ENCRYPTION/DECRYPTION OF DATA USING INVERSE MATRIX METHOD

Group 8 : Inverse Matrix

AU2040051 - Jevin Jivani

AU2040002 - Shrey Somani

AU2040048 - Ronit Shah

Abstract- Cryptography is something which is used in our everyday life but most people don't know about it. Cryptography secures data with the help of encryption and decryption. Various ciphers are available to encrypt the data which use linear algebra. In this project we will be using Hill Cipher and Play Fair Cipher to encrypt and decrypt words and demonstrate how this whole thing works.

Keywords—Cryptography, encryption, decryption, data, ciphers, secure

I. INTRODUCTION

Securing data and files comes without saying for an individual as it is a matter of privacy. Through this project, we will show how our day-to-day data is secured using cryptography. Cryptography is a way or technique to secure data or some sort of information from third-party apps or people. The messages are secured via encryption and then decrypted for the reader to understand. Encryption converts plaintext into ciphertext and decryption converts it back into its plaintext.

II. BACKGROUND

In earlier times the messenger used to encrypt the information which was to be delivered to the king. The earliest record for encryption dates back to around 400-600 B.C.E where Spartans had used a cipher device called scytale. During World War 1, Germans used the ADFGVX field cipher which involved the use of a 6x6 matrix to encrypt and then pass on the messages and signals. Now, in the modern era computers and algorithms are used to encrypt and decrypt messages. The ciphers which will be used by us are the basics of ciphers. Cyber security firms use even more complex and tough ciphers which are impossible for hackers to crack and break through.

III. MOTIVATION

Until just a few years ago, encryption was not a vital part of everyone's life. People were not so conscious to maintain the confidentiality of their data. Firms and companies saw encryption as a tool to invite customers and show how serious the company is to secure data. With the increase in cybercrimes and data breaches, it has now become a regulation. Encryption/decryption assures people their confidentiality is maintained and that whoever supplies or accesses the data is authorized personnel. It also ensures that the message or data sent is the same when it is received. Another reason for encryption is non-repudiation which means that the sender or recipient cannot deny the validity of data and that the data is ready for use and at optimum performance level. To sum it up, the main reasons for encryption/decryption are confidentiality, authentication, integrity, non-repudiation and availability.

IV. LITERATURE SURVEY

Substitution cipher is one of the basic components of classical ciphers. A substitution cipher is an encryption method in which plaintext units are replaced with ciphertext according to a set of rules; the units can be single letters, pairs of letters, triplets of letters, combinations of the above, and so on. The text is decoded by the recipient via an inverse substitution. There are a number of different types of substitution cipher, for example if a cipher operates on large groups of letters, it is called polygraphic. A monoalphabetic cipher uses fixed substitution over the entire message whereas a polyalphabetic cipher uses a number of substitutions at different times in the message such as with homonym, where a unit from the plaintext is mapped to one of various outcomes in the ciphertext. Hill cipher is a type of monoalphabetic polygraphic substitution cipher. Hill cipher is a type of monoalphabetic polygraphic substitution cipher. Hill cipher is a block cipher that has several advantages such as disguising letter frequencies of the plaintext, its simplicity because of using matrix multiplication and inversion for enciphering and deciphering, its high speed, and high throughput. Hill cipher algorithm has a drawback. It uses random key matrix where we may not be able to decrypt the encrypted message, if the key matrix is not invertible. Also, the computational complexity can be reduced by avoiding the process of finding inverse of the matrix at the time of decryption, as we use Involutory key matrix for encryption in the Advanced Hill Cipher.

V. CONTRIBUTION

Jevin Jivani: -

- Coded the main content of the project. Used hill cipher and Play-Fair cipher to apply the concept of linear algebra.
- Analysed the code and text encryption/decryption algorithm.
- Prepared slides for presentation.
- Find the relevant detail which are used for the project like articles, useful links.

Somani Shrey: -

- Analysed the code and text encryption/decryption algorithm.
- Collected information for the content.
- Prepared slides for presentation.
- Find the relevant detail which are used for the project like articles, useful links.

Ronit Shah: -

- Collected information for the content.
- Analysis of code and text encryption/decryption algorithm.
- Prepared slides for presentation.
- Found articles for literature survey.

VI. REFERENCE

Howard Anton, Chris Rorres (2005), Elementary Linear Algebra, Application Version 9th Edition, Wiley India.
https://www.amazon.in/Elementary-Linear-Algebra-Applications-Solutions/dp/0471433292

Isha Upadhyay (2021, January 5), Hill Cipher: A Comprehensive Guide, Jigsaw Academy.
https://www.jigsawacademy.com/blogs/cyber-security/hill-cipher/

Murray Eisenberg, Hill ciphers and modular linear algebra, mimeographed notes, University of Massachusetts, 1998, 19 pages
https://apprendre-en-ligne.net/crypto/hill/Hillciph.pdf