Cracking Vigenere´s Cipher

by Bartosz Grabek

Table of Contents

1. *Author Note*
2. *Introduction*
3. *About Vigenere’s Cipher*
   1. *History*
   2. *Polyalphabetical cipher*
   3. *Encryption and Decryption*
4. *Hacking Vigenere’s Cipher*
   1. *Indispensable assumptions*
   2. *Finding the length of the password*
   3. *Converting into several monoalphabetical ciphers*
   4. *Statistic methods*
   5. *Reading the message*
5. *Glossary*
6. *Bibliography*

# Author

*Hi! My name is Bartek, but friends call me “Grave”, probably due to my seriousness and alias distant connection to my last name .*

*I’ve been interested in programming and Computer Science since I was a 14-year old kid. It was in the middle school, where on IT lessons I created a few very simple programs using Logomotion, although I didn’t enjoy it at first. I took up a new challenge to learn Python. Since then, I have read probably thousands of articles and several books, watched quintillion of youtube and Udemy tutorials and developed my own programming projects, one of which is described in this document. I have decided to take Matura exam in IT and apply to a foreign university, preferably in the UK.*

*This time we’ll take a closer look on the basics of cryptology.*

This document contains useful information on how to hack polyalphabetical ciphers, particularly Vigenere’s Cipher. It has been written using simple language, so that everyone can understand all the ideas behind the topic. For maximum comprehension it is advisable to look at the code executing the mechanics described in each section. The code is currently available only in Python language.

This document includes:

* theoretical approach to cracking Vigenere’s Cipher
* practical realization of ideas described in Python code

For Your comfort of reading more sophisticated words and professional phrases are additionally described in adnotations under each section.

Some ideas point to particular code lines using numbers in square brackets, e.g. [2].

# Introduction

# About Vigenere’s Cipher

## History

The history behind Vigenere’s cipher is quite simple and there’s absolutely nothing to talk about. The history behind Vigenere’s cipher is quite simple and there’s absolutely nothing to talk about. The history behind Vigenere’s cipher is quite simple and there’s absolutely nothing to talk about. The history behind Vigenere’s cipher is quite simple and there’s absolutely nothing to talk about. The history behind Vigenere’s cipher is quite simple and there’s absolutely nothing to talk about. The history behind Vigenere’s cipher is quite simple and there’s absolutely nothing to talk about. The history behind Vigenere’s cipher is quite simple and there’s absolutely nothing to talk about.

## Polyalphabetical Cipher

Polyalphabetical cipher is said to be a more sophisticated version of monoalphabetical cipher, but it’s not. It can be divided/converted into monoalphabetical cipher, but only if certain conditions are met. Polyalphabetical cipher is said to be a more sophisticated version of monoalphabetical cipher, but it’s not. It can be divided/converted into monoalphabetical cipher, but only if certain conditions are met. Polyalphabetical cipher is said to be a more sophisticated version of monoalphabetical cipher, but it’s not. It can be divided/converted into monoalphabetical cipher, but only if certain conditions are met. Polyalphabetical cipher is said to be a more sophisticated version of monoalphabetical cipher, but it’s not. It can be divided/converted into monoalphabetical cipher, but only if certain conditions are met.

## Encryption and Decryption

Here is the description of how to encrypt and decrypt messages. Here is the description of how to encrypt and decrypt messages. Here is the description of how to encrypt and decrypt messages. Here is the description of how to encrypt and decrypt messages. Here is the description of how to encrypt and decrypt messages. Here is the description of how to encrypt and decrypt messages. Here is the description of how to encrypt and decrypt messages. Here is the description of how to encrypt and decrypt messages. Here is the description of how to encrypt and decrypt messages. Here is the description of how to encrypt and decrypt messages. Here is the description of how to encrypt and decrypt messages. Here is the description of how to encrypt and decrypt messages. Here is the description of how to encrypt and decrypt messages. Here is the description of how to encrypt and decrypt messages. Here is the description of how to encrypt and decrypt messages. Here is the description of how to encrypt and decrypt messages. Here is the description of how to encrypt and decrypt messages. Here is the description of how to encrypt and decrypt messages. Here is the description of how to encrypt and decrypt messages. Here is the description of how to encrypt and decrypt messages.