Cryptography and the World of the Mystery

Ismail Kably & Duc Phan

June 4, 2018

Table of Contents

What we are going to do?

Let's explore the world of encryption!

What is cryptography?

a. Cryptography or cryptology is the practice and study of techniques for secure communication in the presence of third parties called adversaries.

b. More generally, cryptography is about constructing and analyzing protocols that prevent third parties or the public from reading private messages.

The link between Linear Algebra and Encryption

Because many types of encryption Matrix use the Math behind matrices to encrypt, Linear Algebra is required for Encryption and Decryption!

Is it complicated?

a. The idea behind encryption is not hard to understand at all!

b. Cipher matrix can be as simple as a 3x3 matrix composed of random integers that represent the characters in the plain-text.

A simple encryption method

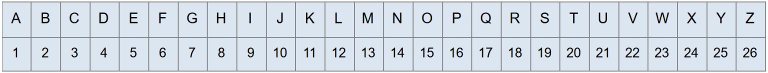
Let's take a look at a simple encryption type :D

The general Idea

1. Convert a plain-text to a matrix
2. Encrypt the matrix
3. Decrypt the encrypted matrix

Plain-text to Matrix

Each **character** in plain-text must be denoted with a **numerical value** and placed into a matrix.

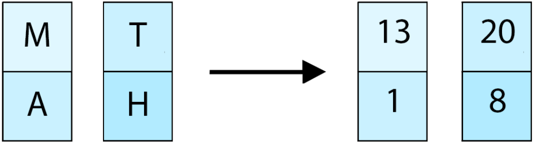


A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Plain-text to Matrix

The **numerical values** are then separated into **vectors**, such that:

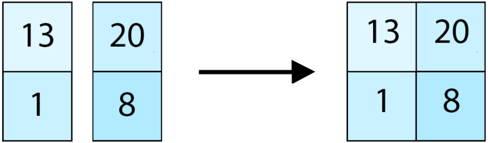
a. The number of **rows** of each **vector** is equivalent to the numbers of rows of the **cipher matrix**.
b. **Values** are placed **one at a time**, **going down** a row for each value.
c. Vectors are filled **one to another**.
d. The remaining **empty entries** in the **last vector** is filled with **space**.



$$\begin{bmatrix} M \\ A \end{bmatrix} \begin{bmatrix} T \\ H \end{bmatrix} \longrightarrow \begin{bmatrix} 13 \\ 1 \end{bmatrix} \begin{bmatrix} 20 \\ 8 \end{bmatrix}$$

Plain-text to Matrix

The vectors are then **augmented** to form a **plain-text matrix**.



$$\begin{bmatrix}13\\1\end{bmatrix}\ \begin{bmatrix}20\\8\end{bmatrix}\longrightarrow\begin{bmatrix}13&20\\1&8\end{bmatrix}$$

Encrypting the matrix

The plain-text matrix is then **multiplied** by another **cipher-matrix** to create the **encrypted matrix**.

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

Decrypting the matrix

First, we need to find the **inverse** of the **cipher-matrix**.

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

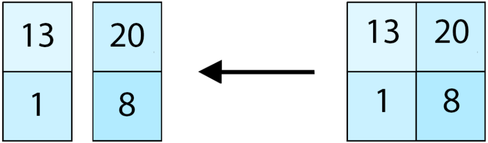
Decrypting the matrix

The **inverted matrix** is then **multiplied** with the **cipher-text matrix**. The **product** is the original **plain-text matrix**.

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

Decrypting the matrix

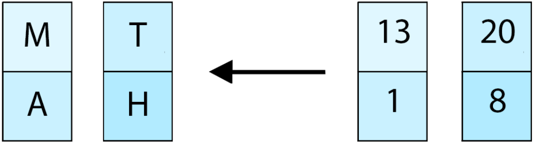
The **plain-text** can be found by **splitting** the **products** into **vectors**



$$\begin{bmatrix}13\\1\end{bmatrix}\quad\begin{bmatrix}20\\8\end{bmatrix}\longleftarrow\begin{bmatrix}13&20\\1&8\end{bmatrix}$$

Decrypting the matrix

And then use the **numerical rules** to convert the **numbers** back into their **letter forms**.



$$\begin{bmatrix} M & T \\ A & H \end{bmatrix} \longleftarrow \begin{bmatrix} 13 & 20 \\ 1 & 8 \end{bmatrix}$$

More advanced encryption

Let's take a look at AES, a more secure encryption type!