



UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CIENCIAS

**Práctica 01: Reporte - Las Canijas Lagartijas**

ALUMNOS

**Gabriela López Diego -** 318243485
**Abraham Jiménez Reyes -** 318230577
**Javier Alejandro Rivera Zavala -** 311288876
**Juan Daniel San Martin Macias -** 318181637

PROFESORA

**Anayanzi Delia Martínez Hernández**

AYUDANTES

**Cecilia del Carmen Villatoro Ramos**
**Roberto Adrián Bonilla Ruíz**
**Ivan Daniel Galindo Perez**
**Roberto Adrián Bonilla Ruíz**

ASIGNATURA

**Criptografía y Seguridad**

13 de Febrero del 2024

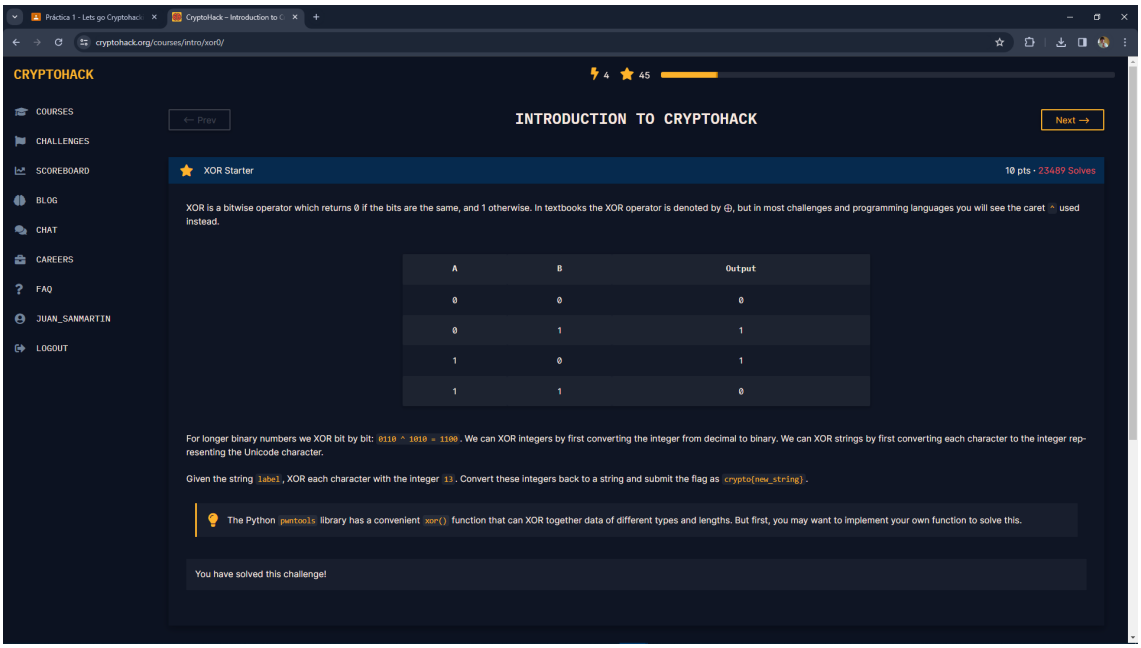
# 1. Introducción

Esta practica consistió de una breve una introducción a la criptografía a través de la plataforma *Cryptohack*. El módulo de introducción que se encuentra en dicha plataforma, consta de 10 ejercicios para principiantes. El objetivo del módulo, es que logremos aprender a través de los acertijos a resolver, algunos aspectos sobre el operador/función XOR, así como de algunas herramientas presentes en Python, que nos permiten codificar ó cifrar el contenido de nuestros mensajes. Conforme avanzamos en los ejercicios la dificultad aumenta y esto hace que ya no solo utilicemos funciones que están definidas en Python sino que surge entonces, la necesidad de definir algunas funciones propias, un poco mas detalladas para obtener la respuesta.

En esta práctica logramos ver en acción, como la codificación es importante para aumentar la seguridad de nuestras contraseñas, mensajes, documentos con información sensible, entre otras cosas. También tuvimos una pequeña muestra, sobre como algunas áreas de las matemáticas, en particular la teoría de números, se relacionan con las ciencias de la computación y dotan a nuestra disciplina de poderosas herramientas.

# 2. Desarrollo

1. **XOR Starter**




*Código desarrollado para resolver el ejercicio:*

```
    label = "label"
    xor_result = ""

    for char in label:
        ascii_value = ord(char)
        xor_result += chr(ascii_value ^ 13)

        print(f"crypto{{{xor_result}}}")

```

Al ejecutar éste algoritmo nos devuelve la bandera *crypto*{*aloha*}, se le dio ese formato a la línea del print ya que al sólo concatenar la cadena obtenida con el formato de la bandera, es decir:

```
print("crypto{",xor_result,"}")

```

se imprimía con un espacio en blanco antes y después de la cadena obtenida. Por otro lado, como se puede observar en el código, no se utilizó la función que se menciona como hint en CryptoHack ya que

no opera en caracteres directamente, sino en sus representaciones numéricas. En cambio, utilizamos la función ord() para obtener el valor numérico de cada carácter, aplicamos la operación XOR a estos valores y luego utilizamos la función chr() para convertir los valores resultantes nuevamente en caracteres.

## NIVEL 1

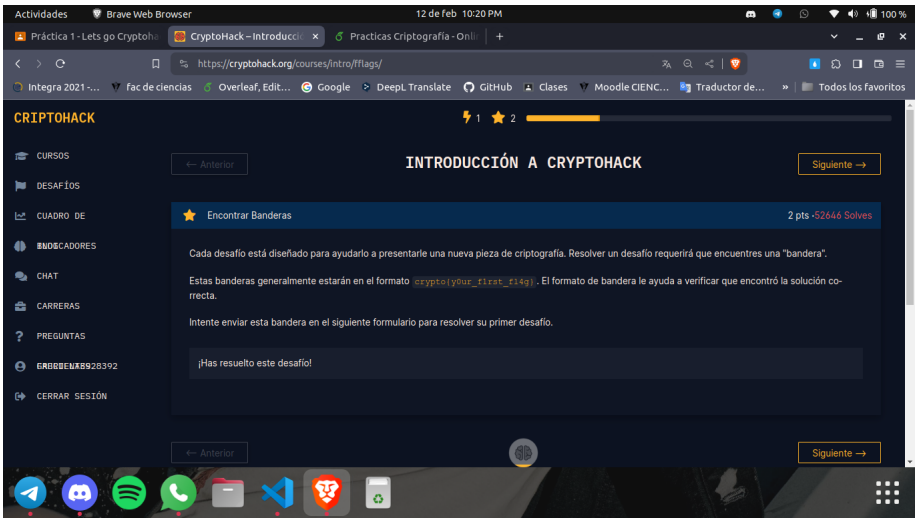



Figura 1: Evidencia nivel 1: Introducción a cryptohack

## RECURSO UTILIZADO

```
ninguno, el test fue de prueba
```

BANDERA = crypto{y0ur_first_fl4g}

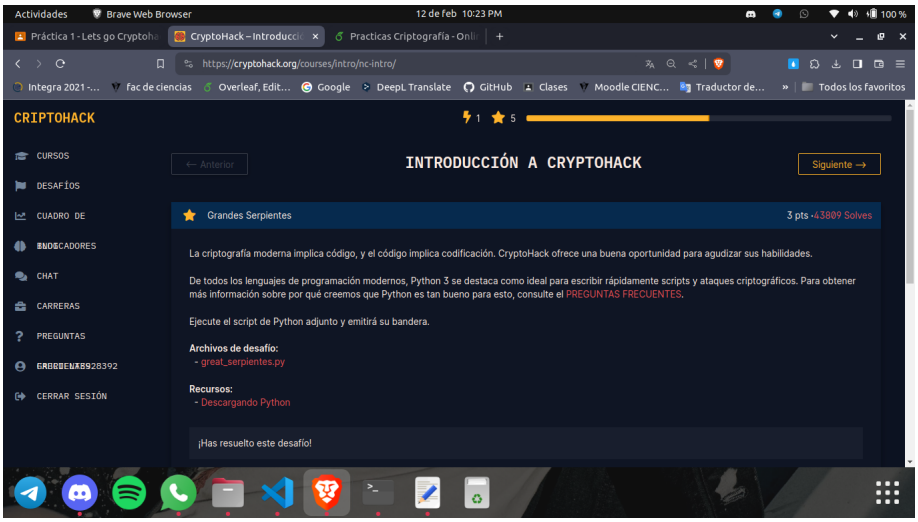



Figura 2: Evidencia nivel 1: Introducción a cryptohack

## RECURSO UTILIZADO

```
import sys
ords = [81, 64, 75, 66, 70, 93, 73, 72, 1,
92, 109, 2, 84, 109, 66, 75, 70, 90, 2, 92, 79]

print("Here is your flag:")
print("".join(chr(o ^ 0x32) for o in ords))
```

BANDERA = crypto{z3n_0f_pyth0n}

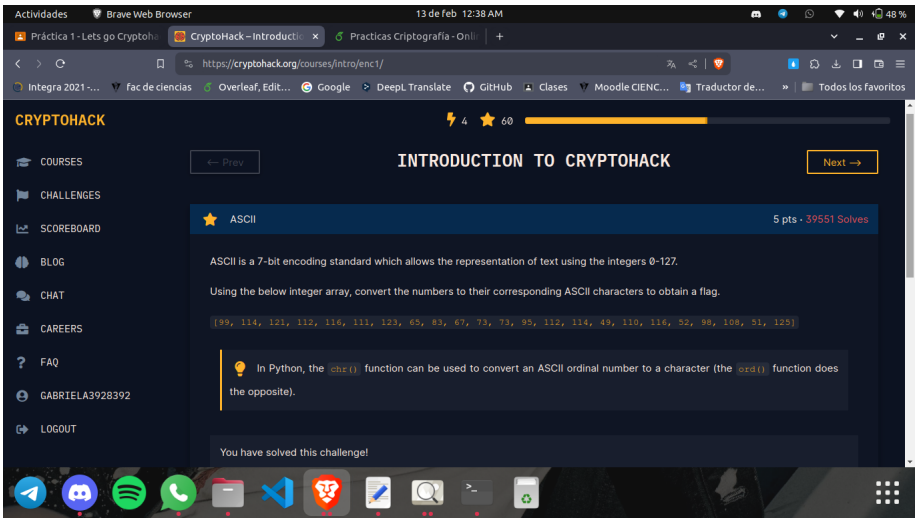



Figura 3: Evidencia nivel 1: Introducción a cryptohack

## RECURSO UTILIZADO

```
lista_enteros = [99, 114, 121, 112, 116, 111, 123, 65, 83, 67, 73, 73, 95, 112, 114, 49, 110,
116, 52, 98, 108, 51, 125]
bandera = ''.join(chr(i) for i in lista_enteros)
print("La bandera es:", bandera)
```

BANDERA = crypto{ASCII_pr1nt4bl3}

## NIVEL 2


Figura 4: Evidencia Nivel 2

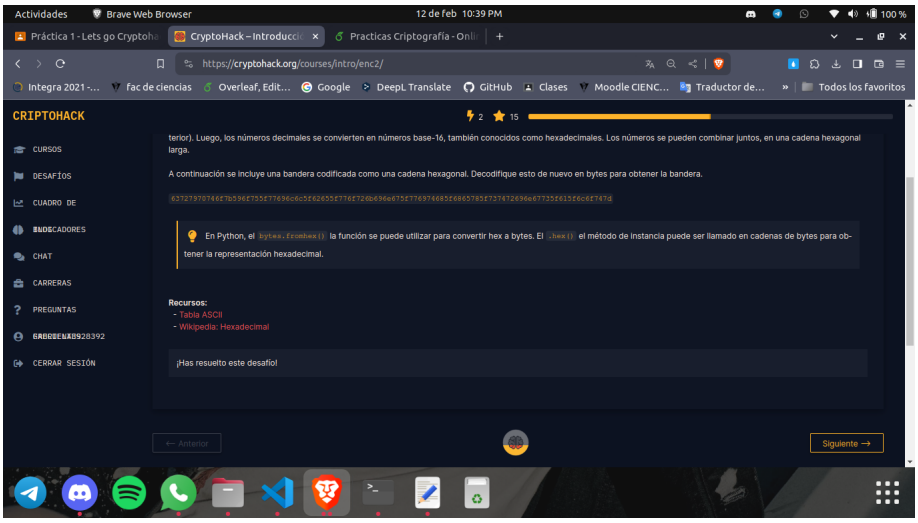



Figura 5: Evidencia nivel 2: Introducción a cryptohack

## RECURSO UTILIZADO

```
cadena = "63727970746f7b596f755f77696c6c5f62655f776f726b696e675f776974685f6865785f737
472696e67735f615f6c6f747d"
bandera= bytes.fromhex(cadena)
print("La bandera en bytes es:", bandera)
```

BANDERA = crypto{Youwill_be_working_with_hex_strings_a_lot}

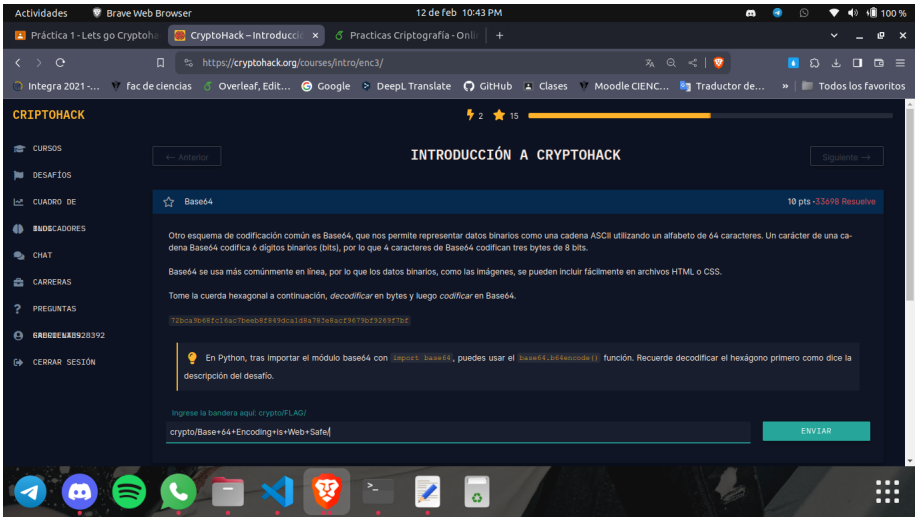



Figura 6: Evidencia nivel 2: Introducción a cryptohack

## RECURSO UTILIZADO

```
import base64

cadena = "72bca9b68fc16ac7beeb8f849dca1d8a783e8acf9679bf9269f7bf"
#Decodificar a bytes
cadena_en_bytes = bytes.fromhex(cadena)
# Codificar los bytes en Base64
cadena_base64 = base64.b64encode(cadena_en_bytes)
print("--->La bandera es:", cadena_base64.decode('utf-8'))
```

BANDERA = crypto/Base+64+Encoding+is+Web+Safe/

**NIVEL 3** (No logre tomar captura pero para este momento se ha llegado al nivel 3)

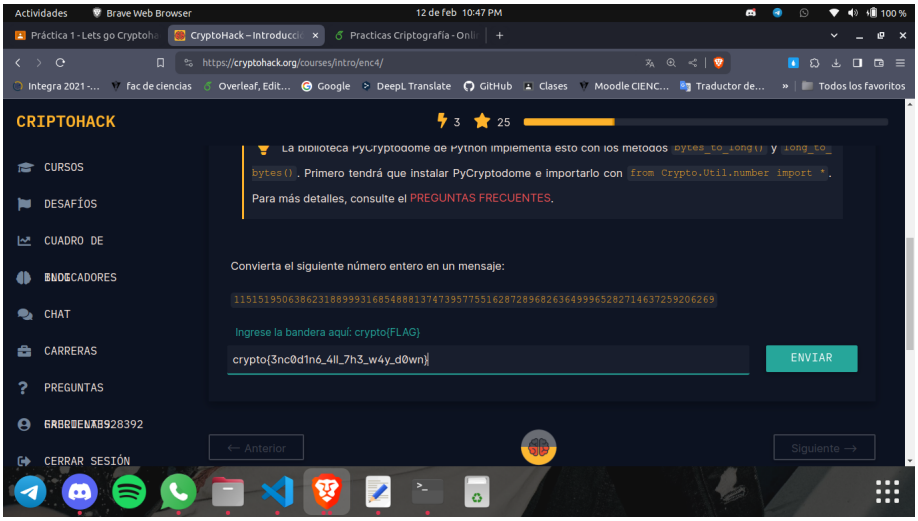



Figura 7: Evidencia nivel 3: Introducción a cryptohack

## RECURSO UTILIZADO

```python
from Crypto.Util.number import *;

numero = 11515195063862318899931685488813747395775516287289682636499965282714637259206269
convertido_a_bytes = long_to_bytes(numero)
bandera = convertido_a_bytes.decode('utf-8')
print("--->La bandera es:", bandera)
```

BANDERA = crypto{3nc0d1n6_4ll_7h3_w4y_d0wn}


Figura 8: Evidencia nivel 3: Introducción a cryptohack

## RECURSO UTILIZADO

```python
label = "label"
entero = 13

#Transformamos cada caracter en su valor numerico unicade
valores_unicode = [ord (c)  for c in label]
#Realizamos XOR con cada valor de la lista y la variable entero
valores_xor = [valor ^ entero for valor in valores_unicode]
```

```python
#Convertimos cada valor en su correspondiente caracter unicode y formamos una nueva cadena
bandera = "".join (chr(valor) for valor in valores_xor)
print ("crypto{"+bandera+"}")
```

BANDERA = crypto{aloha}

**NIVEL 4**

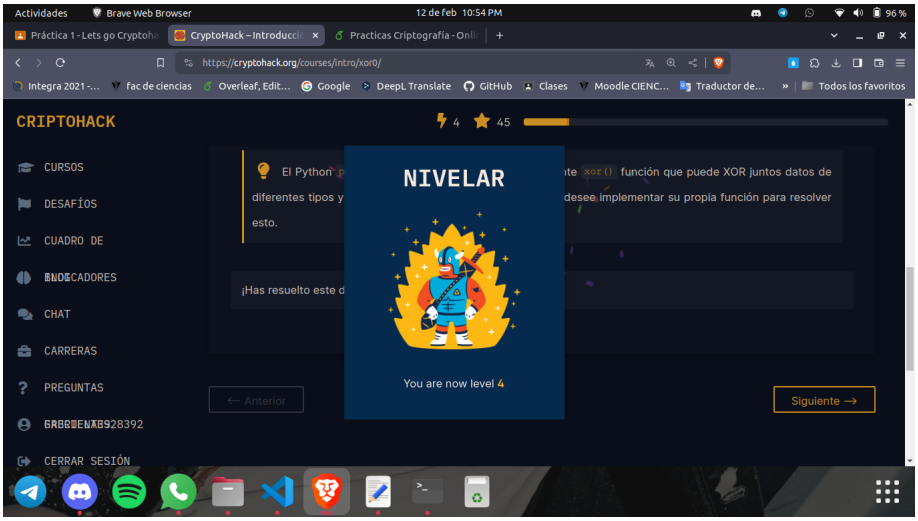



Figura 9: Evidencia NIVEL 4

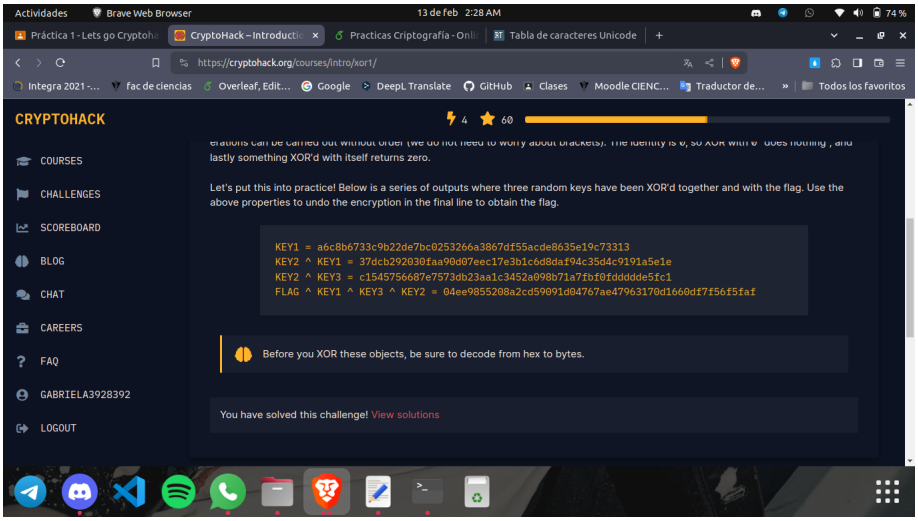



Figura 10: Evidencia nivel 4: Introducción a cryptohack

## RECURSO UTILIZADO

```python
from pwn import xor

key1 = bytes.fromhex('a6c8b6733c9b22de7bc0253266a3867df55acde8635e19c73313')
key2_3 = bytes.fromhex('c1545756687e7573db23aa1c3452a098b71a7fbf0fdddde5fc1')
flag_k123 = bytes.fromhex('04ee9855208a2cd59091d04767ae47963170d1660df7f56f5faf')
print(xor(flag_k123,key1,key2_3))
```

BANDERA = crypto{x0r_i5_ass0c1at1v3}

## 2.1. Investigación

### 2.1.1. Malware:

Se refiere a cualquier tipo de software diseñado específicamente para dañar, controlar o acceder de manera no autorizada a un sistema informático o a los datos que contiene. Los malware pueden incluir virus, gusanos, troyanos, ransomware, spyware, entre otros tipos de programas maliciosos.

### 2.1.2. Spam:

El spam es el envío masivo de mensajes no solicitados, generalmente a través de correo electrónico. Estos mensajes suelen contener publicidad no deseada, enlaces a sitios web maliciosos o fraudulentos, o intentos de estafas.

# 3. URL del perfil de cada integrante del equipo

- López Diego Gabriela 318243485
  **URL:** `https://cryptohack.org/user/Gabriela3928392/`

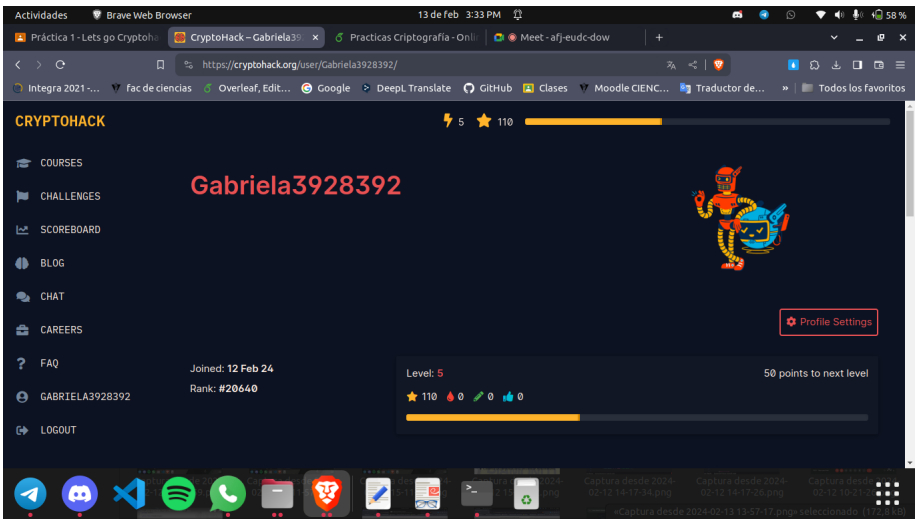



Figura 11: Perfil Gabriela

- Jiménez Reyes Abraham - 318230577
  **URL:** `https://cryptohack.org/user/abraham08/`

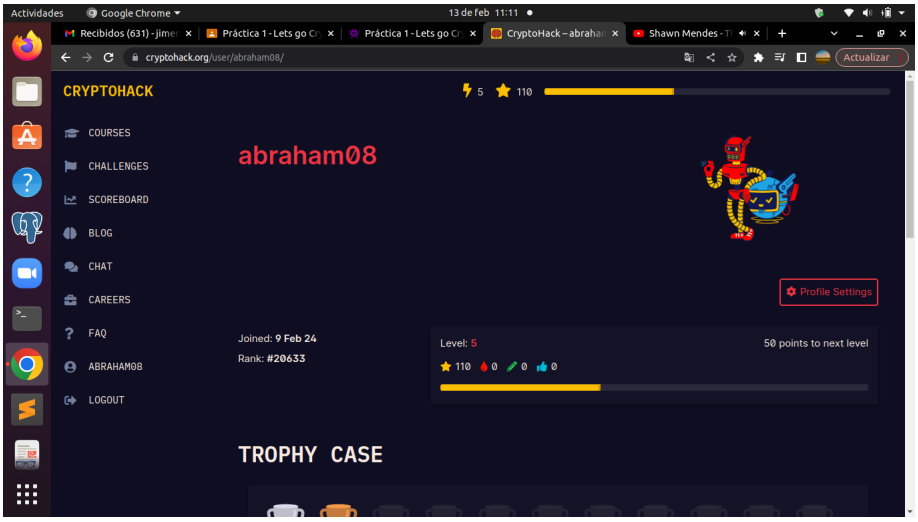



Figura 12: Perfil Abraham

- Rivera Zavala Javier Alejandro - 311288876
  **URL:** `https://cryptohack.org/user/AlejandroRZ95/`

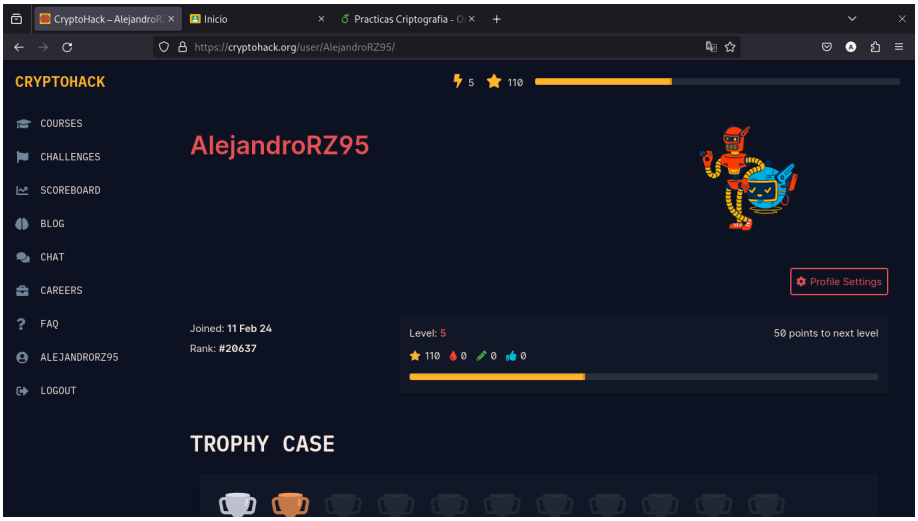



Figura 13: Perfil Alejandro

- San Martin Macias Juan Daniel - 318181637
  **URL:**`https://cryptohack.org/user/Juan_SanMartin/`


Figura 14: Perfil Juan

# 4. Conclusiones

Esta práctica nos fue de gran utilidad para comenzar a hilar los conocimientos teóricos adquiridos a lo largo de la clase, con aplicaciones en el mundo real aunque estas fueran muy sencillas. Pudimos apreciar también una relación hasta ahora desconocida, entre un operador muchas veces mencionado y utilizado en el contexto del hardware, la lógica y otras áreas de la computación, pero no en el ramo de la seguridad computacional, o al menos, no lo habíamos nosotros no lo habíamos conocido en ese contexto.

Aprendimos también, sobre distintas formas de representar la información contenida en una computadora. Entre las distintas formas vistas, las más significativas fueron la representación en base 16 y en base 64, mismas que son empleadas en muchos de los protocolos de seguridad e intercambio de información más comunes en el mundo.

Con base en lo anterior, es un tanto más claro para nosotros que podemos aplicar en nuestra vida, algunas de las prácticas y conocimientos aquí aprendidos, al colocar contraseñas más seguras, siguiendo protocolos de seguridad más solidos, cuidando con quién compartimos nuestra información, etc. La criptografía y su estrecha relación con la seguridad, es algo que de primera impresión podemos avizorar, pero son prácticas como esta. las que nos permiten cristalizar todas las impresiones desarrolladas a lo largo de las clases.

# 5. Extra

**Preguntas Ep: 000 - Operation Aurora**

1. ¿Qué sucedió el 14 de Diciembre de 2009 en Google? Un grupo de piratas informáticos con base en China (y financiados por el gobierno chino), robó información de disidentes chinos y documentos clasificados del departamento de seguridad del gobierno estadounidense, junto con otra información sensible de corporaciones privadas y organismos públicos.

2. ¿En qué consiste el proyecto Aurora? Es el nombre que se le dio a la amenaza tras ver algo raro en el código del malware, ya que no solo había 1's y 0's si no que tenían palabras que significaban algo y entre ellas el nombre de Aurora. Por lo anterior, decidieron llamar Aurora a la operación de salvaguardar la información y evitar que siguieran robando la información.

3. ¿Qué relevancia tiene el nombre "Aurora"? En octubre de 1917 un acorazado ruso de nombre ABPOPA (Aurora) disparó un cañonazo, el proyectil estaba vació pero la función de dicho cañonazo era comunicar un mensaje: la revolución Rusa de 1917 acababa de comenzar. El nombre Aurora se encontraba dentro del código del malware.

4. Describe en tus propias palabras ¿qué es el análisis forense? El análisis forense busca en dispositivos digitales pruebas de manera similar que en el caso del análisis forense en crímenes, al igual que sus homólogos encargados de hacer cumplir la ley, los investigadores forenses informáticos deben de realizar la búsqueda de pruebas digitales así como su recopilación, manipulación y procesamiento.

5. ¿Qué es un **Galimatías**? Un mensaje sin sentido, escrito en un lenguaje enredado y aparentemente indescifrable, También puede emplearse ese término para referirse al lenguaje en si mismo y no sólo al mensaje.

6. ¿Cómo entró en acción el equipo de Google para erradicar el ataque? Por las fechas de navidad, los ingenieros, investigadores de seguridad y todo el selecto personal involucrado en el manejo de la crisis, debían desconectar a todo el mundo de la red y restablecer las contraseñas de todos los usuarios dentro del lapso de una hora. Haciendo lo anterior, echaron al atacante de todos los sistemas a la vez.

7. ¿De dónde provenía el ataque? Provenía de China.

**Preguntas Ep: 001 - Threat Analysis Group**

1. ¿Internet está lleno de personas que intentan hacer cosas malas? ¿Cual es el deber por parte del equipo de Google?
   Sí. El deber de Google es averiguar quienes y como operan los atacantes para poder impedir que burlen la seguridad del sistema.

2. Menciona algunas amenzas monitorizadas por Google

   - Ransomware
   - Amenazas de desinformación
   - Amenazas respaldadas por el gobierno

3. ¿Qué significa TAG? ¿Qué tipo de contenido bloquea?
   Threat Analysis Group (Grupo de análisis de amenazas) Se encargan de bloquear contenido peligroso y/o malicioso que llega a nuestro correo personal.

4. ¿Qué es WannaCry? Explica brevemente lo que hace y de donde proviene.
   Fue el ataque de ransomware más importante registrado en la historia. En un día logro infectar aproximadamente 200,000 ordenadores de todo el mundo, alrededor de 150 países. Entre ellos, instituciones importantes como banco y/o universidades. Mas tarde, se descubrió provenía del Gobierno de Corea del Norte.

5. Con tus propias palabras, ¿Qué es el phishing?
   Se trata de una técnica muy utilizada por atacantes que buscan obtener información personal, datos bancarios, contraseñas, etc de forma engañosa mediante el envió de correos electrónicos o mensajes que simulan pertenecer a alguna institución verificada, de alguna red social y/o amig@. Estos correos o mensajes suelen contener links de los cuales el usuario confía y llega a otorgar sus datos personales al atacante. También puede llegar a ocurrir que el ordenador se instale algún malware.

# 6. Referencias


- La página web *CryptoHack* ofrece cursos en criptografía[1].
- La siguiente plataforma nos fue de ayuda para resolver el ejercicio 10 del módulo introduction to cryptohack: `https://captainmich.github.io/programming$_$language/CTF/Challenge/CryptoHack/general.html`
- No hay nombre del autor. Sitio web de la interpol - Análisis forense digital `https://www.interpol.int/es/Como-trabajamos/Innovacion/Analisis-forense-digital`
- Editor sin nombre. Sitio web de ESET - ¿Qué es la operación Aurora? `https://www.welivesecurity.com/la-es/2010/01/21/que-es-operacion-aurora/`
- No hay nombre del autor. XOR Gate Truth Table, Symbol, Logic Diagram - Geeksforgeeks `https://www.geeksforgeeks.org/xor-gate/`
- Malwarebytes. (s.f.). Malwarebytes. Recuperado de `https://es.malwarebytes.com/malware/`
- ESET. (s.f.). Características del spam. Recuperado de `https://www.eset.com/es/caracteristicas/spam/`


[1] CryptoHack: Cursos en criptografía, `https://cryptohack.org/courses/`