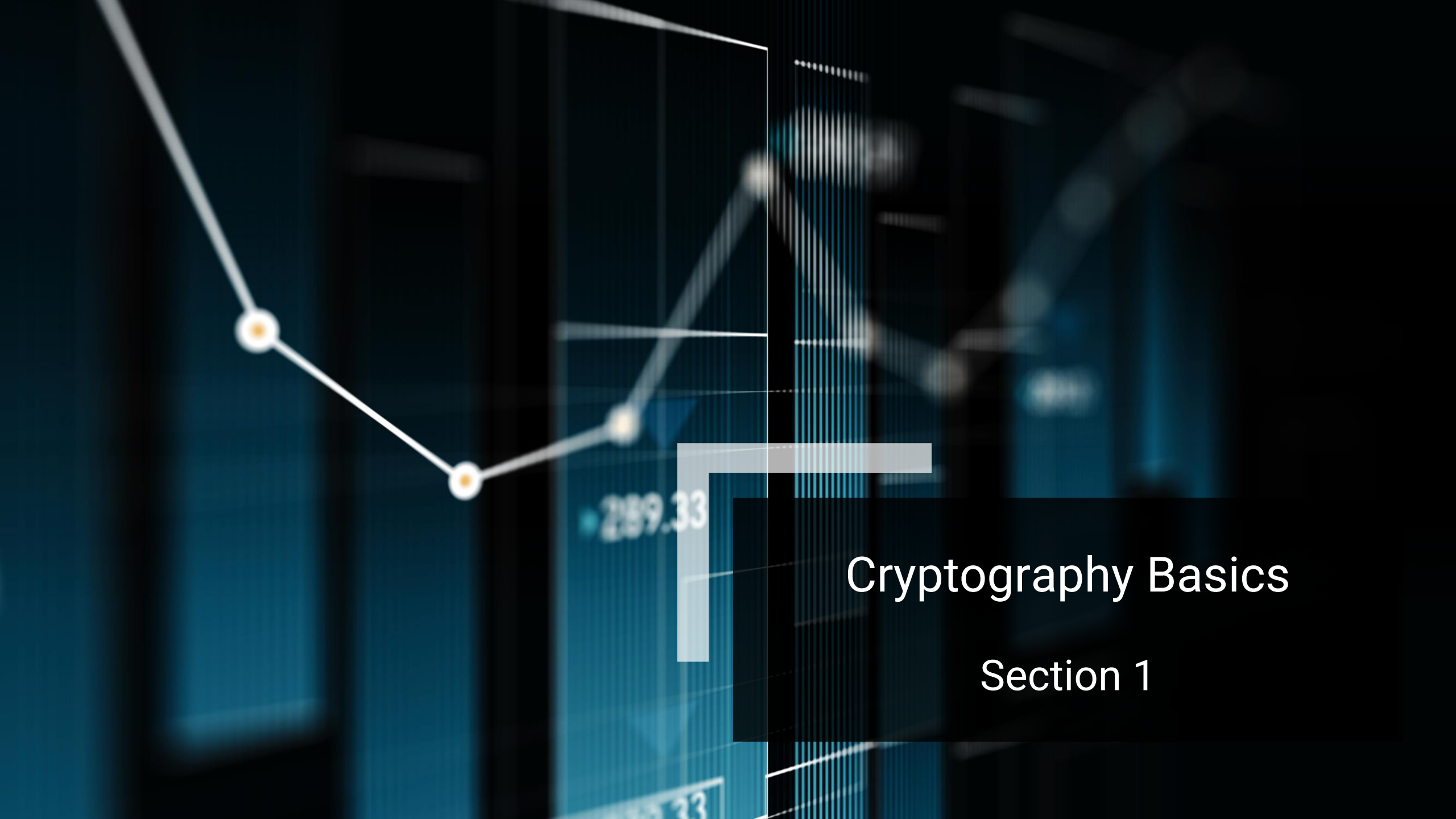
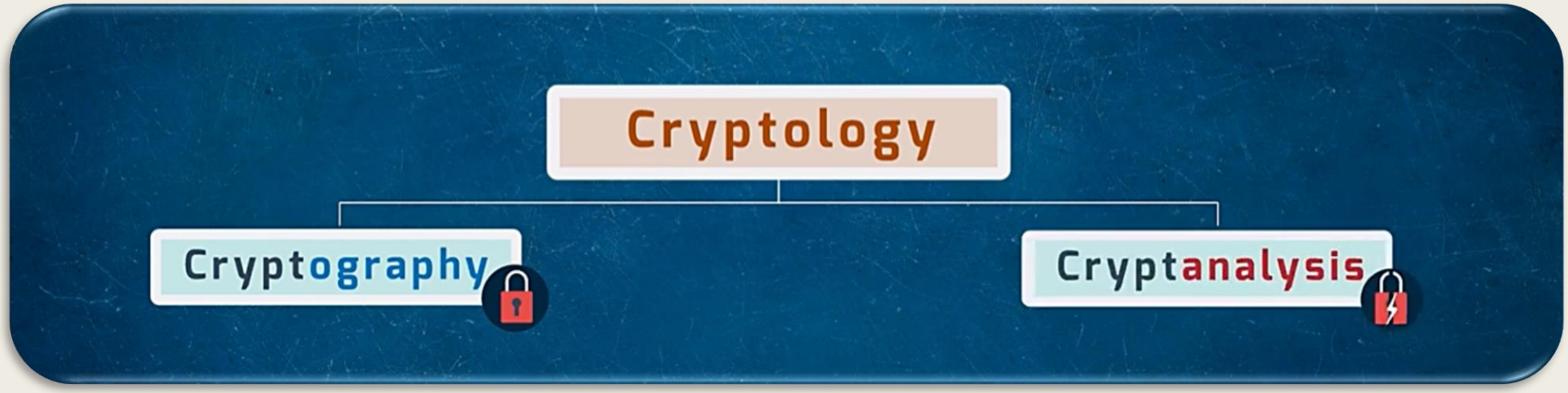


Cryptography Basics

Section 1

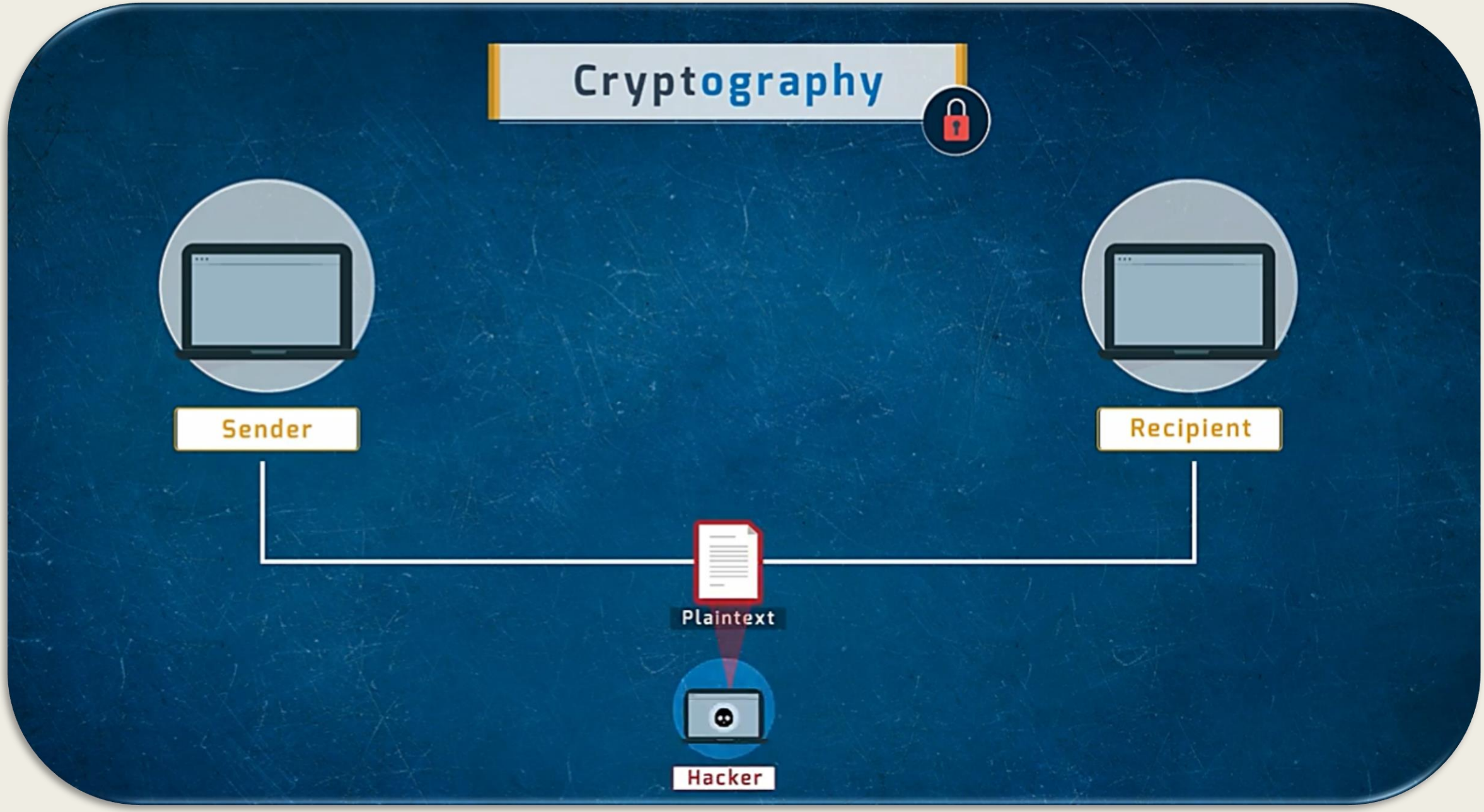
Cryptology

- *Cryptology*, the study of cryptosystems, can be subdivided into two disciplines. *Cryptography* concerns itself with the design of cryptosystems, while *cryptanalysis* studies the breaking of cryptosystems.



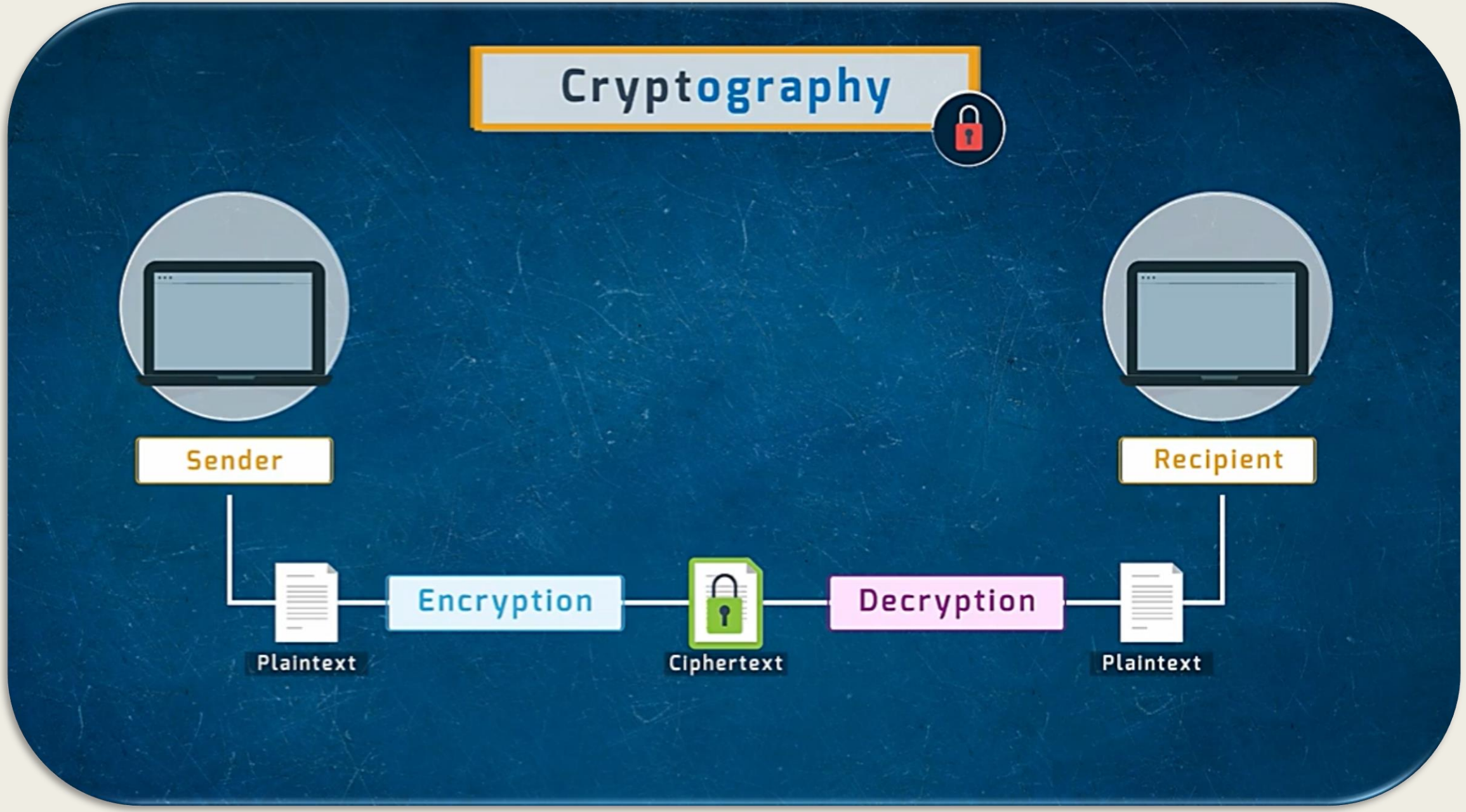
Cryptography

- *Cryptography* is the art of communication between two users via coded messages. The science of cryptography emerged with the basic motive of providing security to the confidential messages transferred from one party to another.
- *Cryptography* is defined as the art and science of concealing the message to introduce privacy and secrecy as recognized in information security.


Cryptography
Sender
Recipient
Plaintext
Hacker

Terminologies of Cryptography

- Plain Text
  - *The plain text message is the text which is readable and can be understood by all users. The plain text is the message which undergoes cryptography.*
- Cipher Text
  - *Cipher text is the message obtained after applying cryptography on plain text.*
- Encryption
  - *The process of converting plain text to cipher text is called encryption. It is also called as encoding.*
- Decryption
  - *The process of converting cipher text to plain text is called decryption. It is also termed as decoding.*

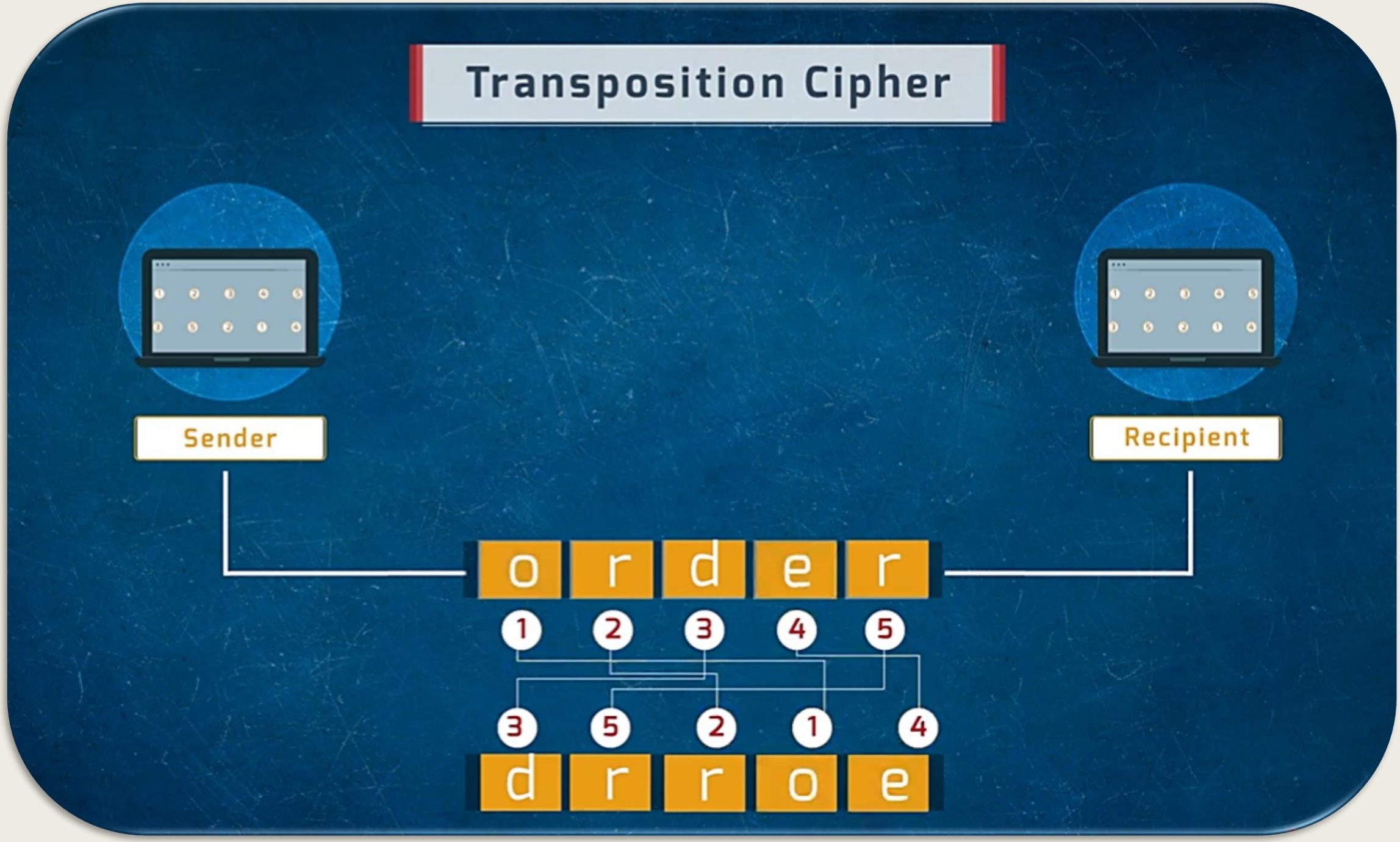

Cryptography
Sender
Recipient
Plaintext
Encryption
Ciphertext
Decryption
Plaintext

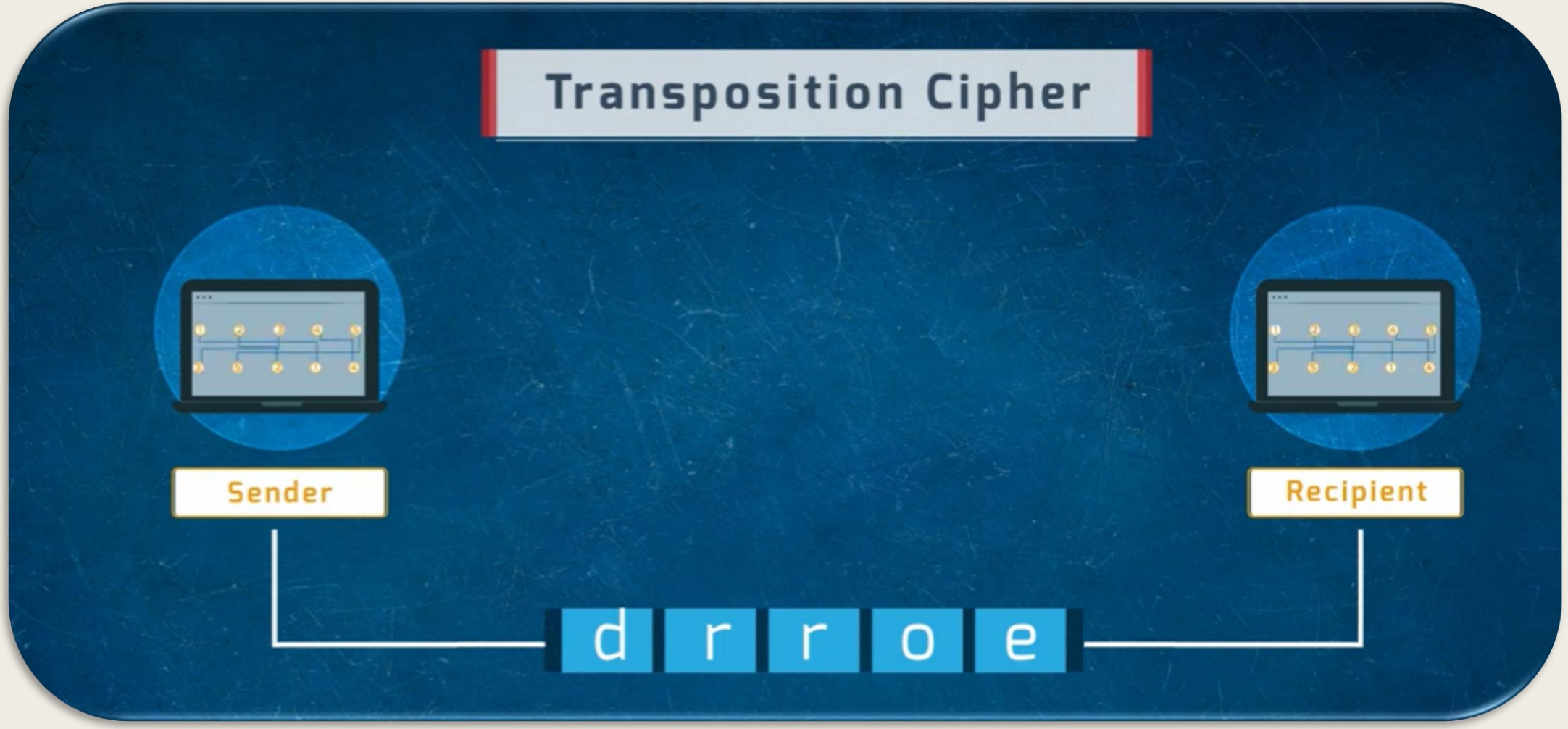
Cryptography History

- Transposition Cipher.
- Substitution Cipher.

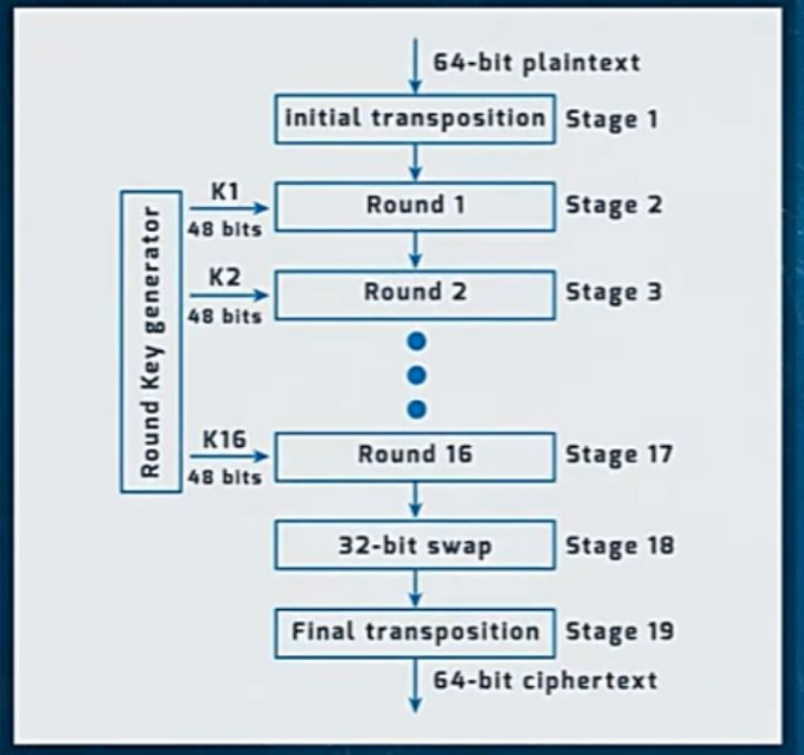
Transposition Cipher

Rearranging the plain text letters **in a new order**

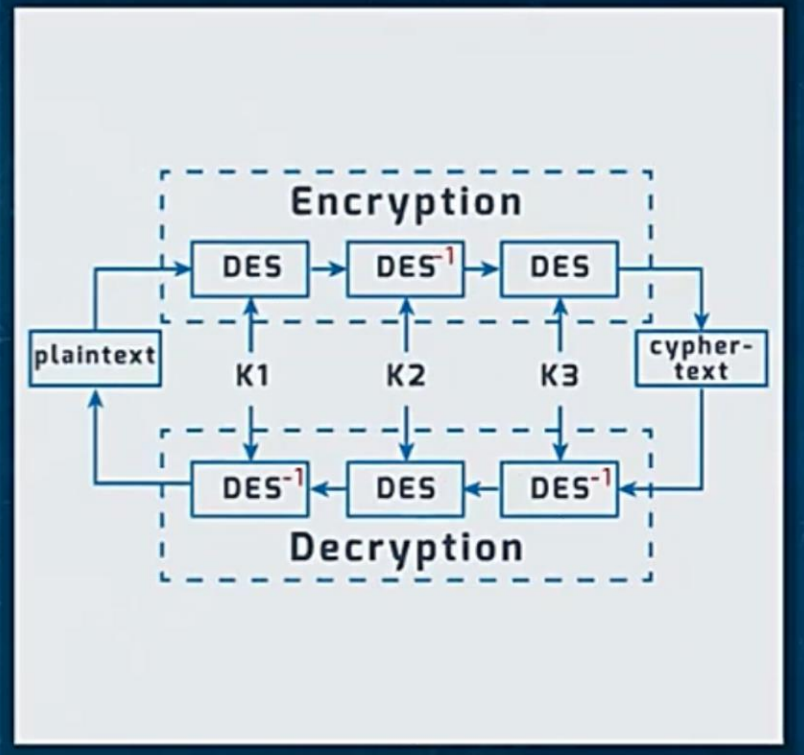

Transposition Cipher
Sender
Recipient
o r d e r
1 2 3 4 5
3 5 2 1 4
d r r o e


Transposition Cipher
Sender
Recipient
d r r o e

Transposition Cipher based algorithms



DES



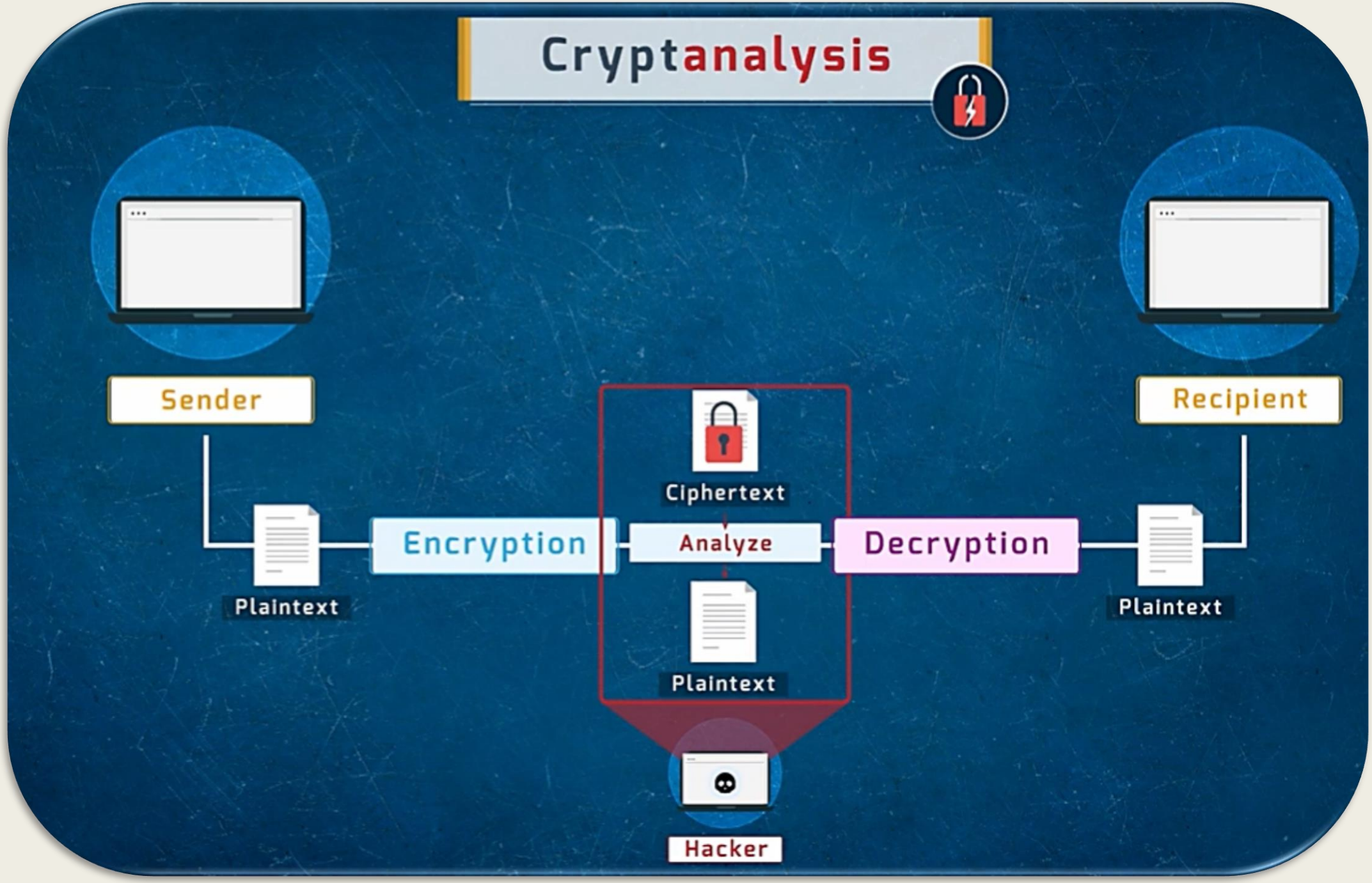
3DES

Substitution Ciphers

Shifting all the letters **a certain number** of spaces in the alphabet

Cryptanalysis

- Cryptanalysis is the decryption and analysis of codes, ciphers or encrypted text. Cryptanalysis uses mathematical formulas to search for algorithm vulnerabilities and break into cryptography or information security systems.

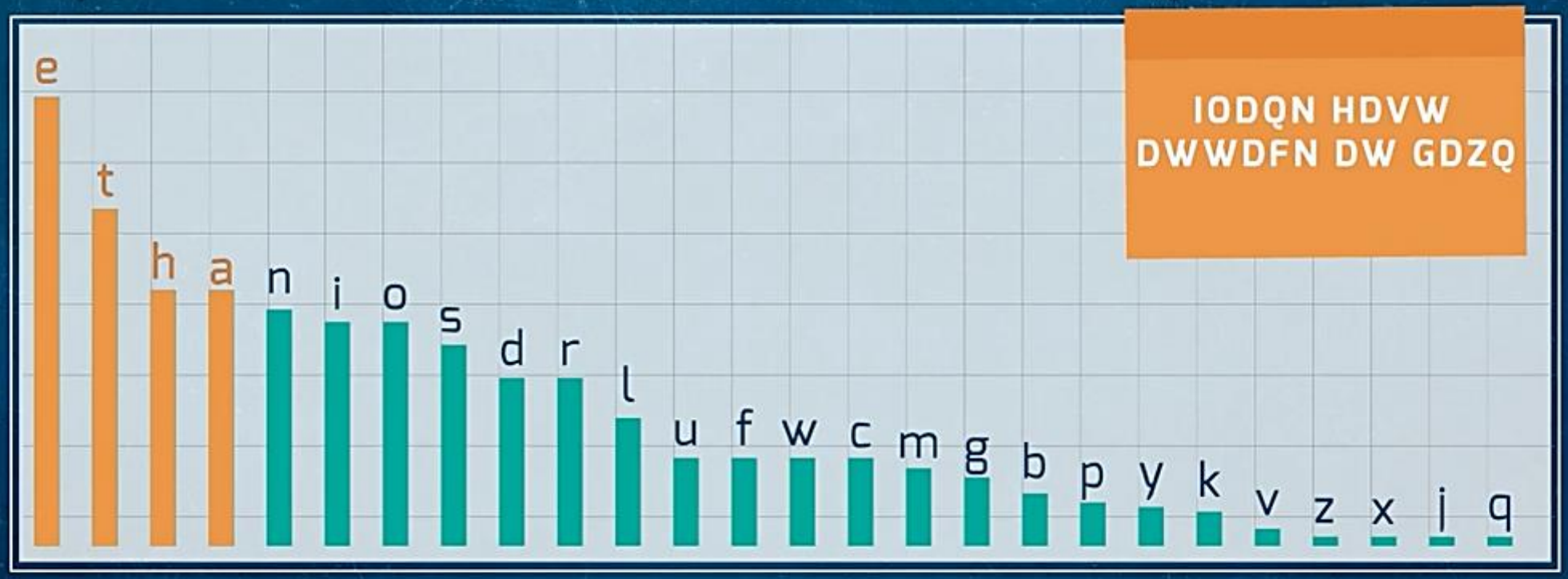

Cryptanalysis
Sender
Recipient
Ciphertext
Encryption
Analyze
Decryption
Plaintext
Plaintext
Plaintext
Hacker

Cryptanalysis Methods

1. Brute Force Attack
   - *involves trying every possible decryption key (guessing). This technique does not demand much effort and is relatively simple for a hacker.*
2. Frequency of letters in the English language
   - *(also known as counting letters) is the study of the frequency__of__letters or groups of letters in a ciphertext. The method is used as an aid to breaking classical ciphers.*

Cryptanalysis Methods

2. Frequency of letters in the English language



Cryptography with Python

Python Strings

Strings in python are surrounded by either single quotation marks, or double quotation marks:

'Hello' is the same as "Hello"

You can display a string literal with the print() function.

Example

```
print("Hello")
print('Hello')
```

String Length

To get the length of a string, use the len() function

Example

```
a = "Hello, World!"
print(len(a))   #13
```

Accessing Values in Strings

To access substrings, use the square brackets for slicing along with the index or indices to obtain your substring.

Example

Get the character at position 1 (remember that the first character has the position 0):

```
var1 = 'Hello World!’
var2 = "Python Programming"

print("var1[0]: "   + var1[0])
print("var2[1:5]: " + var2[1:5])
```

```
var1[0]: H
var2[1:5]: ytho
```

Python lists

Python Lists

The lists of python can be declared as compound data types, separated by commas and enclosed within square brackets (**[]**).

```
list = [ 'abcd', 786 , 2.23, 'john', 70.2 ]

tinylist = [123, 'john']
```

```
print("list[3]:",list[3])          #john
```

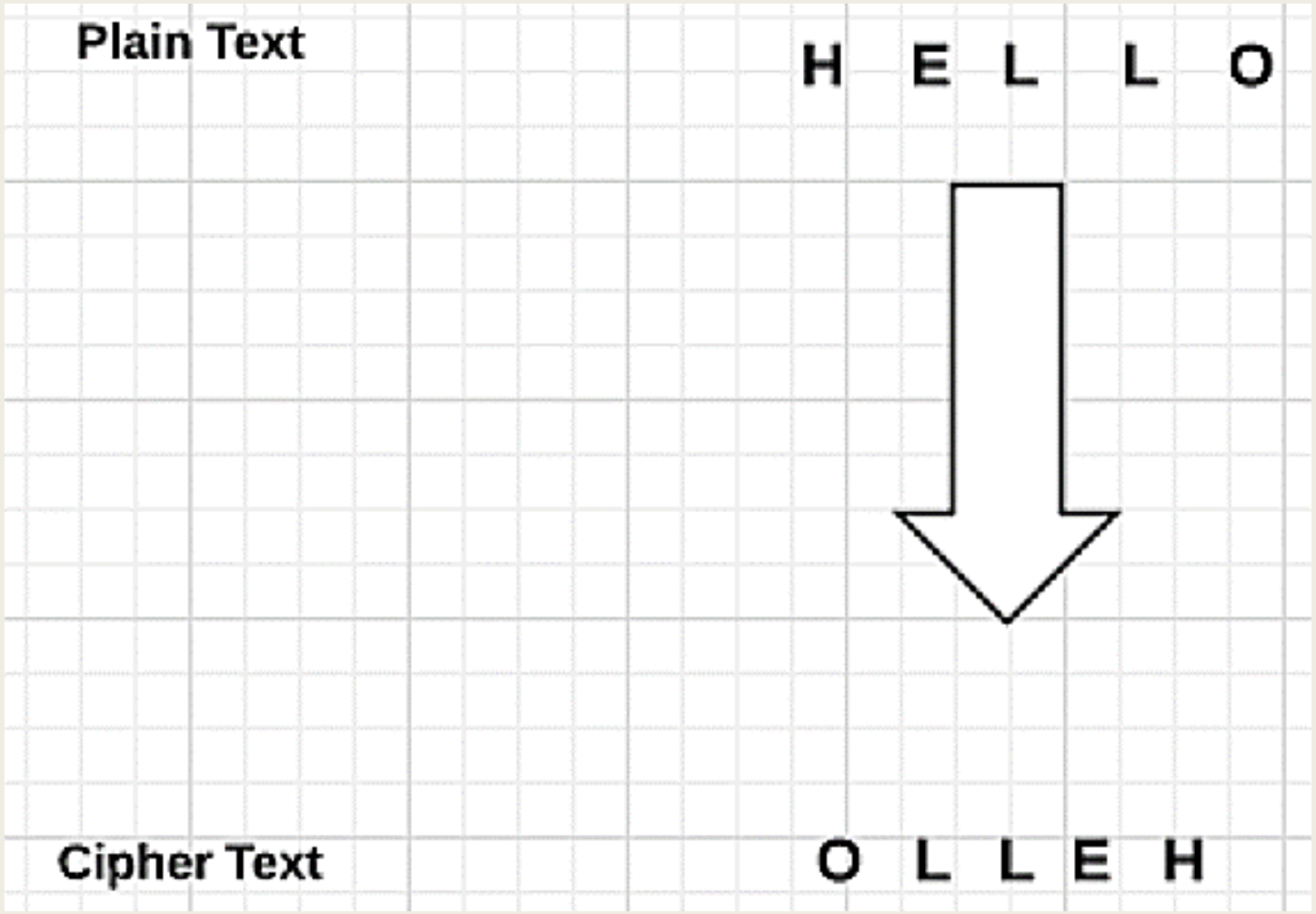
1- Reverse Cipher

Algorithm of Reverse Cipher

The algorithm of reverse cipher holds the following features:

- Reverse Cipher uses a pattern of reversing the string of plain text to convert as cipher text.
- The process of encryption and decryption is same.
- To decrypt cipher text, the user simply needs to reverse the cipher text to get the plain text.

1- Reverse Cipher



Example

Consider an example where the statement **This is program to explain reverse cipher** is to be implemented with reverse cipher algorithm. The following python code uses the algorithm to obtain the output.

```
message = 'This is program to explain reverse cipher.'
translated = ''      #cipher text is stored in this variable
i = len(message) - 1
while i >= 0:
    translated = translated + message[i]
    i = i - 1

print("The cipher text is: " + translated)
```

Output:

```
The cipher text is: .rehpic esrever nialpxe ot margorp si sihT
```


Thank
you