MysteryTwister C3
THE CRYPTO CHALLENGE CONTEST

Alberti Challenge – Part 2

Author: Peter Uelkes

May 2022

Introduction (1/2)

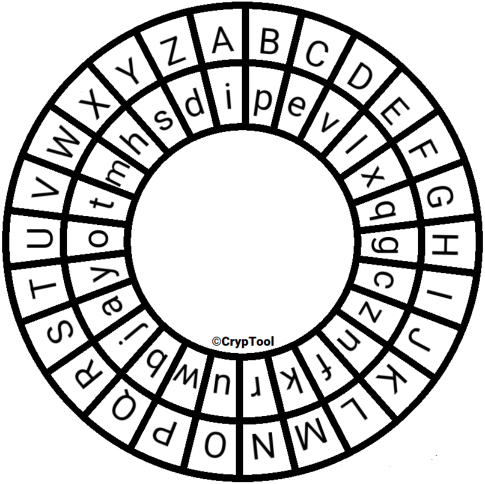
The Alberti cipher [1] was invented by Leon Battista Alberti in the 15th century and is one of the first polyalphabetic ciphers [2]. As long as the algorithm was unknown to an attacker, it used to be quite secure. The cipher uses two disks, which are labeled with two alphabets of the same size. One of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

Introduction (2/2)

Also, for the following example only, we label the inner, movable disk with the permuted alphabet: `ipevlxqgcznfkruwbjayotmhsd`. During encryption of the five actual ciphertexts in this challenge, different permutations of the alphabet `abcdefghijklmnopqrstuvwxyz` were used.

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

Alberti Cipher Disk


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
i p e v l x q g c z u f k r n w b j a y o t m h s d
©CrypTool

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 chosen indicator letter and the labeling on the disks.
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).

How it works (2/3)

3. Now an arbitrary letter of the outer disk is selected, let's choose “P”. The inner disk is then 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.
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 disk as the corresponding ciphertext character. The ciphertext is now “Pcfwd”.

How it works (3/3)

5. We now choose a new character on the outer disk, for example “J”, and proceed with the alignment of the indicator “m” to “J” before 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”.
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 labels of the disks, must be agreed on in advance between the parties. A new indicator letter should be chosen before each session.

The unicity distance (1/3)

The concept of the **unicity distance** originates from a seminal work by Claude Shannon [3], one of the inventors of information theory. The unicity distance U is defined [4] as:

$$U = \frac{H(k)}{D} \tag{1}$$

Here $H(k)$ is the entropy of the key space k, expressed in bits. D is the redundancy of the plaintext P in bits per symbol and can be expressed as $D = H(C) - H(P)$ [5]. Here $H(C)$ is the information content in bits, of a symbol C of the relevant language. For the English language, $H(C) = \log_2(26) \approx 4.7$. $H(P)$ is the empirically determined real information content of a symbol of the relevant language, for English $H(P) \approx 1.5$ is assumed, resulting in a redundancy of $D = 3.2$.

The unicity distance (2/3)

The meaning of the **unicity distance** now lies in the fact that it indicates a theoretical lower limit for the length of a ciphertext, above which cracking the cipher is usually possible unambiguously. For ciphertexts with a length below the unicity limit, this is usually not possible.

Example: Let there be an encryption by the affine cipher (see [6]) with the key (a, b). There are $5+7+9+11+15+17+19+21+23+25 = 152$ possible key pairs and thus $H(k) = \log_2(152) \approx 7.3$. The unicity distance is then calculated as follows:

$$U = \left\lceil \frac{7.3}{3.2} \right\rceil = \lceil 2.28\ldots \rceil = 3$$

The unicity distance (3/3)

For an affine cipher, even short ciphertexts are usually sufficient to decode them unambiguously.

For ciphers with a much larger key space on the other hand, significantly longer texts are required for an unambiguous decryption.

A one-time pad (OTP) of infinite length has an infinitely large unicity distance, as the key space itself is unbounded. This also applies to the special case with a Vigenère encryption, where the key length is equal to or longer than the plaintext length.

Challenge (1/4)

Five ciphertexts of different lengths are given:

- Ciphertext 1 (plaintext length: 85 characters):

  ```
  CpicpwwWendgrinodkxLvmozqzgpdeojrqzIlyxisdifadcfy
  dxUprbkqdcvqqgsoQawdbtzwkcoxkvzZwahuwagmnyh
  ```

- Ciphertext 2 (plaintext length: 55 characters):

  ```
  FersgAiqnoiqjgzpzUnkzrhvhrhlaxnIaibjcwyzcqwpolUkljnzdjqlaNrvf
  ```

- Ciphertext 3 (plaintext length: 42 characters):

  ```
  IpvyzxpyxqTgwukxsaxmttatwNkaoeixebdundyVyjhyuf
  ```

- Ciphertext 4 (plaintext length: 33 characters):

  ```
  KmhzhpbhBhlmnauidawaumqcmWzukjtfdasd
  ```

- Ciphertext 5 (plaintext length: 28 characters):

  ```
  OxjizwadbaGeuhjethqcbsxNliswbei
  ```

Challenge (2/4)

All five English plaintexts were encrypted with the Alberti cipher. The keys, consisting of the labeling of the inner disk and the chosen indicator letter, are all different between the 5 ciphertexts. No encryption parameters were reused besides the aforementioned labeling of the outer disk (see page 2). Your task is to decrypt every ciphertext. From each resulting plaintext, the last word must be submitted in capital letters as the solution. The order of the words corresponds to the order of the given ciphertexts and the words must be separated by spaces.

Challenge (3/4)

In addition, please answer the following two questions:

1. With a known inner alphabet and an unknown indicator, what is the unicity distance $\mathcal{U}_1$ of the Alberti cipher? (This corresponds to the situation in part one of the challenge series).
2. What is the unicity distance $\mathcal{U}_2$ of the Alberti cipher when the inner alphabet and indicator are unknown? (This corresponds to the situation in this second part of the challenge series.)

Please round up each of the two results to the next larger integer and append those two numbers, again separated by spaces, to the solution words of the five ciphertexts.

Challenge (4/4)

Example: If the respective last words of the plaintexts to the ciphertexts one to five are SHANNON, TURING, NEUMANN, REJESWKI, and YARDLEY and the sought unicity lengths are 5.3234... and 8.234234..., then enter the solution:

SHANNON TURING NEUMANN REJEWSKI YARDLEY 6 9

You also have a "wildcard" at your disposal: You may replace one of the solution words with "???" (but not one of the solution numbers!). For example, if you could not find the third word to the solution above, the following input would be accepted as well, as long as the other six items are correct:

SHANNON TURING ??? REJEWSKI YARDLEY 6 9

Now, good luck and have fun!

Sources (1/2)

[1] Wikipedia article about the Alberti cipher: https://en.wikipedia.org/wiki/Alberti_cipher

[2] David Kahn: "The Codebreakers", revision 1996, page 125 ff

[3] Claude E. Shannon: "Communication Theory of Secrecy Systems", Bell System Technical Journal, 28, Oct. 1949, page 656–715 URL: https://www.cs.virginia.edu/~evans/greatworks/shannon1949.pdf

[4] Wikipedia article about the unicity distance: https://en.wikipedia.org/wiki/Unicity_distance

Sources (2/2)

[5] Friedrich L. Bauer: ”Entzifferte Geheimnisse”, second, extendend edition, pages 125, 230, 303, 445-446

[6] Wikipedia article about the affine cipher: https://en.wikipedia.org/wiki/Affine_cipher