Polyalphabetic Ciphers

Irfan Sheikh

Department of Computer Science, University of Delhi

February 4, 2021

Polyalphabetic Ciphers - Motivation

Problem with monoalphabetic ciphers

Highly susceptible to statistical techniques like frequency analysis.

How can we make the cipher stronger?

- Try to lessen the extent to which the structure of the plaintext survives in the ciphertext. How?
- Use different monoalphabetic substitutions as one proceeds through the plaintext message.

Examples

Shift = 3 (first two letters), 1 (next two), 2 (last three)

```
P : B E E T L E S
  + 3 3 1 1 2 2 2
C : E H F U N G U
```

E is substituted by H, then F, and then G. Therefore, the frequency of E's substitute no longer mimics the frequency of E.

Polyalphabetic Ciphers - the Core Idea

What we just described is called a Polyalphabetic Substitution Cipher. It is a cipher based on substitution which uses multiple substitution alphabets throughout the plaintext.

Core idea of polyalphabetic ciphers

- each plaintext letter is assigned more than one substitute.
- consequently, two same letters in the ciphertext need not necessarily decipher to the same plaintext letter.
- this masks the frequency distribution of letters.

Let's take a look at the initially developed polyalphabetic ciphers.

Polyalphabetic Ciphers - The Alberti Cipher (1467)

Alberti Cipher - mixed alphabets, variable period

At random points, change the alphabet used to encrypt the plaintext, indicating the change with an uppercase letter in the ciphertext. First, mutually agree on an index that denotes the letter on the smaller, movable disk, say it is `k`. Select a letter on the outer stationary disk, say `B`, and rotate the inner disk such that `k` and `B` are aligned. This particular alignment of the two discs define a single substitution alphabet.

Figure: The Alberti Cipher Disk - Image taken from `https://sites.wcsu.edu/mbxml/html/section_alberti.html`

The plaintext is denoted by the outer stationary disk, and the ciphertext is denoted by the inner movable disk.

Polyalphabetic Ciphers - The Alberti Cipher

Examples (Encrypting BATTLE using an Alberti Cipher)

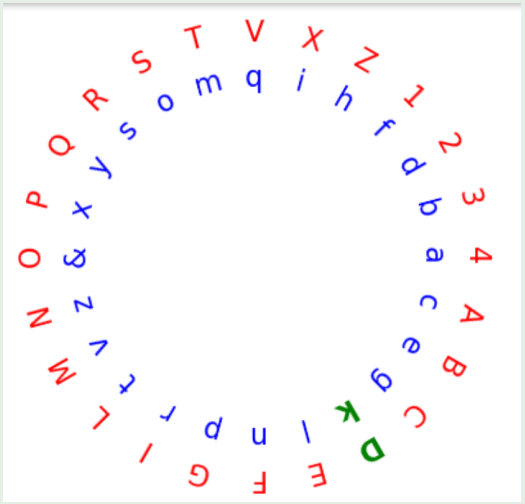
Select index k, aligned with D, denote this using uppercase D and read off the first 3 corresponding cipher letters:

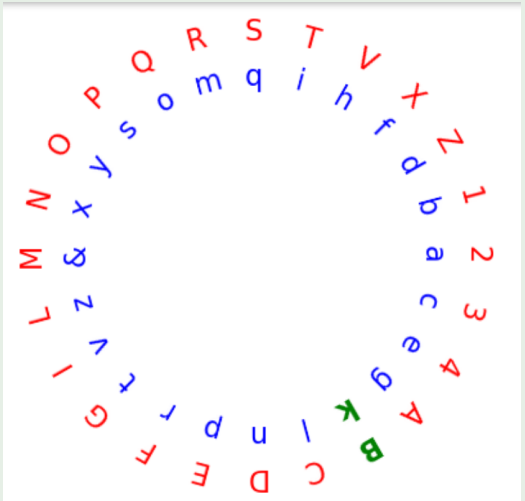
```
P:  B A T  T L E
C:D e c m
```

Similarly, now align k with B and read off the next 3 letters.

```
P:  B A T  T L E
C:D e c m B i z p
```

Images made using the tool at https://sites.wcsu.edu/mbxml/html/section_alberti.html





Polyalphabetic Ciphers - The Trithemius Cipher (1508)

Trithemius cipher - fixed alphabet, fixed period

The idea is to have a fixed alphabet (A-Z), and, instead of switching at random intervals, switch alphabets for each letter of the plaintext (period = 1) by incrementing the shift by 1.

- First letter : first shifted alphabet
- Second letter : second shifted alphabet
- ...and so on

To simplify encryption and decryption, a square table of alphabets called the Tabula recta (or Vigenère square) is often used.

Examples

```
P = B E E T L E S
  + 1 2 3 4 5 6 7
C = C G H X Q K Z
```

Polyalphabetic Ciphers - Breaking Alberti and Trithemius

Problem with the Alberti Cipher

- The capitalized letter is a major clue to the cryptanalyst.
- If the attacker knows about the method, then it is possible to try for all indices on the inner disk. The attacker already knows the key alphabets through the capitalized letters.

Kerckhoffs's principle

A cryptosystem should be secure even if everything about the system, except the key, is public knowledge.

Problem with the Trithemius Cipher

- a very rigid and predictable system - if the attacker knows that this method has been used, it is trivial to break it.
- no concrete concept of a key - violates the Kerckhoffs's principle

Polyalphabetic Ciphers - The Vigenère Cipher (1553)

Vigenère cipher - adding a key

The idea is to extend the Trithemius cipher by adding a key, which is used to dictate the switching of cipher alphabets with each letter. The strength of Vigenère cipher depends on the keyword length.

Examples

The Trithemius cipher we discussed is equivalent to a Vigenère cipher with BCDEFGHIJKLMNOPQRSTUVWXYZA as the key.

A quick summary

- **Alberti**: after a random number of letters (variable period), you change the shift (alphabet) arbitrarily.
- **Trithemius**: after each letter, increment the shift by 1.
- **Vigenère**: after each letter (period $= 1$), change the shift as defined by the keyword.

References

1. Alberti Cipher theory and interactive tool
   https://sites.wcsu.edu/mbxml/html/section_alberti.html
   https://en.wikipedia.org/wiki/Alberti_cipher
2. General Polyalphabetic theory
   William Stallings - Cryptography and Network Security, Seventh Edition
   https://en.wikipedia.org/wiki/Polyalphabetic_cipher