Cryptography - Day 1

August 10, 2020

Crypto

Secret / Hidden

Originated from a Greek word “**kruptos**”

Introduction

- Inception of Cryptography
- A brief history

Inception of Cryptography

Humans ability to Speak and Write

Communication and **Selective Communication** (Secrecy)

Use of Languages as a medium of **Obscurity**

https://bit.ly/2C9MFCk

Cryptography In Daily-Life

- CIA Triad
- Applications of Cryptography

Why is it so important ?

The CIA Triad

- **Confidentiality** - Protecting information from unauthorised access
- **Integrity** - Protecting data modification from any unauthorized party
- **Availability** - Refers to actual availability of your data

*__Non-Repudiation__ - assurance that the sender cannot deny the his actions

Application of Cryptography

- WhatsApp, Snapchat
- Time Stamping
- Electronic Money (e-Wallet, Banking System)
- Email (Not everyone)
- Cryptocurrency

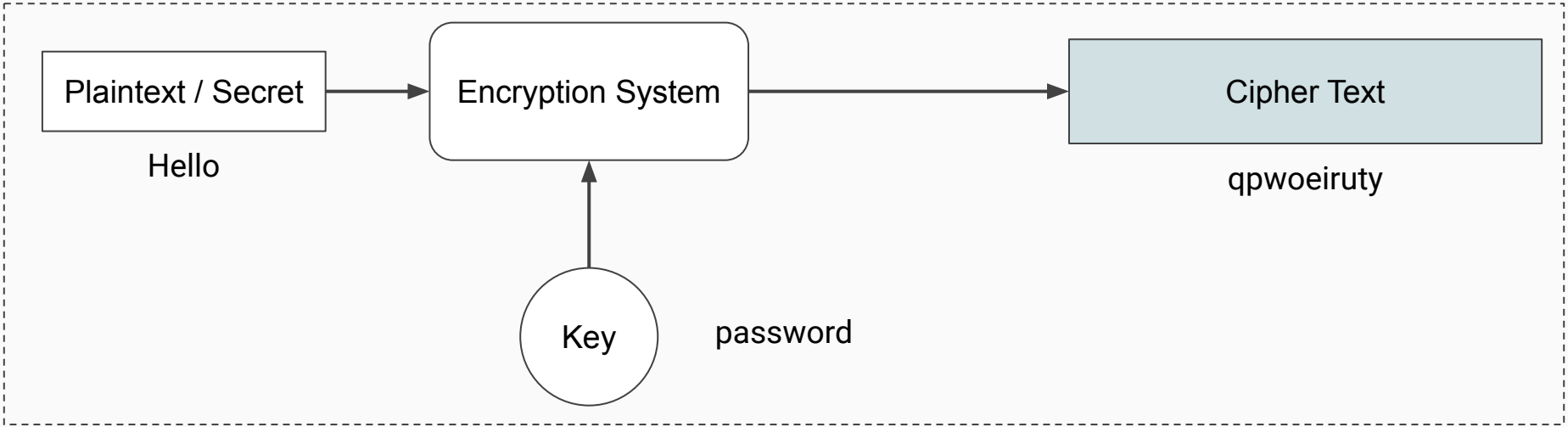
Encrypting your data and connection is the first step towards security!

Cryptography Really Matters

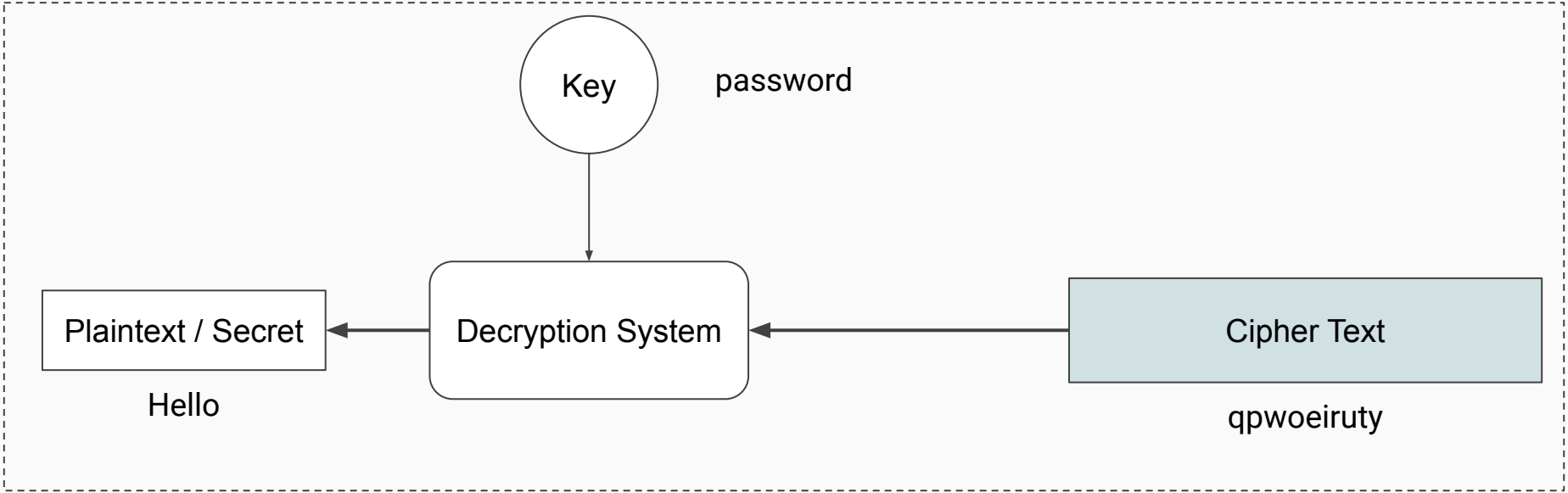
- Internet privacy concerns are real (Attitude Matters)
- Zero Trust Policy
- Hacking is big business (What about Dark Web ?)
- Data Erasure (Conventional vs Cryptographical Way)
- Regulations demand it.
- Do you trust your ISP?
- Is your government spying on you ?

Process of Cryptography

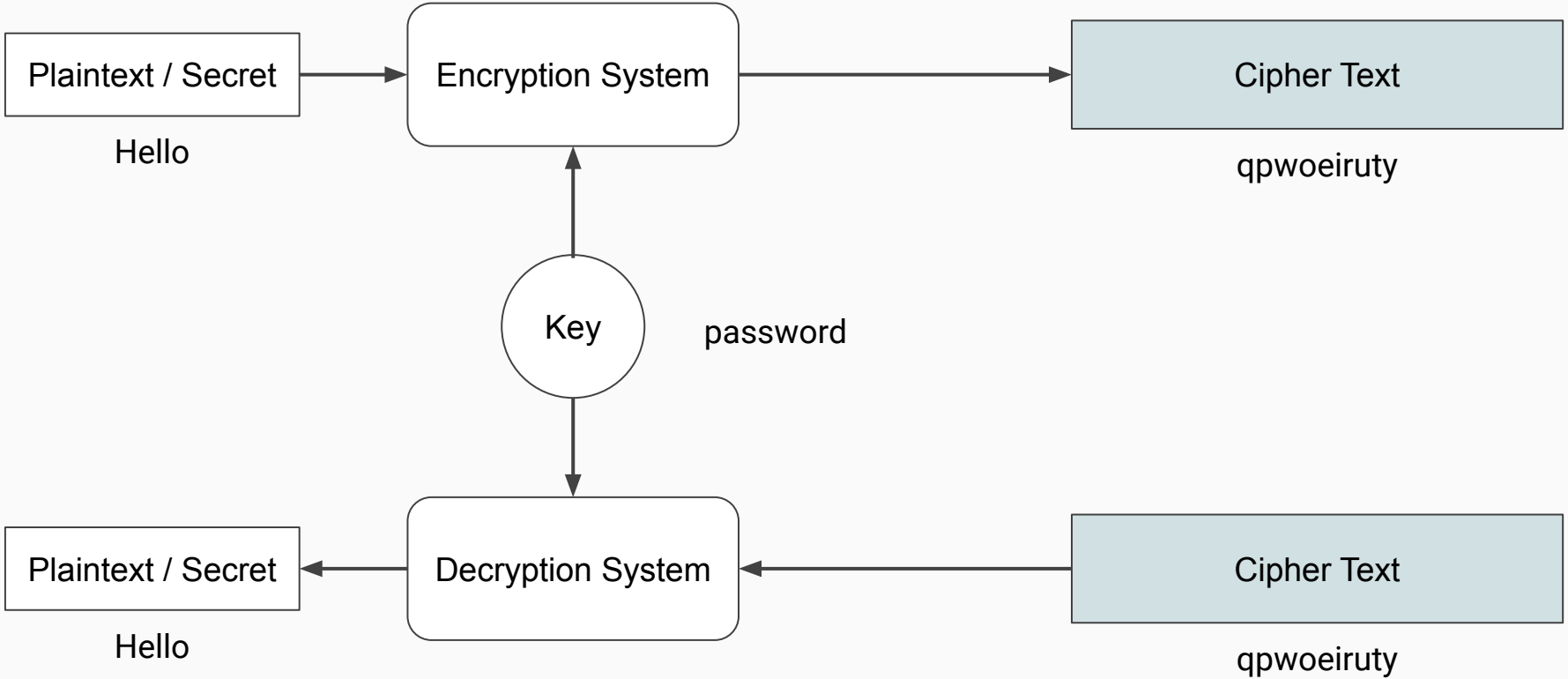
- Encryption (Encoding)
- Decryption (Decoding)



Process of Cryptography - Encryption (Encoding)



Process of Cryptography - Decryption (Decoding)



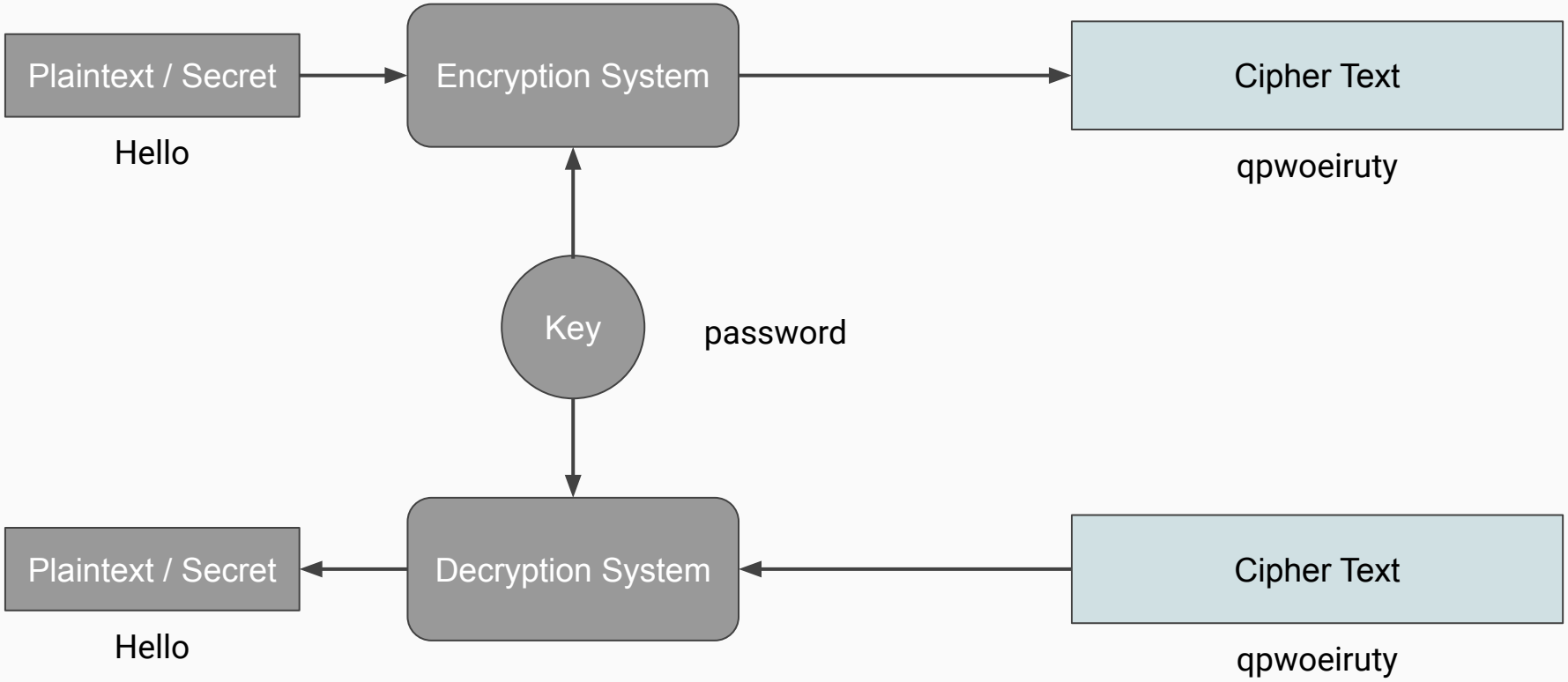
Process of Cryptography - Decryption (Decoding)

“Security through Obscurity”

This paradigm relies on the implementation and design of a system as the main method of providing security.

“In layman terms, if you don’t know what was done, you won’t be able crack the system”

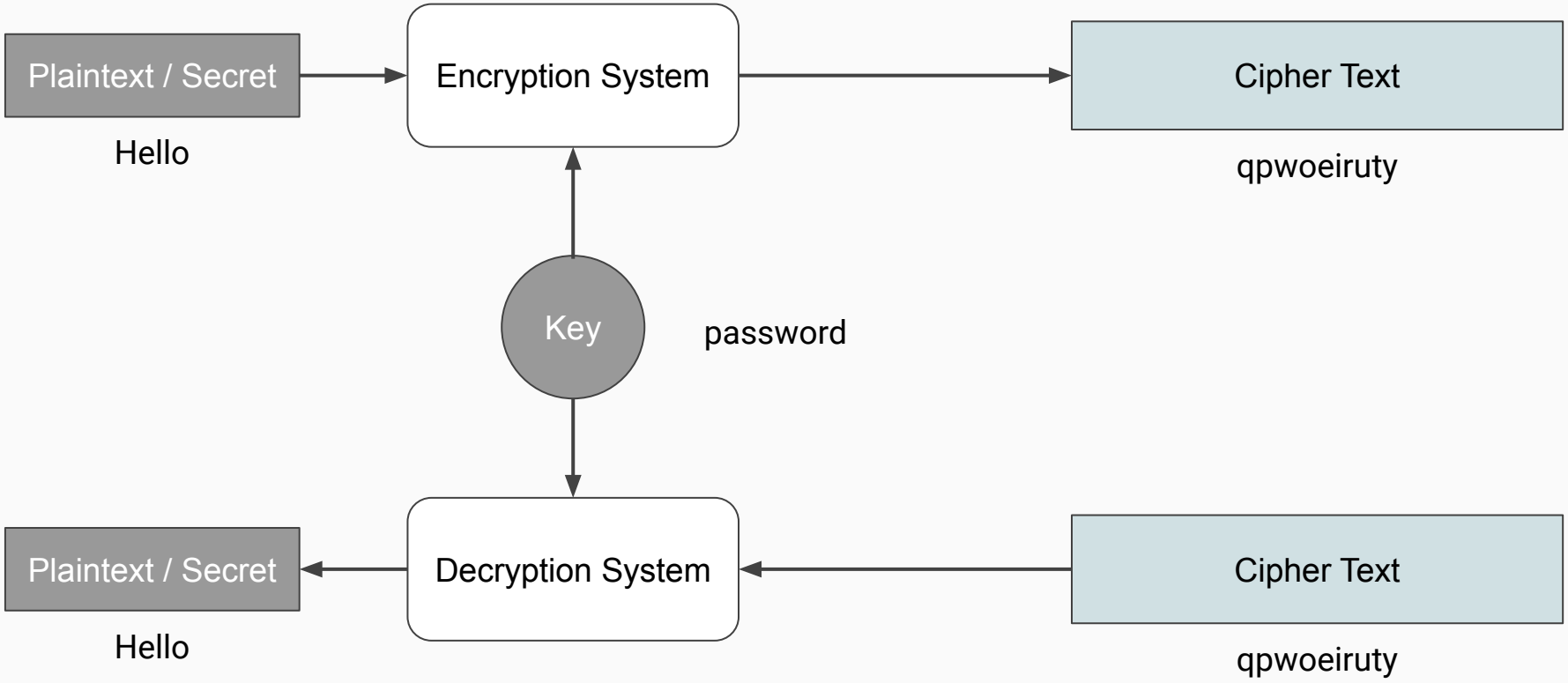
Security through obscurity is different from black box testing



Process of Cryptography - Decryption (Decoding)

Secrecy in Plain Sight
- New Era of Cryptography -

Providing security by withholding the knowledge of the key!



Process of Cryptography

Classic vs Modern Cryptography

Classic

Manipulates traditional characters

Relies on “Security through obscurity”

Requires the entire cryptosystem for communicating confidentially.

Modern

Manipulates bit sequences

Relies on mathematical algorithms

Requires the possession of a particular key to communicate confidentially.

Basic Operations

- XOR
- Shifts
- Permute
- Substitute

XOR

Exclusive or or exclusive disjunction is a logical operation that outputs true only when inputs differ.

100111001011010100111010
010110100001101111011000

110001101010111011100010

Shifts / Rotate

Rotate a given bit stream while still preserving the information of the given stream.

100111001011010100111010

Left Shift - Key = 2 : 011100101101010011101010

Left Shift - Key = 5 : 100101101010011101010011

Permutation

Permutation is a method of bit-shuffling used to permute or transpose bits across the given data while still preserving the information.

1101 - Can be permuted into {0111, 1011, 1110}

Hello - Can be permuted into {elloH, eloHl.....}

Substitution

Substitution is a method of replacing one character with another character!

“Hello” when substituted with these following rules {H:k, e:m, l:b, o:a}, produces “kmbba”

Enigma Machine

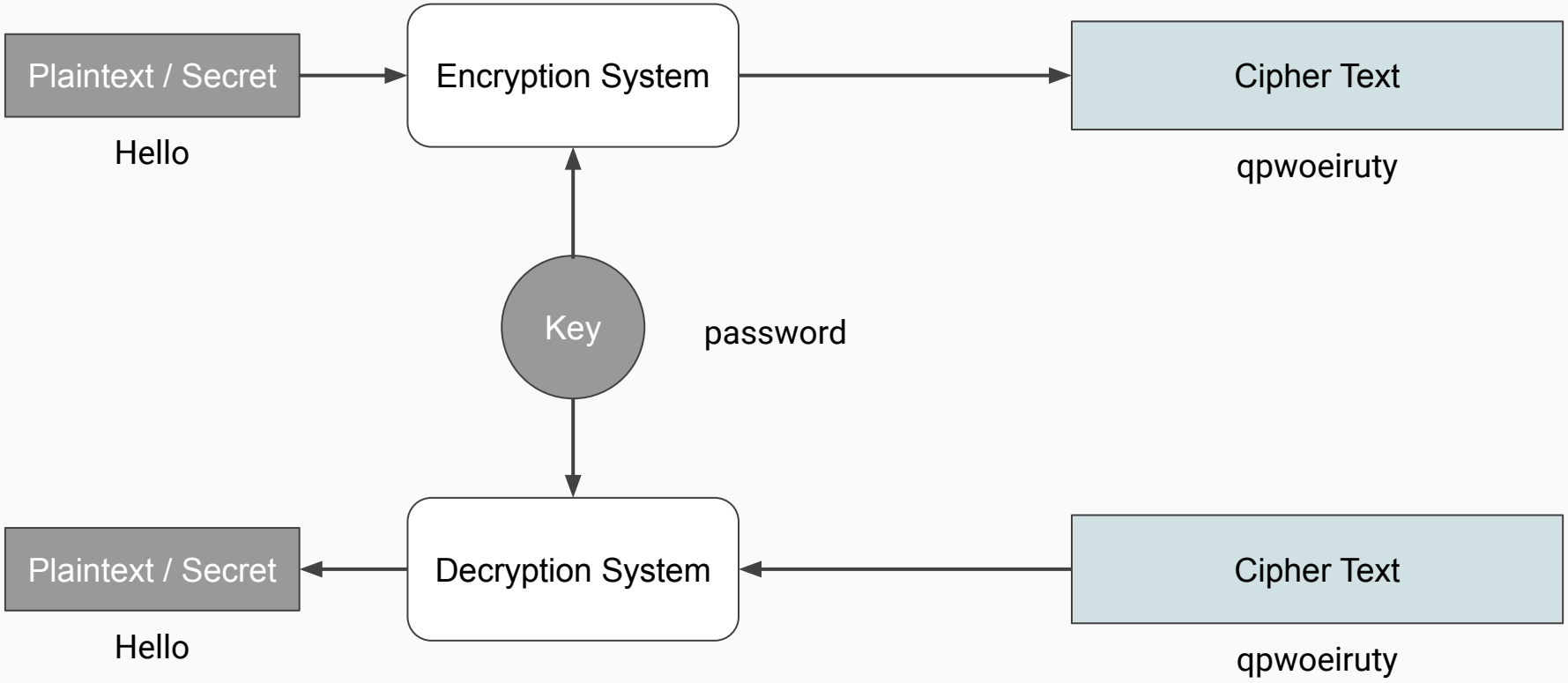
An encryption device developed and used in the early- to mid-20th century to protect commercial, diplomatic and military communication, widely used by Nazi Germany during World War II.

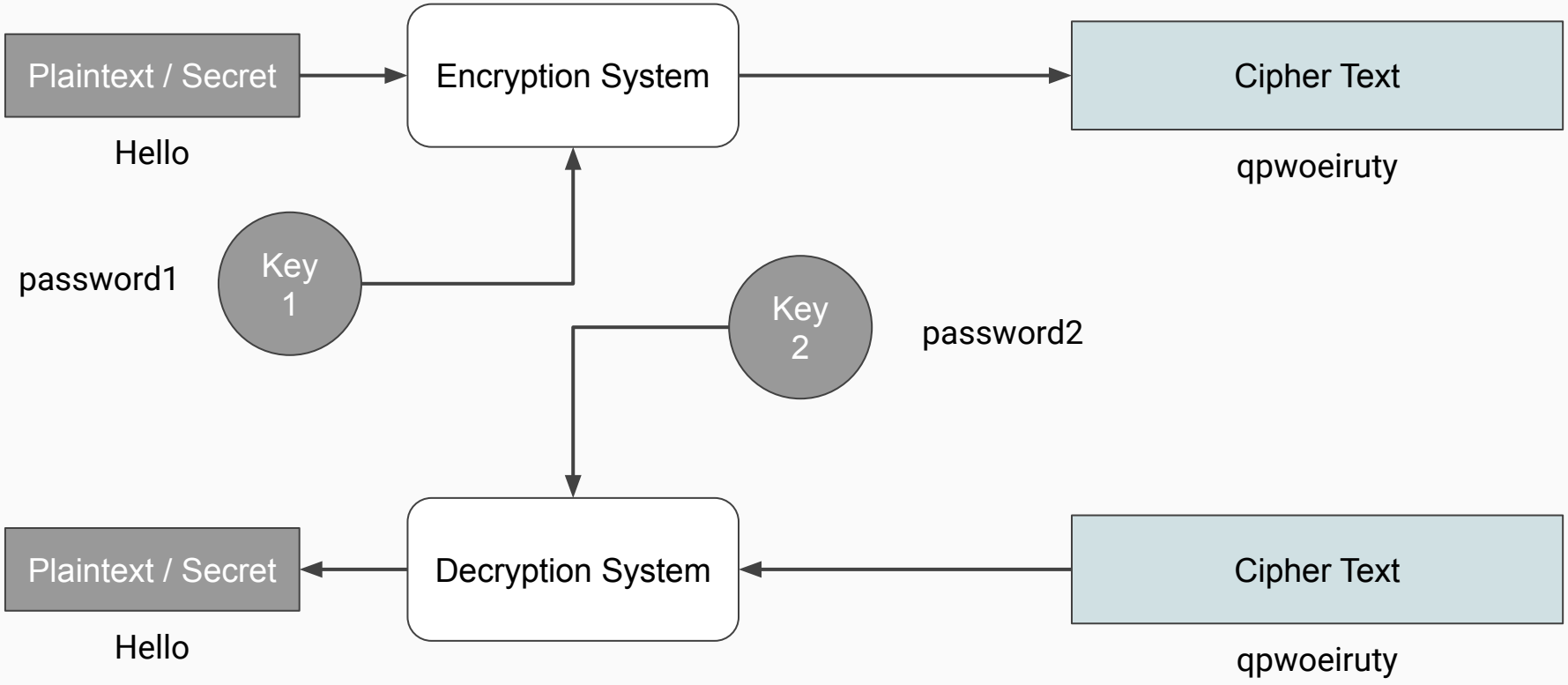
https://thumbs-prod.si-cdn.com/BclHr06K4l68eBelnpcPPc7xz-M=/fit-in/1600x0/https://public-media.si-cdn.com/filer/f5/95/f59548db-c8c7-47a0-8404-9e44cd4b8db6/enigma.jpg

These four operations where the foundations of Enigma Machine!

Types of Encryption

- Symmetric Encryption
- Asymmetric Encryption


Plaintext / Secret
Hello
Encryption System
Cipher Text
qpwoeiruty
Key
password
Plaintext / Secret
Hello
Decryption System
Cipher Text
qpwoeiruty


Plaintext / Secret
Hello
Encryption System
Cipher Text
qpwoeiruty
password1
Key 1
Key 2
password2
Plaintext / Secret
Hello
Decryption System
Cipher Text
qpwoeiruty

Examples

- Caesar Cipher
- Substitution Cipher
- Vigenère Cipher

Caesar Cipher

Plaintext: defend the castle
Ciphertext (Key = 1): efgfoe uif dbtumf

Plaintext: defend the castle
Ciphertext (Key = 2): fghgpf vjg ecuvng

As most ciphers, even Caesar Cipher can be represented in a mathematical formula!

Caesar Cipher

In a mathematical language, say '**x**' be our secret/plaintext, '**k**' be our key and the whole encryption and decryption system be represented by '**e(x)**'.

Encryption: $e(x) = (x + k) \pmod{26}$

Decryption: $e(x) = (x - k) \pmod{26}$

Substitution Cipher

Plaintext: defend the castle
Password: jasmzqupdtnckviehrogwlxbfy
Ciphertext: mzqzvm gpz sjogcz

Plaintext: defend the castle
Password: kpwmhxlvunazisyqbrgectdjfo
Ciphertext: mhxhsm evh wkgezh

One-to-One Mapping

Vigenère Cipher

Vigenere Cipher uses a rectangular matrix method to encrypt and decrypt the plain text!

Plaintext:	defend the castle
Password:	protect
Ciphertext:	svtxrf mwv qtwvet

	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
A	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
B	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	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	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

Vigenere Cipher

Cryptanalysis

- Process

Process of Cryptanalysis

Cryptanalysis is the process of deciphering coded messages without directly having access to the key.

How do we even do that ?

Multiple possibilities

- The cryptanalyst knows that what the cipher is.
- The cryptanalyst is totally unaware of the kind of cipher.
- Chosen ciphertext attack.
- Chosen plaintext attack

  *__Note:__ The cryptanalyst should clearly know beforehand what his expectations are!

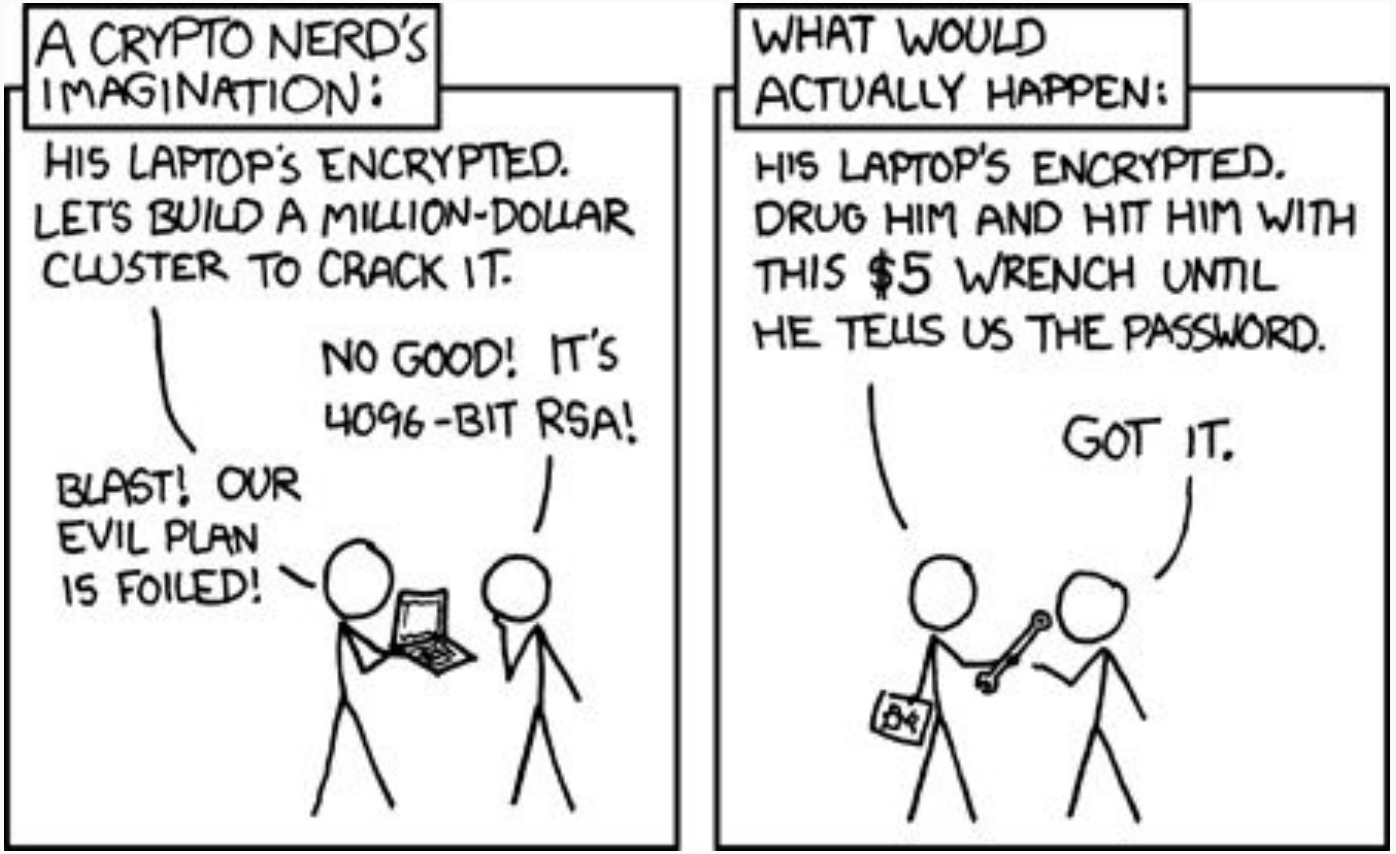
Let’s try breaking Caesar Cipher

1. Easiest way to break Caesar cipher is to try to decode with key from 0 to 25 (Brute force)
    - Bpqa eia miag. Bzg bpm vmfb wvm!
    - awdnj ouelkef dwahsq asdn wadaw

Let’s try breaking Caesar Cipher

1. Easiest way to break Caesar cipher is to try to decode with key from 0 to 25 (Brute force)
    - Bpqa eia miag. Bzg bpm vmfb wvm!
    - awdnj ouelkef dwahsq asdn wadaw

2. Another method is to try frequency distribution! (**Caveat:** It should be a meaningful english words/sentences)



https://xkcd.com/538/

Let’s try breaking Substitution Cipher

1. Brute force ? - 26 Characters
    - gwxueeq iv tusv kjukova wm

    26 characters will result in a possible search sample of 26! (26 Factorial)

2. Another method is to try frequency distribution! (**Caveat:** It should be a meaningful english words/sentences)

Effort vs Reward Ratio

Not every cryptosystem is worth breaking!

Try to understand the amount of work required to break a cryptosystem and the reward it contains

Thank You

Atit Gaonkar

atit-gaonkar.me/
linkedin.com/in/atit-gaonkar/
instagram.com/atit.sgaonkar/