Code a Python Playfair Cipher

Reading

10m - 30m

Status Incomplete

Introduction

In this reading, you will be introduced to the Playfair Cipher algorithm, a historical encryption technique that played an important role in the early days of cryptography.

As a new cyber security professional, it is important to understand the principles of this algorithm, as it provides insight into the historical development of cryptography and lays the foundation for more advanced techniques used today. Additionally, the Playfair Cipher algorithm demonstrates the importance of key management and the vulnerabilities that can arise if keys are not managed securely, which are relevant considerations for any modern encryption scheme.

About the Playfair Cipher Algorithm

The Playfair cipher was the first practical digraph substitution cipher. The scheme was invented in 1854 by Charles Wheatstone but was named after Lord Playfair, who promoted the use of the cipher. In the Playfair cipher, unlike the traditional cipher, we encrypt a pair of alphabets (digraphs) instead of a single alphabet.

It was used for tactical purposes by British forces in the Second Boer War and World War I, and the same objective by the Australians during World War II. That's because Playfair is reasonably quick to use and requires no special equipment.

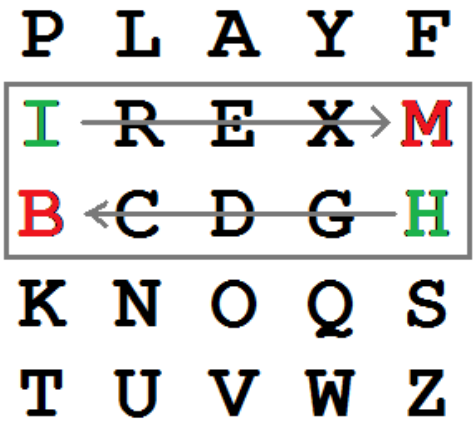
Steps in Algorithm

The algorithm consists of two steps:

1. **Generate the key square matrix (5 × 5)**: the matrix grid of alphabets that acts as the key to encrypt the plain text. Each of the 25 alphabets must be unique, and one letter of the alphabet (usually J) is omitted from the table (since the table can only contain 25 alphabets). If the plain text contains J, it is replaced with I. The initial letters in the key square are the key's unique letters in the order they appear, followed by the remaining letters of the alphabet in order.

2. **Split the words into pairs of letters and encrypt:** the plain text is split into pairs of two letters (digraphs). If there is an odd number of letters, a Z is added to the last letter. Encrypt the message using two letters each time.

The image below shows an example of the Playfair Cipher, using the key 'Playfair', where the diagraph "HI" becomes "BM"



There can be some complications with this process. The four rules below are in place to times where the choice is not obvious:

1. When you get two letters, if they are the same letter, you add a "filler" in the middle. It can be the letter 'x'.
2. If the two letters fall in the same row of the matrix, you substitute them with the next letter in the row. Rows have a circular behaviour. The next letter of the last in a row is the first letter in that row.
3. If the two letters fall in the same column of the matrix, you substitute them with the next letter in the column (going down). Columns have a circular behaviour. The next letter of the last in a column is the first letter in that column.
4. If the two letters are not in the same row and column, then you substitute each letter with the letter in the same row and the column of the second letter.

Further Reading

To learn more about the Playfair Cipher Algorithm, you can begin by exploring and reading the following resource:

- Playfair Cipher (Wikipedia)

Conclusion

The Playfair Cipher algorithm is a fascinating historical encryption technique that is still relevant to cyber security professionals today. Understanding the principles and limitations of this algorithm provides insight into the evolution of cryptography and highlights the importance of secure key management in any encryption scheme.

In the next activity, you will have the opportunity to put your knowledge into practice by coding your own Playfair Cipher.

✓ Mark Completed

Previous
The Use of Cryptography

Next
Code a Python Playfair Cipher

How well did this activity help you to understand the content?

Let us know how we're doing

☆ ☆ ☆ ☆ ☆

W06D5

Fri Aug 2

Outline & Notes (1)

Lectures (1)

Work (10)

7 hrs

- Cryptanalysis
- The Use of the Historical vs. Modern Encryption
- Cryptanalysis Quiz
- Cryptography Features and Objectives
- Typical Levels of Cryptography
- The Use of Cryptography
- Code a Python Playfair Cipher
- Cryptographic Encryption
- Cryptographic Methods with GPG

W06D5 Schedule »