The Art of Cryptography

Ismail Kably & Duc Phan

Portland Community College

June 10, 2018

Summary

This paper seeks to discuss cryptography and how it works through some examples

1 What is cryptography?

Cryptography or cryptology is the practice and study of techniques for secure communication in the presence of third parties called adversaries. Cryptography is associated with the process of converting ordinary plain text into unintelligible text and vice-versa. It is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it.

Cryptography not only protects data from theft or alteration, but can also be used for user authentication. More generally, cryptography is about constructing and analyzing protocols that prevent third parties or the public from reading private messages.

2 Why Linear Algebra?

Cryptography exists in many forms, some use Number Theories, some use Linear Algebra. However, because the type of encryption discussed in this paper use the Math behind matrices, the knowledge of Linear Algebra is required.

Even though the algorithms to implement encryption can become very complicated, the general idea is easy to understand. Cryptography can as simple as using a 3x3 matrix composed of random integers that represent the characters in the plain-text to encrypt the text.

3 A simple example of Encryption

In this example, we will try to encrypt the word "MATH." There are various ways to achieve the goal, but this example, we will use a very simple type of cryptography.

The process consists of three steps:

1. Convert the word "MATH" into a plain-text matrix.
2. Encrypt the plain-text matrix.
3. Decrypt the encrypted matrix.

3.1 Conversion

Each character in plain-text must be denoted with a numerical value and placed into a matrix. The numerical rules can vary as long as they are consistent throughout the process.

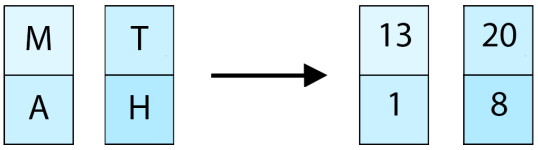
In this example, we will use the numerical rule shown below:

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	26

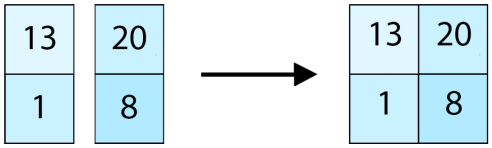
First, each letter will be used as entries of vectors to put into the matrix, such that:

1. The number of entries of each vector is equivalent to the number of rows of the cipher matrix (which will be discusses later).
2. Letters are placed one at a time, going down a row for each value.
3. Vectors are filled one to another.
4. The remaining empty entries in the last vector is filled with space.

Afterward, the characters in the vectors are then converted into their corresponding numerical values using the rule above.



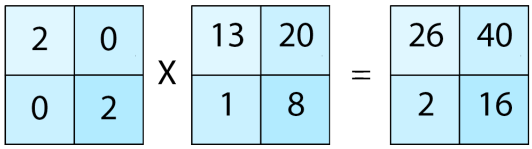
Finally, the vectors are augmented to form the plain-text matrix.



3.2 Encryption

In this method, we will use a matrix called cipher-matrix for the encryption step.
The cipher matrix's values can be randomly generated as long as it is invertible, but its size is fixed beforehand.

To make it easy, we will use a 2x2 matrix.
The cipher matrix will then be used to multiply with the plain-text matrix as shown below:



We can keep adding more steps for the encryption process to enhance the security, but doing so will greatly increase the complexity of the algorithm with the cost of performance.
To keep it simple, we'll stop in this step for this example. Thus, the product is called the encrypted matrix.

3.3 Decryption

After the encryption is completed, the encrypted and the cipher matrix will be sent to the recipient. In order to read the message, the recipient needs to go through the process of decryption, which - in this case - will be the encryption process in reverse. Since the sending process is out of topic, it will not be discussed in this paper.

Let's take a look at this logic:

$$\begin{aligned} & C \times P && = && E \\ \iff & C^{-1} \times C \times P && = && C^{-1} \times E \\ \iff & P && = && C^{-1} \times E \end{aligned}$$

where C is the cipher matrix, P is the plain-text matrix and E is the encrypted matrix.

Because the encrypted matrix was found using the multiplication between the cipher matrix and the plain-text matrix where the cipher matrix is on the left side of the plain-text matrix - since the recipient is given the cipher matrix and the encrypted matrix - the plain-text matrix can be found using the multiplication of the inverse of the cipher matrix and the encrypted matrix.

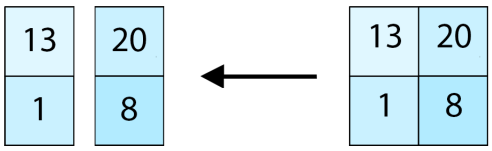
First, we can find the inverse using the sledgehammer given by our teacher, Mr. Damien!

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

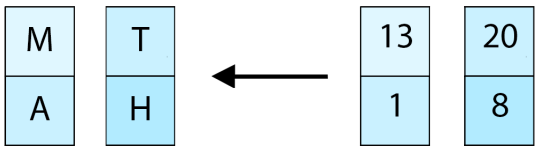
The inverted matrix is then multiplied with the cipher-text matrix (which will be on the left side). The product is the original plain-text matrix.

$$\begin{bmatrix} 1/2 & 0 \\ 0 & 1/2 \end{bmatrix} \times \begin{bmatrix} 26 & 40 \\ 2 & 16 \end{bmatrix} = \begin{bmatrix} 13 & 20 \\ 1 & 8 \end{bmatrix}$$

Afterward, we need to convert the matrix into the original message.
First, we need to split the columns of the decrypted matrix into vectors.



Then, using the same numerical values to convert each character into the original message vectors.



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	26

Each character in the vectors are then taken out to form the original message, from left to right, from top to bottom.

Finally, we successfully decrypt the word "MATH"!

References

[1] Write the author of the book here, *Write the title of the book here*, Write the publisher of the book here, Write the year the book was published here.

[2] etc., *If you use another book, do the same thing as before.*
https://economictimes.indiatimes.com/definition/cryptography