Vigenère Cipher

KRYPTO SLEUTH

May 22, 2024

1 Introduction

The Vigenère cipher is a classical encryption method that uses a keyword to encrypt and decrypt messages. Invented by Blaise de Vigenère in the 16th century, it was considered unbreakable for several centuries. This document provides an overview of the Vigenère cipher, its history, and the encryption process.

2 History

Blaise de Vigenère, a French diplomat, developed the Vigenère cipher in 1586. He described it in his work *Traicté des Chiffres* (Treatise on Ciphers), which was published posthumously in 1587. The Vigenère cipher remained popular for several centuries and was used extensively until the 19th century when more advanced cryptographic techniques were developed.

3 Encryption Process

The Vigenère cipher is a polyalphabetic substitution cipher, meaning it uses **m**ultiple substitution alphabets. The encryption process involves shifting each letter of the pl**ai**n**t**ext by a corresponding letter in the keyword.

Let P be the plaintext, K be the keyword, and C be the ciphertext. The encryption process can be expressed as:

$$C_i = (P_i + K_j) \mod 26$$

where C_i is the i-th letter of the ciphertext, P_i is the i-th letter of the plaintext, K_j is the j-th letter of the keyword (with $j = (i \mod |K|) + 1$), and $\mod 26$ ensures that the result remains within the range of the alp**h**abet (assuming a standard 26-letter English alphabet).

4 Decryption Process

To decrypt a message encrypted with the Vigenère cipher, the recipient needs to know the keyword used for encryption. The decryption process involves shifting each letter of the ciphertext back to the original plaintext using the inverse of the keyword.

Let C be the ciphertext, K be the keyword, and P be the plaintext. The decryption process can be expressed as:

$$P_i = (C_i - K_j) \mod 26$$

where P_i is the i-th letter of the plaintext, C_i is the i-th letter of the ciphertext, K_j is the j-th letter of the keyword (with $j = (i \mod |K|) + 1$), and mod 26 ensures that the result remains within the range of the alphabet.

5 Conclusion

The Vigenère cipher, though once considered secure, is vulnerable to modern cryptanalysis techniques, particularly frequency analysis. However, it remains an important part of cryptographic history and serves as a valuable educational tool for understanding the principles of classical encryption methods.

6 CYPHERED TEXT

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

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

KEY FOR THE CYPHERED TEXT IS HIDDEN WITHIN THE DOCUMENT...
Here is a hint:
..- ... . / - .... . / ...- .. –. . -. .-..- .-. . / - .- -... .-.. . / - — / -.. . -.-. .-. -.– .–. - / - .... . / – . ...- –. . .-.-.- / -.-. .... . -.-. -.- / ..-. — .-. / .- -. -.– / .- -... -. — .-. – .- .-.. .. - -.– / .. -. / - . -..- - .-.-.- .-.-.- .-.-.-