HPU2 Journal of Sciences:
Natural Sciences and Technology

journal homepage: https://sj.hpu2.edu.vn

Article type: Research article

Applications of linear algebra in encryption

Thanh-Giang Nguyen Thi*

University of Information and Communication Technology, Thai Nguyen University, Thai Nguyen, Vietnam

Abstract

Information security is always a crucial issue in the continuously developing society. There are many solutions that have been proposed to secure information. In this article, the author discusses the introduction of encryption using knowledge from the Linear Algebra course to first-year students so that they can perceive the application of Linear Algebra. The information encryption process uses the knowledge of matrices, matrix operations, inverse matrices, transposition, Gauss elimination, linear transformation……..

Keywords: information security, encryption, encryption methods, linear algebra applications

1. Introduction

The study of secret messaging encryption and decryption is called cryptography. Although secret codes have existed since the early days of text communication, there has been an increasing interest in the topic due to the demand to maintain the confidentiality of information transmitted over public communication channels. In the cryptography language, the code is called cipher, the unencrypted message is called the plaintext and the encrypted message is called the ciphertext. The process of converting the plaintext into ciphertext is called encryption and the reverse process is called decryption.

The simplest encryption technique is the substitution encryption. It involves replacing each letter in the alphabet with another letter or number. For example, replace “a” with “m” and “b” with “k”..... The drawback of this type of encryption is that it preserves the frequency of individual letters, making it easy to break the codes using simple statistical methods [12].

The solution to the above mentioned problem is to group letters in the plaintext and encrypt by

* Corresponding author, E-mail: nttgiang@ictu.edu.vn

https://doi.org/10.56764/hpu2.jos.2023.1.2.46-52

Received date: 05-4-2023 ; Revised date: 24-4-2023 ; Accepted date: 25-4-2023

group instead of individual letters. A cryptosystem in which the plaintext is divided into sets of n letters, and each set is replaced with a set of n cipher letters is called a multitextual system. In this section, the author studies a class of polygraph systems based on matrix transformation. In this case, inverse matrices can be used to provide better substitution encryption [6].

2. The study

2.1. Encryption process

First, associate a number with a letter in the alphabet. For example, using the following conversion table:

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

Table 1.

In this simplest encryption technique, the plaintext is converted into the ciphertext by the following procedure:

Step 11: Select a 3x3 square matrix with integer values.

$$A=\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}$$

to perform the encryption. We add some additional conditions for the matrix A to be applicable as follows:

Step 2: We group consecutive letters in the original text into groups of three letters, and add any arbitrary "fake" letters to the last group if it has less than three letters. Then, we replace each letter in the plaintext with its corresponding numerical value from Table 1.

Step 3: Convert each of the above groups of three letters into a column vector one by one.

$$P=\begin{bmatrix} p_1 \\ p_2 \\ p_3 \end{bmatrix}$$

and perform the calculation AP. We call P the plaintext vector and AP the corresponding ciphertext vector.

Step 4: Convert the ciphertext vector into its equivalent letters according to Table 1.

However, when dealing with values that exceed 25, there may be no corresponding letter in Table 1. To solve this problem, we will do as follows: when the resulting number is greater than 25, we will replace it with the remainder obtained by dividing this integer by 26. This is because the remainder after dividing by 26 is one of the integers 0, 1, ..., 25. Then, the result will be a single integer that corresponds to a letter in Table 1 [1], [2].

The above procedure is shown for n=3. It can be performed for any general case of n. In this case,

the matrix A is an n x n matrix, and the relevant knowledge will be applied to the corresponding rank matrix.

However, when dealing with values that exceed 25, there may be no corresponding letter in Table 1. To solve this problem, we will do as follows: when the resulting number is greater than 25, we will replace it with the remainder obtained by dividing this integer by 26. This is because the remainder after dividing by 26 is one of the integers 0, 1, ..., 25. Then, the result will be a single integer that corresponds to a letter in Table 1 [1], [2].

The above procedure is shown for n=3. It can be performed for any general case of n. In this case, the matrix A is an n x n matrix, and the relevant knowledge will be applied to the corresponding rank matrix.

2.2. Some linear algebra knowledge used in decryption [10]

Matrix: a matrix is a table of numbers consisting of m rows and n columns, denoted as the mxn matrix, represented by symbol $\boldsymbol{[a_{ij}]_{m\times n}}$

$$A=\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$$

Each number a_{ij} s called the element row *i* column *j* of matrix A. When $m = n$, we call A the square matrix of order *n*.

Transposition matrix: the transposition matrix of $A = [a_{ij}]_{m\times n}$, denoted as A^T is the matrix n $[a_{ji}]_{n\times m}$ obtained from A by converting columns into rows or vice versa.

Matrix operations:

Matrix addition: Given two matrices of the same size $\boldsymbol{A = [a_{ij}]_{m\times n}}$, $\boldsymbol{B = [b_{ij}]_{m\times n}}$.The sum of the two matrices, denoted as $A+B$, is the $m\times n$ matrix defined by $A+B=\left[a_{ij}+b_{ij}\right]_{m\times n}$.

Scalar multiplication: Given the matrix $A=\left[a_{ij}\right]_{m\times n}$ and a number $\lambda\in\mathbb{R}$. The product of λ and *A*, denoted as λA, is the matrix of size $m\times n$ defined by $\left[\lambda a_{ij}\right]_{m\times n}$.

Matrix multiplication: Given $A=\left[a_{ik}\right]_{m\times p}$, $B=\left[b_{kj}\right]_{p\times n}$. The product of *A* and *B*, denote as *AB*, is the matrix *C* size $m\times n$ defined by

$$c_{ij}=\sum_{k=1}^{p}a_{ik}b_{kj},\ \forall i=1...m,\ j=1...n$$

.

2.3. Use of Linear Algebra in decryption

Given the process of encryption presented in section (2.1) together with the knowledge of linear algebra, we can encode information into specific data by analyzing it as follows. [12]:

Assume that $n=3$ we choose any matrix *A*, *let's say we choose as follows:*

$$A = \begin{bmatrix} 0 & 2 & -1 \\ 1 & -2 & 1 \\ -1 & -1 & 1 \end{bmatrix}$$

We have the inversion of matrix A as:

$$A^{-1} = \begin{bmatrix} 1 & 1 & 0 \\ 2 & 1 & 1 \\ 3 & 2 & 2 \end{bmatrix}$$

Assuming that the data communicated between the two parties is the conversion table (Table 1) and the matrix A. When a party wants to send a message, it needs to convert it into a sequence of numbers. The second step is to divide this sequence into groups of 3, then multiply each group with the matrix A to create new groups and build a new sequence of numbers. Then, send the resulting sequence as a string of numbers or letters. The receiving party performs the decoding by dividing the sequence into groups of 3, multiplying with i A^{-1} and finally converting it into letters.

Example 1: Assuming that you want to encrypt and send the following message: "HỌC ĐẠI SỐ TUYẾN TÍNH".

First, use the conversion table, find the corresponding numbers which associate with each letter in "HỌC ĐẠI SỐ TUYẾN TÍNH"

we have the following sequence:

8 15 3 4 1 9 19 15 20 21 25 5 14 20 9 14 8

Then, divide the above sequence into groups of three and write each group as a 3x1. Since the last group may have less than 3 digits, we add an arbitrary fake character in the plaintext. Let's assume we add the letter "G". Then, we get the following character sequence:

HỌC ĐẠI SỐ TUYẾN TÍNH

And the corresponding sequence of numbers is:

8 15 3 4 1 9 19 15 20 21 25 5 14 20 9 14 8 7

At this point, we have the following vectors:

$$\begin{bmatrix} 8 \\ 15 \\ 3 \end{bmatrix} \begin{bmatrix} 4 \\ 1 \\ 9 \end{bmatrix} \begin{bmatrix} 19 \\ 15 \\ 20 \end{bmatrix} \begin{bmatrix} 21 \\ 25 \\ 5 \end{bmatrix} \begin{bmatrix} 14 \\ 20 \\ 9 \end{bmatrix} \begin{bmatrix} 14 \\ 8 \\ 7 \end{bmatrix}$$

Next, multiply *A* with the above vectors, we have the following vectors:

$$\begin{bmatrix} 27 \\ -35 \\ -20 \end{bmatrix} \begin{bmatrix} -7 \\ 3 \\ 4 \end{bmatrix} \begin{bmatrix} 10 \\ -29 \\ -14 \end{bmatrix} \begin{bmatrix} 45 \\ -66 \\ -41 \end{bmatrix} \begin{bmatrix} 31 \\ -45 \\ -25 \end{bmatrix} \begin{bmatrix} 9 \\ -23 \\ -15 \end{bmatrix}$$

This will give us the sequence of numbers that we can send.

27 -35 -20 -7 3 4 10 -29 -14 45 -66 -41 31 -45 -25 9 -23 -15

The receiving party will divide it into groups of 3 and create vectors, then multiply each vector with A^{-1}. After obtaining a sequence of numbers, we use the conversion table to convert the number sequence into letters and we will have the decrypted message.

How to decrypt?

The above discussed encryption and decryption techniques use inverse matrices to perform linear transformation. The purpose of cipher is to find a safe way of communication to prevent unauthorized entities from understanding the content of the message. Therefore, with each type of encryption, one of the necessary questions to be asked is how much information is needed to decode? Since we use linear transformations to encode and decode when using matrices, we need to understand their attributes. We know that any linear transformation $L:V\to W$ is absolutely defined by the graph of a basis *V* [10]. Thus, if *A* is a matrix size nxn, we need to know *n* vectors $P_1,P_2,...,P_n$ in the plaintext and the vectors in the ciphertext (encrypted) $AP_1,AP_2,...,AP_n$ to decrypt. Decryption means we obtain the matrix A^{-1}. To do this, we need a matrix *P*

$$P=\left[P_1\middle|P_2\middle|...\middle|P_n\right]$$

with the columns being the vectors in the plaintext

$$P_1,P_2,...,P_n$$

and a matrix

$$Q=\left[AP_1\middle|AP_2\middle|...\middle|AP_n\right]$$

Therefore, $Q=AP$ and $A^{-1}=PQ^{-1}$. This will provide us a tool to decode the message. We perform on the rows to find A^{-1}, we can write $A^{-1}=PQ^{-1}$ or $A^{-1}Q=P$ or $Q^T\left(A^{-1}\right)^T=P^T$. To obtain A^{-1}, first we need to find $\left(A^{-1}\right)^T$, by using Gaussian elimination $\left[Q^T\middle|P^T\right]$ into $\left[I\middle|\left(A^{-1}\right)^T\right]$.

Example 2: Assuming that we receive the message:

LU PO ZM AE AE GI UA BJ

Use the conversion table to convert the above sequence into:

12 21 16 15 0 13 1 5 1 5 7 9 22 1 2 10

Or the sequence (the remainder after divided by 26),

12 47 16 67 52 65 27 83 79 135 33 113 48 53 80 140

Assuming we don't remember matrix *A* or A^{-1}. However, we know the fifth to eighth letters in the plaintext are GOOD, then how do we find the plaintext?

Since we know the letters GOOD, we can find the numbers corresponding with these letters, namely 7 15 for GO and 15 4 for OD. We also know that the numbers corresponding to the fifth to eighth letters in the encrypted message are 52 65 for ZM and 27 83 for AE. Consequently, we can create matrices *P* and *Q*.

$$p_1=\begin{bmatrix}7\\15\end{bmatrix}\leftrightarrow c_1=\begin{bmatrix}52\\65\end{bmatrix};\ p_1=\begin{bmatrix}15\\4\end{bmatrix}\leftrightarrow c_1=\begin{bmatrix}27\\83\end{bmatrix}$$

We can create

$$Q^T = \begin{bmatrix} c_1^T \\ c_2^T \end{bmatrix} = \begin{bmatrix} 52 & 65 \\ 27 & 83 \end{bmatrix}$$ và $$P^T = \begin{bmatrix} p_1^T \\ p_2^T \end{bmatrix} = \begin{bmatrix} 7 & 15 \\ 15 & 4 \end{bmatrix}$$

Create matrix $\left[Q^T \middle| P^T\right]$ and use the Gaussian elimination to demote Q^T to an identity matrix, matrix $\left[Q^T \middle| P^T\right]$ is converted to $\left[I \middle| \left(A^{-1}\right)^T\right]$. Then:

$$\begin{bmatrix} 52 & 65 & 7 & 15 \\ 27 & 83 & 15 & 4 \end{bmatrix}$$

will become matrix

$$\begin{bmatrix} 1 & 0 & -2/13 & 5/13 \\ 0 & 1 & 3/13 & -1/13 \end{bmatrix}$$

because matrix $\begin{bmatrix} -2/13 & 5/13 \\ 3/13 & -1/13 \end{bmatrix}$ is the transposition of matrix A^{-1}, so we need to transpose this matrix to obtain A^{-1}.

hence

$$A^{-1} = \begin{bmatrix} -2/13 & 3/13 \\ 5/13 & -1/13 \end{bmatrix}$$

Receiving a secret message with A^{-1}, we will have the sequence of numbers

9 1 13 1 7 15 15 4 19 20 21 4 5 14 20 20

Using the conversion table, we find the corresponding letters: IAMAGOODSTUDENT. This provides us with the message: “I AM A GOOD STUDENT”

3. Conclusion

The article has presented the encryption technique which involves the use of the knowledge of linear algebra in order that students realize the application of the learnt knowledge in practice and have a broader view of the course.

References

[1]. Lester S. Hill “*Cryptography in an Algebraic Alphabet*,” American Mathematical Monthly, *36* (June– July 1929), pp. 306–312;

[2]. Lester S. Hill “*Concerning Certain Linear Transformation Apparatus of Cryptography*,” American Mathematical Monthly, *38* (March 1931), pp. 135–154.).

[3]. Howard Anton, Chris Rorres “*Elementary linear algebra*”, copyrighted Material (2005).

[4]. V. Levenshtein, *Application of Hadamard matrices to one problem of coding theory*, Problemy Kibernetiki 5, (1961), 123–136.

[5]. R. Lidl and H. Niederreiter, *Finite Fields, Addison-Wesley, Reading*, MA (1983); now distributed by Cambridge University Press.

[6]. Raymond Hill, (1993). "*A First Course in Coding Theory*", Clarendon Press, Oxrord, USA. ISBN : 0-19-853803-0.

[7]. Yehuda Lindell, “*Introduction to Coding Theory*”, Lecture Notes, Department of Computer Science Bar-Ilan University , Israel (2010).

[8]. Tom Richardson, Rudiger Urbanke. "*Modern Coding Theory*". Cambridge University Press (2008).

[9]. Đặng Văn Chuyết, Nguyễn Tuấn Anh.(1998)"*Basic Communication Theory*". Education publishing House.

[10]. Phạm Huy Điển, Hà Huy Khoái, *Encryption. Mathematical Foundations & Applications*, VNU Publishing House, 2004.

[11]. Đặng Văn Chuyết, Nguyễn Tuấn Anh, *Basic Information Theory (books 1 & 2)*, Education Publishing House, 1998.

[12]. Nguyễn Thúy Vân, *Cipher Theory*, Science and Technics Publishing House, 2000.