

Cryptography and the World of the Mystery

Ismail Kably & Duc Phan

June 4, 2018

Table of Contents

Cryptography
and the World
of the Mystery

Ismail Kably
& Duc Phan

Introduction

What is
Cryptography

How does
Linear Algebra
and
Encryption
connected?

The
fundamental
example of
Encryption

AES -
Advanced
Encryption
Standard

Conclusion

1 Introduction

2 What is Cryptography

3 How does Linear Algebra and Encryption connected?

4 The fundamental example of Encryption

5 AES - Advanced Encryption Standard

6 Conclusion

What we are going to do?

Cryptography
and the World
of the Mystery

Ismail Kably
& Duc Phan

Introduction

What is
Cryptography

How does
Linear Algebra
and
Encryption
connected?

The
fundamental
example of
Encryption

AES -
Advanced
Encryption
Standard

Conclusion

Let's explore the world of encryption!



What is cryptography?

Cryptography
and the World
of the Mystery

Ismail Kably
& Duc Phan

Introduction

What is
Cryptography

How does
Linear Algebra
and
Encryption
connected?

The
fundamental
example of
Encryption

AES -
Advanced
Encryption
Standard

Conclusion

- 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

Cryptography
and the World
of the Mystery

Ismail Kably
& Duc Phan

Introduction

What is
Cryptography

How does
Linear Algebra
and
Encryption
connected?

The
fundamental
example of
Encryption

AES -
Advanced
Encryption
Standard

Conclusion

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

Is it complicated?

Cryptography
and the World
of the Mystery

Ismail Kably
& Duc Phan

Introduction

What is
Cryptography

How does
Linear Algebra
and
Encryption
connected?

The
fundamental
example of
Encryption

AES -
Advanced
Encryption
Standard

Conclusion

- a. The idea behind encryption is not hard to understand at all!
- b. Cipher matrix can be as simple as a 3×3 matrix composed of random integers that represent the characters in the plain-text.

A simple encryption method

Cryptography
and the World
of the Mystery

Ismail Kably
& Duc Phan

Introduction

What is
Cryptography

How does
Linear Algebra
and
Encryption
connected?

The
fundamental
example of
Encryption

AES -
Advanced
Encryption
Standard

Conclusion

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

The general Idea

Cryptography
and the World
of the Mystery

Ismail Kably
& Duc Phan

Introduction

What is
Cryptography

How does
Linear Algebra
and
Encryption
connected?

The
fundamental
example of
Encryption

AES -
Advanced
Encryption
Standard

Conclusion

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

Plain-text to Matrix

Cryptography
and the World
of the Mystery

Ismail Kably
& Duc Phan

Introduction

What is
Cryptography

How does
Linear Algebra
and
Encryption
connected?

The
fundamental
example of
Encryption

AES -
Advanced
Encryption
Standard

Conclusion

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

Cryptography
and the World
of the Mystery

Ismail Kably
& Duc Phan

Introduction

What is
Cryptography

How does
Linear Algebra
and
Encryption
connected?

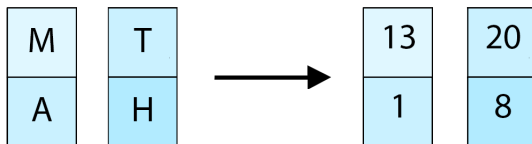
The
fundamental
example of
Encryption

AES -
Advanced
Encryption
Standard

Conclusion

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**.



Plain-text to Matrix

Cryptography
and the World
of the Mystery

Ismail Kably
& Duc Phan

Introduction

What is
Cryptography

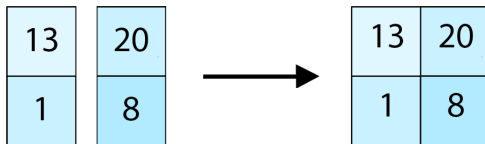
How does
Linear Algebra
and
Encryption
connected?

The
fundamental
example of
Encryption

AES -
Advanced
Encryption
Standard

Conclusion

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



Encrypting the matrix

Cryptography
and the World
of the Mystery

Ismail Kably
& Duc Phan

Introduction

What is
Cryptography

How does
Linear Algebra
and
Encryption
connected?

The
fundamental
example of
Encryption

AES -
Advanced
Encryption
Standard

Conclusion

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

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

Decrypting the matrix

Cryptography
and the World
of the Mystery

Ismail Kably
& Duc Phan

Introduction

What is
Cryptography

How does
Linear Algebra
and
Encryption
connected?

The
fundamental
example of
Encryption

AES -
Advanced
Encryption
Standard

Conclusion

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

Cryptography
and the World
of the Mystery

Ismail Kably
& Duc Phan

Introduction

What is
Cryptography

How does
Linear Algebra
and
Encryption
connected?

The
fundamental
example of
Encryption

AES -
Advanced
Encryption
Standard

Conclusion

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

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

Decrypting the matrix

Cryptography
and the World
of the Mystery

Ismail Kably
& Duc Phan

Introduction

What is
Cryptography

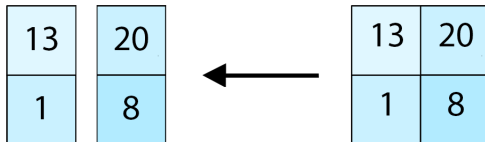
How does
Linear Algebra
and
Encryption
connected?

The
fundamental
example of
Encryption

AES -
Advanced
Encryption
Standard

Conclusion

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



Decrypting the matrix

Cryptography
and the World
of the Mystery

Ismail Kably
& Duc Phan

Introduction

What is
Cryptography

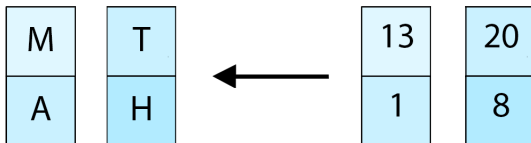
How does
Linear Algebra
and
Encryption
connected?

The
fundamental
example of
Encryption

AES -
Advanced
Encryption
Standard

Conclusion

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



More advanced encryption

Cryptography
and the World
of the Mystery

Ismail Kably
& Duc Phan

Introduction

What is
Cryptography

How does
Linear Algebra
and
Encryption
connected?

The
fundamental
example of
Encryption

**AES -
Advanced
Encryption
Standard**

Conclusion

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

AES - ...

Cryptography
and the World
of the Mystery

Ismail Kably
& Duc Phan

Introduction

What is
Cryptography

How does
Linear Algebra
and
Encryption
connected?

The
fundamental
example of
Encryption

AES -
Advanced
Encryption
Standard

Conclusion

AES - Advanced Encryption Standard - is:

- a. a symmetric encryption algorithm.
- b. very powerful.
- c. widely used in software and hardware throughout the world!

The general Process

Cryptography
and the World
of the Mystery

Ismail Kably
& Duc Phan

Introduction

What is
Cryptography

How does
Linear Algebra
and
Encryption
connected?

The
fundamental
example of
Encryption

AES -
Advanced
Encryption
Standard

Conclusion

- a. AES operates on 4×4 matrix.
- b. Each character in the plain-text is denoted with a corresponding numerical value

An example

Cryptography
and the World
of the Mystery

Ismail Kably
& Duc Phan

Introduction

What is
Cryptography

How does
Linear Algebra
and
Encryption
connected?

The
fundamental
example of
Encryption

AES -
Advanced
Encryption
Standard

Conclusion

Let's take a look at an example to understand the process

We'll encrypt and decrypt the plain-text:

"Come here I got cash"

First, let's take a look at how to encrypt the message

From text to plain-text matrix

Cryptography
and the World
of the Mystery

Ismail Kably
& Duc Phan

Introduction

What is
Cryptography

How does
Linear Algebra
and
Encryption
connected?

The
fundamental
example of
Encryption

AES -
Advanced
Encryption
Standard

Conclusion

Just like in the last example, we use the same rules to convert the text into a matrix.

$c_{0,0}$	$o_{0,1}$	$m_{0,2}$	$e_{0,3}$
$h_{1,0}$	$e_{1,1}$	$r_{1,2}$	$e_{1,3}$
$I_{2,0}$	$g_{2,1}$	$o_{2,2}$	$t_{2,3}$
$c_{3,0}$	$a_{3,1}$	$s_{3,2}$	$h_{3,3}$

Conversion Plain-text to Numerical Matrix

Cryptography
and the World
of the Mystery

Ismail Kably
& Duc Phan

Introduction

What is
Cryptography

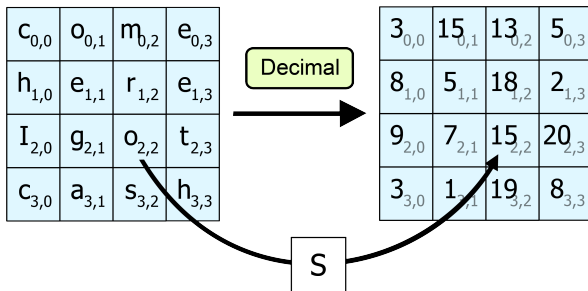
How does
Linear Algebra
and
Encryption
connected?

The
fundamental
example of
Encryption

AES -
Advanced
Encryption
Standard

Conclusion

Then, we convert the plain-text into its corresponding numerical 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

Shifting rows

Cryptography
and the World
of the Mystery

Ismail Kably
& Duc Phan

Introduction

What is
Cryptography

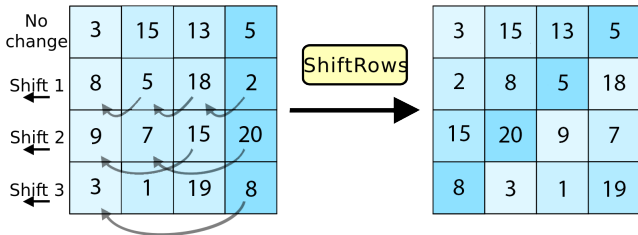
How does
Linear Algebra
and
Encryption
connected?

The
fundamental
example of
Encryption

AES -
Advanced
Encryption
Standard

Conclusion

- 1 First row is unchanged
- 2 Second row is shifted to the left 1 time
- 3 Third row is shifted to the left 2 times
- 4 Fourth row is shifted to the left 3 times



Mixing the columns

Cryptography
and the World
of the Mystery

Ismail Kably
& Duc Phan

Introduction

What is
Cryptography

How does
Linear Algebra
and
Encryption
connected?

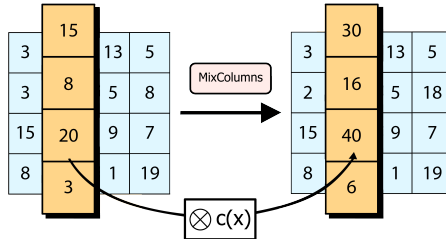
The
fundamental
example of
Encryption

AES -
Advanced
Encryption
Standard

Conclusion

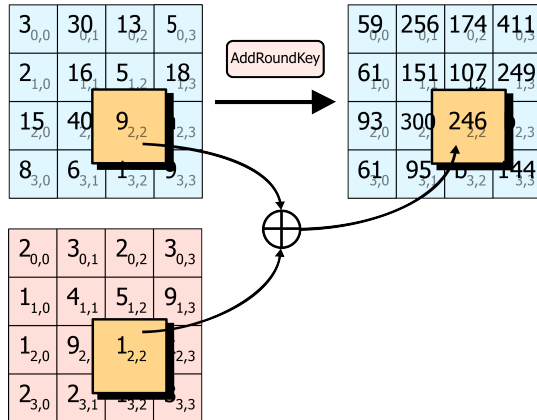
The four decimals in each column are transformed using a linear transformation

In this example, we'll scale the second column by 2



Adding round keys

We then multiply the matrix by another randomly generated invertible matrix, which is the private key



Sending and Deciphering

Cryptography
and the World
of the Mystery

Ismail Kably
& Duc Phan

Introduction

What is
Cryptography

How does
Linear Algebra
and
Encryption
connected?

The
fundamental
example of
Encryption

AES -
Advanced
Encryption
Standard

Conclusion

After encrypting the matrix, it is now secure to be sent to the recipient(s).

To decrypting, we can decipher the message using the private key that contains all the operation backward!

Conclusion

Cryptography
and the World
of the Mystery

Ismail Kably
& Duc Phan

Introduction

What is
Cryptography

How does
Linear Algebra
and
Encryption
connected?

The
fundamental
example of
Encryption

AES -
Advanced
Encryption
Standard

Conclusion

- Encryption plays an essential role in securing our private data.
- The examples use Linear Algebra to handle the Math, but there can be other methods!

Cryptography and the World of the Mystery

Ismail Kably
& Duc Phan

Introduction

What is
Cryptography

How does
Linear Algebra
and
Encryption
connected?

The
fundamental
example of
Encryption

AES -
Advanced
Encryption
Standard

Conclusion

Thank you very much for watching!