#HASHING_IN_DEEP

Jawad Fakiha

أكاديمية طويق
TUWAIQ ACADEMY

TABLE OF CONTENTS

أكاديمية طويق
TUWAIQ ACADEMY

#1

#INTRODUCTION

as we know the Main Goal of Cybersecurity is to protect the CIA Triad
but in this Subject we are focusing on " Confidienielty and Integrity "

أكاديمية طويق
TUWAIQ ACADEMY

#INTRODUCTION

In a Simple Way ,

Encryption is converting plaintext to encrypted text via a ***two-way*** algorithm
Encoding is converting plaintext to a value with a specific format
Hashing is a ***one-way*** algorithm that produces a fixed-length bit string value

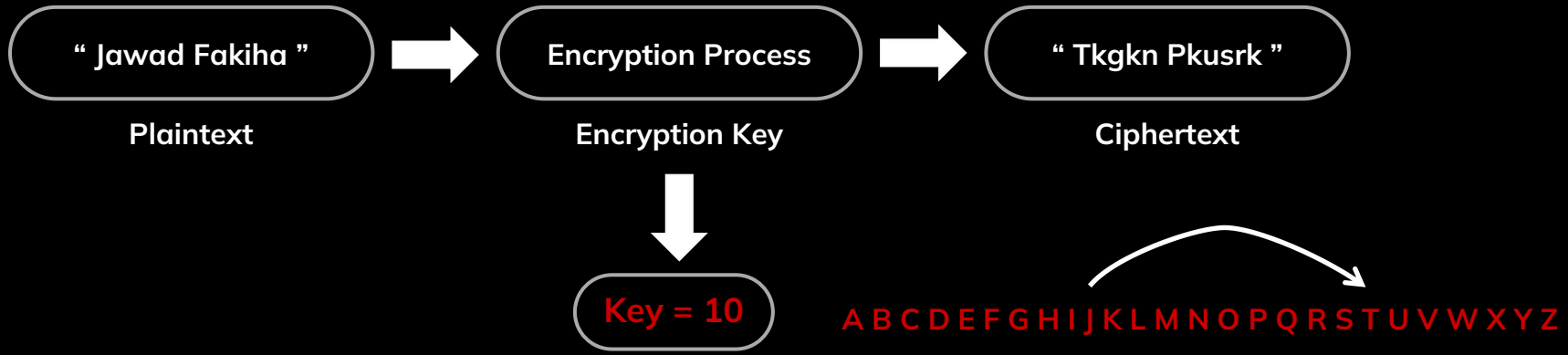
#2

#Encryption

Basic Encryption

#Encryption

- How Encryption Works ?

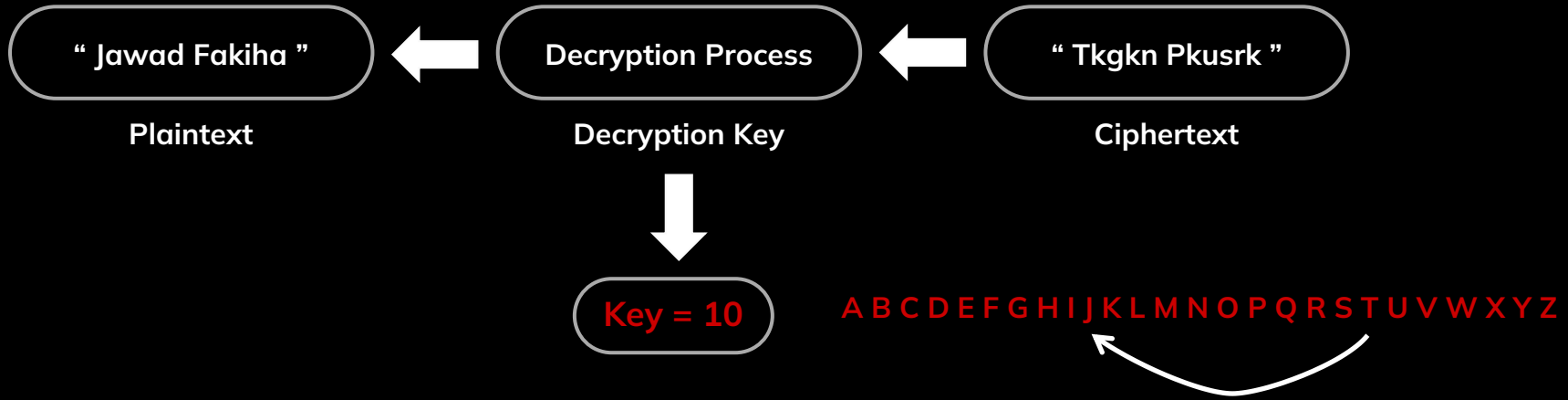


So this cipher will substitute every alphabet from the plaintext to the N^{th} letter after it in the alphabet and while we know that our encryption key is “ 10 ” then it will substitute it to the corresponding 10^{th} letter after it as we see in the example

* as we know there is Symmetric and Asymmetric Encryption but its not our deal now

#Decryption

- Reversing Our Encryption Method



as we see in the decryption mechanism we used the same key but in the opposite way and it displayed to us the plaintext as it was , this what we call a “ *two-way* ” function

#3

#Encoding

Basic Encoding

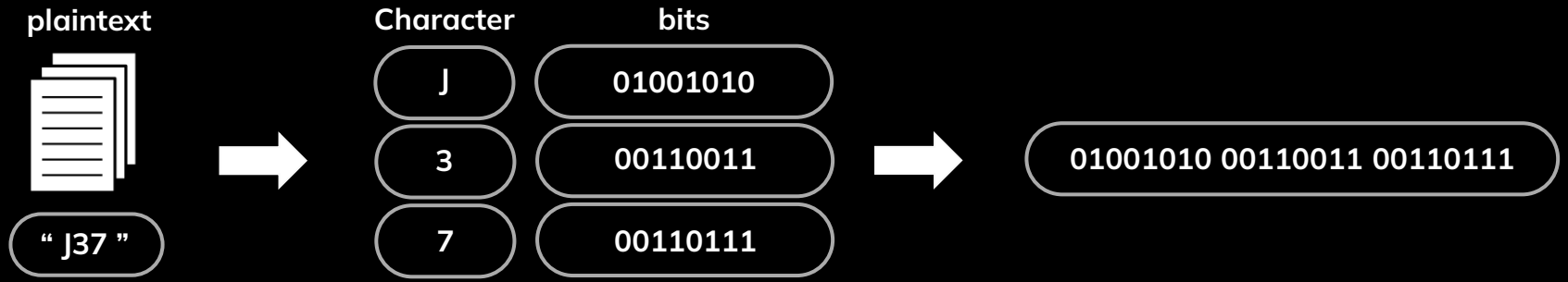
#Encoding

- From the First look what are these types of Encoding ?

1. VHV3YWlxQWNhZGVteQ==
2. IN4WEZLSONSWG5LSNF2HSICCN5XXIY3BNVYA====
3. 01001010 00110011 00110111

#Encoding

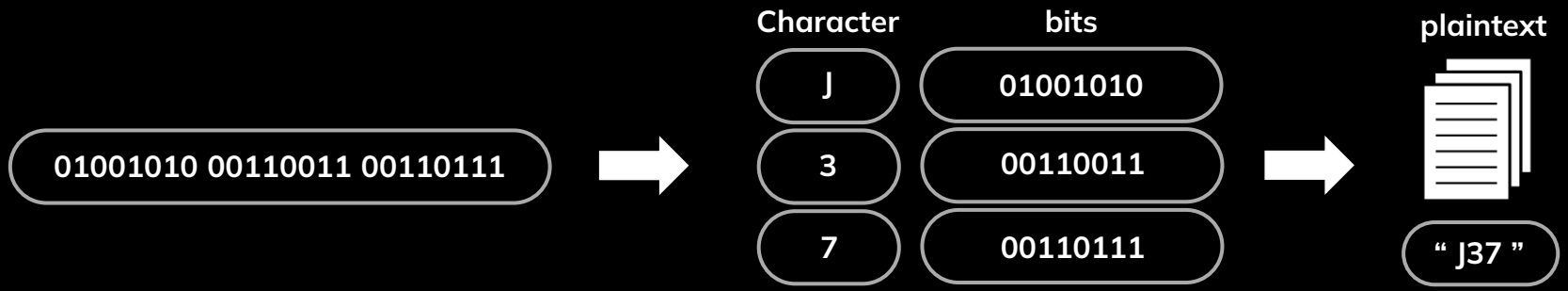
- How Encoding Works ?



As we see for every character we have an equivalent sequence of bits that will be the value after encoding

#Decoding

- How Decoding Works ?



As we see for every sequence of bits we have an equivalent character that will be the value after decoding

#4

#Hashing

Deep Insights into Hashing

#Hashing

a Hashing Algorithm takes an Input and apply the Algorithm on it to Produce a **fixed-sized** value

SO

We have an **Input** and a **Mathematical Process** that will give us a unique **Output** ?

Then **HOW** we can't reverse this Process to retrieve the Input again as Encryption and Encoding **???**

#Hashing

One-way Mathematical Operation
(Hard to Reverse)

p * q = n

= HASH

+

Fixed Output Size
(Digest)

+

Avalanche Effect
(a Small Change in the Input Produces an Extremely Different Output)

Non-Linear Functions - XOR – Iterations ...

+

Lack of Inverse Operations

#Salt

All That Complexity we discussed before is none comparing to what we are making now ...

WHAT IS SALT ?

A **Random** Data used as an additional input to a hash function to make an additional defensive layer against attacks

Okay then HOW we will we know that this hash belongs to an input if the Salt is Generated Randomly ????

#Salt

Simple Example – Storing Passwords

Registration Process

- User Enter The Password
- Generate a Random Salt
- Combine The Salt with the Password
- Generate The Hash to (Password + Salt)
- Store it Both in the User Records

User	Hash	Salt
Jawad	5eb63b	123
Fakiha	2ef7bd	ABC
J37	a591a6	J37

Authentication Process

- Retrieve the User Stored Hash and Salt
- Combine the Salt with the Entered Password
- Generate the Hash Using the Salted Password
- Compare the hash previously stored wit the Generated Hash we Just got

#Pepper

We Learned That The Salt is Stored in the User Records next to the Hash so WHAT if an attacker could retrieve that info and Differ the Original Hash from the Salt ???

#Pepper

Pepper is a Secret Value known only to the System
and It’s not stored in the User Records

User	Hash	Salt		Pepper
Jawad	5eb63baJefi4sdg	123	:	#
Fakiha	2ef7bddBns34rs	ABC	:	#
J37	a591a6NjsuT21l	J37	:	#

#Question

What Does this three Protect in the CIA Triad ?

1. Encryption ?
2. Encoding ?
3. Hashing ?

I Provide a Simple Python Code Example to Clarify the Points

“ YOU CAN FIND IT ALSO ON MY GITHUB PAGE ”

THANKS FOR LISTENING

HOPE YOU HAVE LEARNED SOMETHING NEW !

أكاديمية طويق
TUWAIQ ACADEMY