ISSN 1870-4069

Hill Algorithm Decryption using Parallel Calculations by Brute Force

Bárbara Emma Sánchez Rinza, Juan Carlos García Lezama

Benemérita Universidad Autónoma de Puebla,
Facultad de ciencias de la computación, Puebla, Mexico

brinza@hotmail.com

Abstract. Hill coding, based on linear algebra, by the American mathematician Lester S. Hill in 1929 in this method we use a square matrix A of integers as a key, which determines the linear transformation Y = A * X where Y, X they are the column vectors. Using this encryption method, a text was encrypted to later decrypt it with the use of brute force, that is, to test each of the possible combinations of keys to find the original text in this article. A 2x2 key was used to encrypt the text with a limit from 1 to 256 for each element in the matrix 256 x 256 x 256 x 256 permutations were found that is 4,294,967,296 possible keys for this decipher this text as it can be clearly seen there are too many operations to perform that can consume a considerable time for the CPU since he must decipher the text for each of these combinations and find the correct one, that is why to do this arduous task, parallel programming was used to generate each of the keys and work with each one of them.

Keywords. Cryptography, encrypt, keys, parallel programming.

1 Introduction

Cryptography comes from an etymological word Kriptos means “hidden”, Graphos means “writing”, which would mean “hidden writings”, or in its broadest sense it would be to apply some technique to make a message unintelligible [1].

The main objective is to encrypt and / or protect the information with an algorithm using keys, without them would be really difficult to obtain the original text. In these years the protection of the information is an indispensable need once saved on a computer, due to its use in great part of daily life.

Even worse, the Internet makes available a large number of people, devices that contain confidential information for each one of us, such as addresses, telephone numbers and financial information, among others.

2014 was a great scenario of major attacks on companies by hackers, which mostly represented great losses for companies, and a big a risk for millions of clients, including eBay, HOME DEPOT, SONY, CASINOS SANDS [2]

For a company, its information is the most important asset, without it, might bring a bankruptcy for example, a company can lose all the products due to a natural disas-

ter and might be able to recover itself by looking for investors, loans, mortgaging its properties, etc., but if it loses all the customer lists, suppliers, debtors, etc. it can be catastrophic because of the great value of this information that would not be recovered.

2 Development

Encrypting data means altering them, through the use of a key or pair of keys, so that they are not readable for those who should not have access to information, that is to say, intruders. Through the decryption process for those who have the key, they can use it to obtain the original information.

This technique protects sensitive information such as personal data or bank accounts of an organization, guaranteeing its authenticity, integrity, and confidentiality, if the encrypted data is intercepted, it cannot be read or modified by intruders.

The cryptographic systems where the encryption and decryption key match, are called "symmetric encryption" that can be seen as the lock of a door where it is possible to open and close with the same key.

There are 3 basic encryption techniques from which all the classic systems of secret key are generated: **Transposition** (units order alteration of the original text according to a given key), **Substitution** (replacement of the original text units by others according to a key), and **Product** (Composition of several ciphers, substitution and / or transposition, each of which will depend on a key).

In this article we will focus on the Polyalphabetic Substitution Method since the algorithm to be treated is this type.

3 Substitution Ciphers

The substitution cipher consists in units of plain text (text without encryption) are replaced by units of encrypted text, there are different cipher substitution types. If the cipher operates on simple letters it is term simple substitution cipher; if the cipher operates on larger groups of letters it is called, polygraphic. A cipher is monoalphabetic when a character of the plaintext is replaced by one and only one of the ciphertext or polyalphabetic. An element in the plaintext can be represented by more than one character. [3]

3.1 Polyalphabetic

A polyalphabetic substitution system is when each character is not always replaced by the same character that is in the system there are several characters that could replace it and according to the circumstances would apply one or the other.

3.2 Hill Cipher

It is based on linear algebra developed by the mathematician Lester S. Hill in 1929 in his article Cryptography in an Algebraic Alphabet, published in The American Mathematical Monthly [4] is a cryptographic system of polyalphabetic substitution.

It consists in associate each alphabet letter with a number, for this article were used 27 characters of the alphabet. In this case, we did it for 256 characters.

A	B	C	D	E	F	G	H	I	J	K	L	M	N
0	1	2	3	4	5	6	7	8	9	10	11	12	13
Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	
14	15	16	17	18	19	20	21	22	23	24	25	26	

Fig. 1. Table of characters.

In Hill's cipher, a square matrix of integers A is used as a key, which determines the linear transformation Y = A X, where Y, X are column vectors.

Let's see an example. Consider the 3x3 square matrix (square matrices of any size can be taken) and the corresponding linear transformation Y = A X:

$$\begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 4 & 5 \\ 1 & 0 & 6 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$$

$$\left.\begin{aligned} y_1 &= 1 \cdot x_1 + 2 \cdot x_2 + 3 \cdot x_3 \\ y_2 &= 0 \cdot x_1 + 4 \cdot x_2 + 5 \cdot x_3 \\ y_3 &= 1 \cdot x_1 + 0 \cdot x_2 + 6 \cdot x_3 \end{aligned}\right\}$$

Fig. 2. Multiplication of a matrix by a column vector.

Taking the plain text "HOLA MUNDO"

Whose numeric transcription according to the PREVIOUS table would be: 7,15,11,0,12,21,13,3,15

Since the linear transformation is in sequences of 3, we are going to group the numbers in three, then we will apply the linear transformation (72,111,108), (97, 32, 74), (117, 97,110).

Next, we are going to transform in a trigraph the previous numbers, through the linear transformation given by the key, into new trigraph that will be the cipher numeric message.

$$\begin{pmatrix}1&2&3\\0&4&5\\1&0&6\end{pmatrix}\cdot\begin{pmatrix}7\\15\\10\end{pmatrix}=\begin{pmatrix}67\\110\\67\end{pmatrix}\equiv\begin{pmatrix}13\\2\\13\end{pmatrix}$$

$$\begin{pmatrix}1&2&3\\0&4&5\\1&0&6\end{pmatrix}\cdot\begin{pmatrix}0\\12\\21\end{pmatrix}=\begin{pmatrix}87\\153\\126\end{pmatrix}\equiv\begin{pmatrix}6\\18\\18\end{pmatrix}$$

$$\begin{pmatrix}1&2&3\\0&4&5\\1&0&6\end{pmatrix}\cdot\begin{pmatrix}13\\3\\15\end{pmatrix}=\begin{pmatrix}412\\393\\361\end{pmatrix}\equiv\begin{pmatrix}21\\6\\22\end{pmatrix}$$

Fig. 3. Multiplicative column vector and operation module 256.

Although the linear transformation of the trigraph (7, 15, 10) is initially (67, 110, 67), since we are working with integers module 27, this trigraph becomes (13, 2, 13), since 67 = 2 x 27 + 13 and 110 = 4 x 27 + 2. Results the same for the rest.

Therefore, the cipher numeric message is "13, 2, 13, 6, 18, 18, 21, 6, 22" by transforming the numbers again into their corresponding letters, it becomes into the cipher message: NCNGRRUGV

In order to decode encrypted messages using the Hill method, the matrix of the linear transformation used, the key, must be an invertible matrix. Our matrix example is, since its determinant is non-zero, | A | = 22. In addition, the inverse matrix of A, is the one needed to decode an encrypted message, is:

$$A^{-1}=\begin{pmatrix}\frac{24}{22}&\frac{-12}{22}&\frac{-2}{22}\\\frac{5}{22}&\frac{3}{22}&\frac{-5}{22}\\\frac{-4}{22}&\frac{2}{22}&\frac{4}{22}\end{pmatrix}$$

Fig. 4. Inverse Matrix key.

We are working with the integers module 27 and we are going to transform the previous inverse matrix into a matrix with integers modulo 27. To begin, we need the inverse of the number 22. We look for a number that multiplied by 22 the module is equal to 1 in the following way: 22 x 16 = 352 is equal to 1, module 27, then 1/22 = 16. And the inverse matrix is transformed, module 27 would be equal to:

$$A^{-1} = \begin{pmatrix} \frac{24}{22} & \frac{-12}{22} & \frac{-2}{22} \\ \frac{5}{22} & \frac{3}{22} & \frac{-5}{22} \\ \frac{-4}{22} & \frac{2}{22} & \frac{4}{22} \end{pmatrix} = \begin{pmatrix} 24\times16 & -12\times16 & -2\times16 \\ 5\times16 & 3\times16 & -5\times16 \\ -4\times16 & 2\times16 & 4\times16 \end{pmatrix}$$

$$= \begin{pmatrix} 384 & -192 & -32 \\ 80 & 48 & -80 \\ -64 & 32 & 64 \end{pmatrix} = \begin{pmatrix} 6 & 24 & 22 \\ 26 & 21 & 1 \\ 17 & 5 & 10 \end{pmatrix}$$

Fig. 5. Inverse matrix module numbers 27.

In order to decode the message it is necessary to use the same previous method, Hill's cipher, but using as inverse key matrix A-1 (module 27) of the coding matrix A.

In the same way, the encrypted message is written in terms of the associated number in Figure 1 (13, 2, 13), (6, 18, 18), (21, 6, 22) they are transformed by the linear transformation with matrix A ^ (-1), that is, Y = A ^ (- 1) · X.

$$\begin{pmatrix} 6 & 24 & 22 \\ 26 & 21 & 1 \\ 17 & 5 & 10 \end{pmatrix} \cdot \begin{pmatrix} 13 \\ 2 \\ 13 \end{pmatrix} = \begin{pmatrix} 412 \\ 393 \\ 361 \end{pmatrix} \equiv \begin{pmatrix} 7 \\ 15 \\ 11 \end{pmatrix}$$

$$\begin{pmatrix} 6 & 24 & 22 \\ 26 & 21 & 1 \\ 17 & 5 & 10 \end{pmatrix} \cdot \begin{pmatrix} 6 \\ 18 \\ 18 \end{pmatrix} = \begin{pmatrix} 508 \\ 552 \\ 372 \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 12 \\ 21 \end{pmatrix}$$

$$\begin{pmatrix} 6 & 24 & 22 \\ 26 & 21 & 1 \\ 17 & 5 & 10 \end{pmatrix} \cdot \begin{pmatrix} 21 \\ 6 \\ 22 \end{pmatrix} = \begin{pmatrix} 736 \\ 694 \\ 739 \end{pmatrix} \equiv \begin{pmatrix} 13 \\ 3 \\ 15 \end{pmatrix}$$

Fig. 6. Inverse matrix transformation and encrypted vector.

The original sequence of the numerical trigraphs associated with the previous coded message is (7, 15, 10), (22, 12, 21), (7, 19, 10). And by translating the numbers to their corresponding letters of the alphabet you get that the original message sent is: HOLA MUNDO

As you can see it is a simple encryption and decryption algorithm knowing the correct key but what would happen if the key is not known? It could take too much time to find the correct key that is why this algorithm was implemented in a program written in the Java language with the use of thread to generate the possible permutations keys and at the same time to test each one of them.

4 Decryption in Java Language

In this application developed in Java language, the decryption of the Hill algorithm by brute force was implemented, that consists in testing in the worst case each of the

possible keys of a set in a parallel way with 3 thread, the main shows the window featured in figure 7.

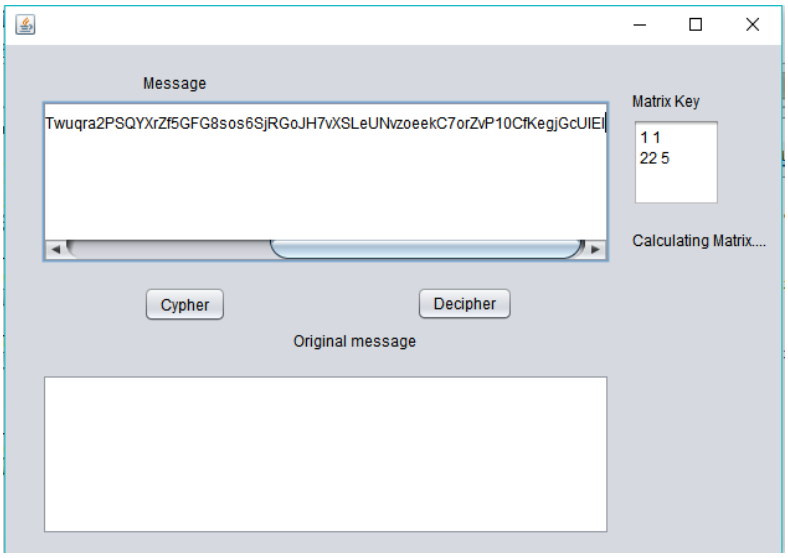

Fig. 7. Main window application.

```
public static double determinante(double[][] matriz)
{
    double det;
    if(matriz.length==2)
    {
        det=(matriz[0][0]*matriz[1][1])-(matriz[1][0]*matriz[0][1]);
        return det;
    }
    double suma=0;
    for(int i=0; i<matriz.length; i++){
    double[][] nm=new double[matriz.length-1][matriz.length-1];
        for(int j=0; j<matriz.length; j++){
            if(j!=i){
                for(int k=1; k<matriz.length; k++){
                int indice=-1;
                if(j<i)
                indice=j;
                else if(j>i)
                indice=j-1;
                nm[indice][k-1]=matriz[j][k];
                }
            }
        }
        if(i%2==0)
        suma+=matriz[i][0] * determinante(nm);
        else
        suma-=matriz[i][0] * determinante(nm);
    }
    return suma;
}
```

Fig. 8. Algorithm where the determinant of a square matrix of n * n is calculated.

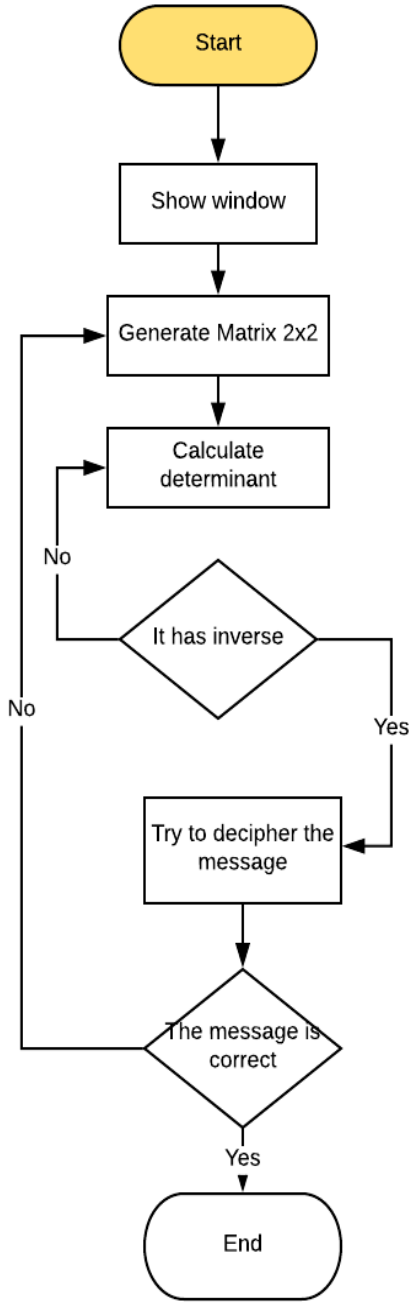

Fig. 9. Decryption process Flowchart.

In thread 2 the possible permutations were generated. 4,294,967,296 possible keys for a square 2x2 matrix from 1 to 256 in each of its elements and verify that this matrix has an inverse, which means that its determinant is different from 0.

In thread 3, the decryption process is done but only if the generated matrix has an inverse if it does not, goes back to generate a new matrix within the established range.

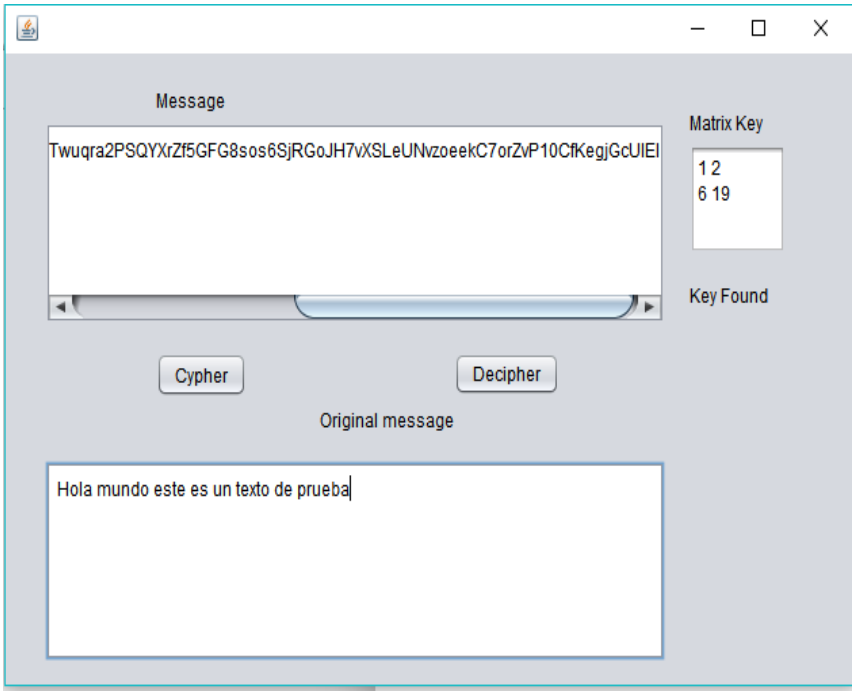

Fig. 10. Window with a test executed.

Enter the encrypted text in the central text box, the possible keys are generated in the upper left corner, after that in the lower text input box, the decrypted text will be displayed after having the correct key.

Test executed in 346800 milliseconds corresponding to 5.78 minutes which is the total time it takes to find the key and decrypt the text with a 2x2 matrix.

5 Conclusions

This article shows how to take advantage of the parallelism to find a correct key in the deciphering process through brute force into an algorithm. This test was developed with a 2x2 matrix considering integers numbers from 1 to 256 however this case is one of the best since the algorithm can be applied to a square matrix of n * n the decryption process can grow exponentially in time if the size of the matrix is not known or even the set of values used in each element.

References

1. Granados, P.G.: Introducción a la criptografía. Digital University Journal, 7 (2006)
2. López, J.: 5 hackeos que sacudieron a empresas en 2014. http://www.elfinanciero.com.mx/tech/hackeos-que-sacudieron-a-empresas-en-2014.html
3. Castañeda, C.B. Caballero, G.P.: Sistemas criptográficos de sustitución. Didactic Mathematics magazine, 30, 15–30 (1997)
4. Lester S.H.: Cryptography in an Algebraic Alphabet. The American Mathematical Monthly, 36(6) 306–312 (1929)
5. Sánchez-Rinza, B.E., Garcia-Ramirez, J., Rossainz, M.: Decodificación de texto en español utilizando frecuencias de palabras mediante cómputo paralelo. IEEE Computer society, 16, 1–6 (2018)
6. Rossainz, M., Capel, M.I., Sánchez-Rinza, B.E.: Uso de objetos paralelos para la decodificación de texto mediante frecuencias de palabras. Avances en arquitectura y tecnología de computadores, 19–28 (2018)