MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

# Alberti Challenge – Part 1

Author: Peter Uelkes

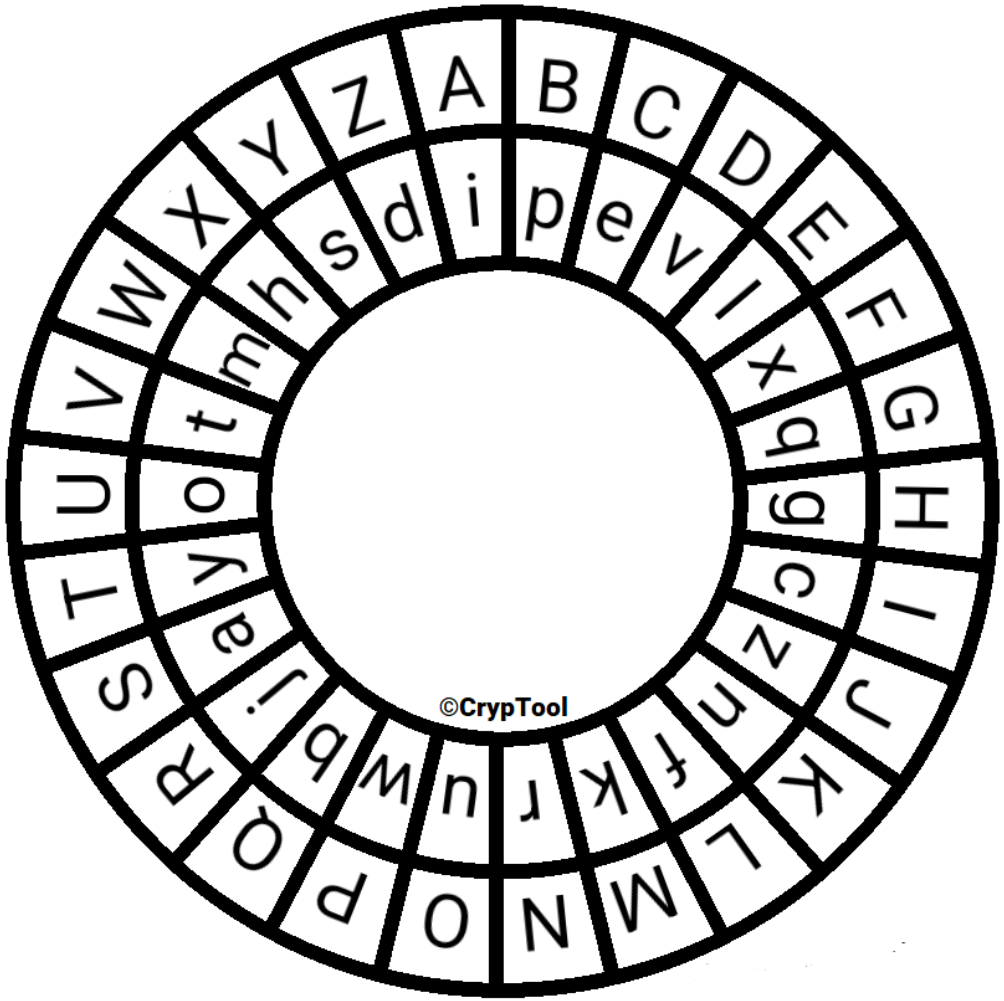
March 2022

# Introduction

The Alberti cipher [1] was inventend by Leon Battista Alberti in the 15th century and is one of the first polyalphabetic ciphers [2]. The cipher uses two disks, which are labeled with two alphabets of the same size in scrambled order. One of the disks is put inside of the other one so the two alphabets can be aligned in different ways by turning the inner disk. For this challenge, we are simplifying this cipher by labeling the outer, stationary disk with the full alphabet of 26 capital letters `ABCDEFGHIJKLMNOPQRSTUVWXYZ` in lexicographical order, without leaving out characters or adding digits as the original suggests. Also we lable the inner, movable disk with the scrambled alphabet: `ipevlxqgcznfkruwbjayotmhsd`

The scrambling of the inner alphabet is a key feature of this cipher.

# Alberti Cipher Disk



# How it works (1/3)

1. After labeling the disks, an indicator letter is selected on the inner disk. For this example we select "m". The key for encryption and decryption consists of the disks labeling and the chosen indicator letter.
2. The text to be encrypted needs to be cleaned up first, as only the symbols that appear on the outer disk can be encrypted, i.e. the capital letters A-Z in this challenge. Let's say, we wanted to encrypt "BEISPIELTEXT" (which means "example text" in German).
3. Now, any letter of the outer disk is selected, let's choose "P". The inner disk is then beeing turned until the indicator letter ("m") aligns with the chosen letter ("P") on the outer disk. The chosen letter ("P") is the first symbol of the ciphertext. Adding the chosen letter to the ciphertext is mandatory for decryption.

# How it works (2/3)

4. Now some plaintext characters, e.g. the 4 characters "BEIS", are encrypted by searching for them on the outer disk and using the aligned character on the inner ring as the corresponding ciphertext character. The ciphertext is now "Pcfwd".
5. We now choose a new character on the outer ring, for example "J", and continue by appending "J" to the ciphertext. This time we decide to encrypt 6 characters. After finding the related ciphertext characters on the inner disk we get the following ciphertext: "PcfwdJetjsqj"

# How it works (3/3)

6. We finish up the encryption by selecting "A", appending it and encrypting the remaining characters. The total ciphertext now is "PcfwdJetjsqjAyw".
7. For decryption, the procedure is reversed accordingly.
8. The key, consisting of the indicator letter and the labeling of the disks, must be agreed on in advance between the parties. A new indicator letter should be chosen before each session.

# Challenge

The described method was used to encrypt an excerpt of English literature from the 19th century. The aforementioned disks (see page 3) and the following ciphertext are given:

```
HtabxmRcgashDfuiomaoWbhaqdatd
IxipdpljqoRljlxtclhNwpwkwmddYfublpJyivvFlg
```

The indicator letter is not revealed. The solution to be submitted is the last word of the plaintext in capital letters.

Example: If the plain text ends with "ORNOTTOBE" you would submit "BE" (without quotes).

# Sources


1. Wikipedia entry:
   `https://en.wikipedia.org/wiki/Alberti_cipher`
2. David Kahn: "The Code-Breakers", revised revision 1996, page 125 ff