WAS A NINETEQNTH CENTURY
```

The solution to the challenge is the keyword used to generate the key followed by the last two words of the plaintext. The keyword is a single English word.
Please enter the solution in upper-case letters with spaces between the three words.

References

- Charles Wheatstone, “Instructions for the Employment of Wheatstone’s Cryptograph”, The Scientific Papers of Sir Charles Wheatstone, The Physical Society of London, 1879, pages 342-347
  books.google.to/books?id=CtGEAAAAIAAJ
- http://www.jproc.ca/crypto/wheatstone.html
- https://incoherency.co.uk/blog/stories/wheatstone-cryptograph.html
- https://eprint.iacr.org/2020/1492