Comparison of Different Encryption Algorithms

Shreyas Prashanth
PES University
CSE Department
Bangalore, India
PES1201701249

Prajna Girish
PES University
CSE Department
Bangalore, India
PES1201701261

***Abstract*—The goal of the project was to compare and contrast different encryption algorithms. We have focussed on those encryption methods that require a cipher- namely Affine, Vigenere, Hill, Playfair and Autokey. All these algorithms are compared on the basis of their time ans space complexities and inferences were drawn from the data.**

I. Introduction

Security is one of the most important aspects of any building any computational system. Encryption is the process of encoding a message or information in a way that only authorised parties can access it and those who are not authorised cannot do so. Through the use of an algorithm, information is made into meaningless cipher text and requires the use of a key to transform the data back into its original form.

II. Algorithms Used

Playfair Cipher

In a Playfair cipher the message is split into digraphs, pairs of two letters. If there is an odd number of letters, a Z is added to the last letter. The Playfair cipher uses a few simple rules relating to where the letters of each digraph are in relation to each other. The rules are:

1. If both letters are in the same column, take the letter below each one (going back to the top if at the bottom)

2. If both letters are in the same row, take the letter to the right of each one (going back to the left if at the farthest right)

3.If neither of the preceding two rules are true, form a rectangle with the two letters and take the letters on the horizontal opposite corner of the rectangle

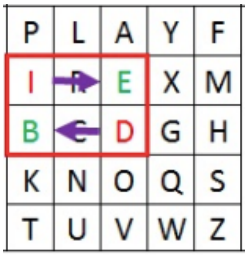

Fig:Encryption using rule 3 of the playfair cipher

Affine Cipher

The Affine cipher works on the following principle:

$$E(x) = (ax + b) \bmod m$$

Where a and b are the key values and a has to be relatively prime to m. Here, we are assuming m is the length of the standard alphabet, that is 26. The cipher's primary weakness comes from the fact that if the cryptanalyst can discover (by means of frequency analysis, brute force, guessing or otherwise) the plaintext of two cipher text characters, then the key can be obtained by solving a simultaneous equation.

Vigenere Cipher

The Vigenere cipher uses a 26×26 table with A to Z as the row heading and column heading.Starting with the second row, each row has the letters shifted to the left one position in a cyclic way. To encrypt, pick a letter in the plaintext and its corresponding letter in the keyword, use the keyword letter and the plaintext letter as the row index and column index, respectively, and the entry at the row-column intersection is the letter in the ciphertext.

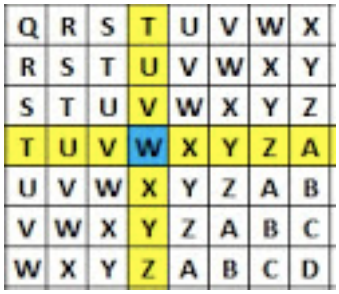

Fig: Intersection of the cipher text and keyword in Vigenere

Autokey Cipher

The Autokey Cipher is a poly-alphabetic substitution cipher. It is closely related to the Vigenere cipher, but uses a different method of generating the key. It was invented by Blaise de Vigenère in 1586, and is in general more secure than the Vigenere cipher.To encipher a message, place the keyword above the plaintext. Once all of the key characters have been written, start writing the plaintext as the key

Hill Cipher

Invented by Lester S. Hill in 1929, the Hill cipher is a polygraphic substitution cipher based on linear algebra. Hill used matrices and matrix multiplication to mix up the plaintext. The plaintext is broken down into a number of chunks equal to the dimensions of the square cipher matrix. On the basis of matrix multiplication and then a modulo 26 operation, we get the resulting encrypted matrix.

III. RESULTS

We ran all the 5 algorithms on the same dataset with the same plaintext and ciphertext and observed the following

Cipher	Space Complexity	Time Complexity
Vigenere	O(k)	O(k)
Affine	O(k)	O(k)
Autokey	O(k)	O(k)
Hill	O(k^2)	O(k^2)
Playfair	O(n)	O(k)

Where k is the length of the plaintext and m is the length of the ciphertext

Cipher Name	Time taken
Vigenere	0.42
Affine	0.00312
Autokey	0.988
Hill	46.12
Playfair	0.7623

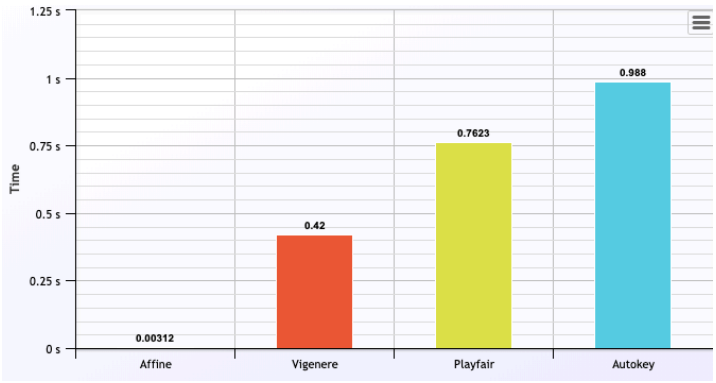

Fig:Bar graph comparing computation times

IV. CONCLUSION

This aim of this project was to compare some different classical encryption algorithms to see how the performed when run over the same data to be encrypted. We see that in this case, the affine cipher has taken the least time to compute, followed by the Vigenere, Playfair and Autokey ciphers. The Hill cipher takes an extremely long time to compute owing to its computationally intensive nature of matrix multiplication. However, each cipher has its own advantages and disadvantages which make them all unique.

Although we faced obstacles while implementing these algorithms, this project has greatly helped us in understanding the practical applications and implementations of some encryption algorithms.

In conclusion, this entire project was a great learning experience where we were able to practically implement some of the algorithms we have only seen on paper.

V. ACKNOWLEDGMENT

We would like to thank our mentor, N S Kumar, for guiding us through the entire project and helping us learn and understand the required concepts. We would also like to thank our peers for constant support and encouragement.

VI. REFERENCES

1. An interactive cryptanalysis algorithm for the Vigenere Cipher ME Dalkilic, C Gungor - ... *Conference on Advances in Information Systems, 2000 - Springer*

2. Ciphertext-policy attribute-based encryption *J Bethencourt, A Sahai, B Waters - 2007 IEEE symposium on ..., 2007 - ieeexplore.ieee.org*

3.http://practicalcryptography.com/ciphers/

4.https://www.techiedelight.com/vigenere-cipher-implementation/

5.https://www.commonlounge.com/discussion/b41d349180624227ae213861ed315168

6.http://practicalcryptography.com/cryptanalysis/cipher-implementations/implementation/