

# **Network Security Lab (CY-331L)**

## **Lab Task**

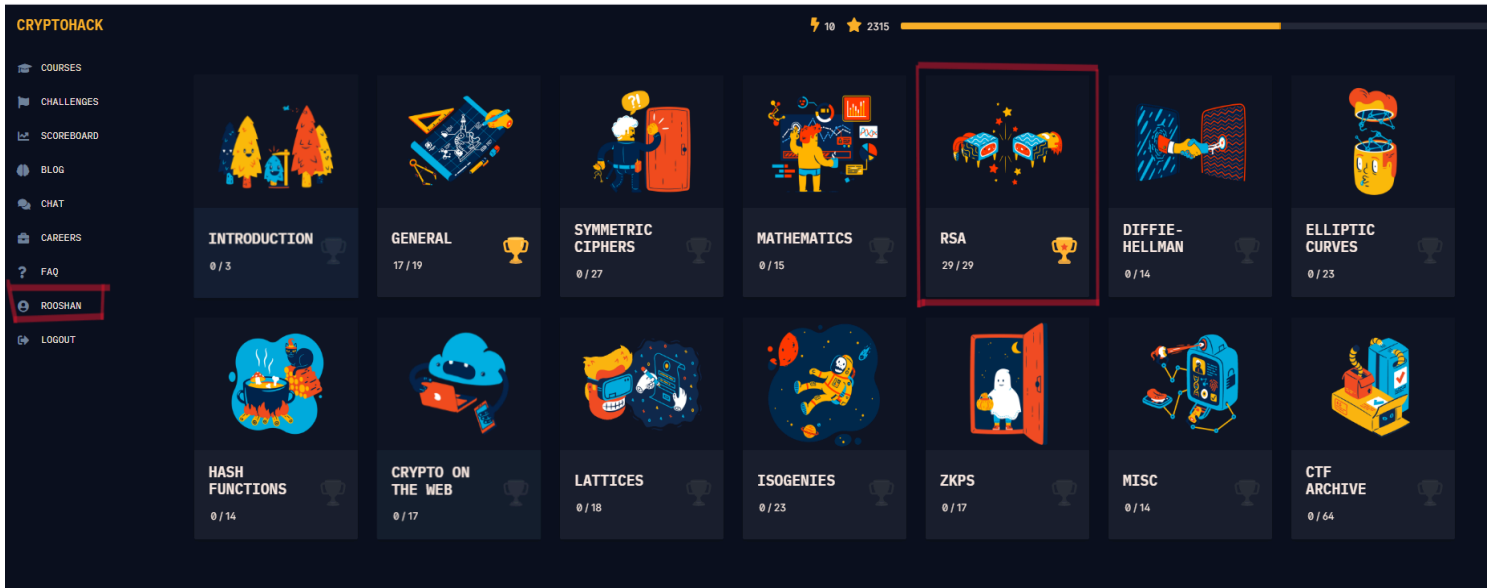


**Name: Rooshan Riaz**

**Reg No: 2022506**

# Cryptohack RSA

## Dashboard



## Starter

STARTER		Toggle
★ Modular Exponentiation	10 pts • 12081 Solves	
★ Public Keys	15 pts • 11499 Solves • 14 Solutions	
★ Euler's Totient	20 pts • 10872 Solves • 15 Solutions	
★ Private Keys	20 pts • 10263 Solves • 22 Solutions	
★ RSA Decryption	20 pts • 9913 Solves • 17 Solutions	
★ RSA Signatures	25 pts • 7595 Solves • 24 Solutions	

## Prime Part 1

PRIMES PART 1		Toggle
★ Factoring	15 pts • 7716 Solves • 13 Solutions	
★ Inferus Prime	30 pts • 5566 Solves • 12 Solutions	
★ Monoprime	30 pts • 6937 Solves • 24 Solutions	
★ Square Eyes	35 pts • 5856 Solves • 17 Solutions	
★ Manyprime	40 pts • 6124 Solves • 28 Solutions	

## Prime Part 2

PRIMES PART 2		Toggle
★ Infinite Descent	50 pts • 2766 Solves • 17 Solutions	
★ Marin's Secrets	50 pts • 2714 Solves • 19 Solutions	
★ Fast Primes	75 pts • 1828 Solves • 6 Solutions	
★ Ron was Wrong, Whit is Right	90 pts • 1719 Solves • 16 Solutions	
★ RSA Backdoor Viability	175 pts • 1279 Solves • 7 Solutions	

# Public Exponent

PUBLIC EXPONENT		Toggle
★ Salty	20 pts • 4257 Solves • 19 Solutions	
★ Modulus Inutils	50 pts • 5782 Solves • 23 Solutions	
★ Everything is Big	70 pts • 3727 Solves • 20 Solutions	
★ Crossed Wires	100 pts • 3268 Solves • 21 Solutions	
★ Everything is Still Big	100 pts • 2769 Solves • 10 Solutions	
★ Endless Emails	150 pts • 2240 Solves • 26 Solutions	

# Padding


PADDING		Toggle
★ Bespoke Padding	100 pts • 1896 Solves • 13 Solutions	
★ Null or Never	100 pts • 1216 Solves • 16 Solutions	

# Signatures

SIGNATURES PART 1		Toggle
★ Signing Server	40 pts • 1760 Solves • 12 Solutions	
★ Let's Decrypt	80 pts • 1168 Solves • 5 Solutions	
★ Blinding Light	120 pts • 1238 Solves • 14 Solutions	
SIGNATURES PART 2		Toggle
★ Vote for Pedro	150 pts • 949 Solves • 10 Solutions	
★ Let's Decrypt Again	175 pts • 562 Solves • 7 Solutions	

# TryHackMe

Learn > Wifi Hacking 101



## Wifi Hacking 101

Learn to attack WPA(2) networks! Ideally you'll want a smartphone with you for this, preferably one that supports hosting wifi hotspots so you can follow along.

📶 Easy ⌚ 0 min

Share your achievement

Start AttackBox

Help

Save Room

1433

Options

Room completed ( 100% )

Task 1 The basics - An Intro to WPA

Task 2 You're being watched - Capturing packets to attack

Task 3 Aircrack-ng - Let's Get Cracking

Created by

Room Type

Users in Room

Created

NinjaJc01

Free Room. Anyone can deploy virtual machines in the room (without being subscribed)!

51,625

1788 days ago

## Task 1:

Answer the questions below

What type of attack on the encryption can you perform on WPA(2) personal?

brute force

✓ Correct Answer

💡 Hint

Can this method be used to attack WPA2-EAP handshakes? (Yea/Nay)

Nay

✓ Correct Answer

What three letter abbreviation is the technical term for the "wifi code/password/passphrase"?

PSK

✓ Correct Answer

What's the minimum length of a WPA2 Personal password?

8

✓ Correct Answer

## Task 2:

Answer the questions below

How do you put the interface "wlan0" into monitor mode with Aircrack tools? (Full command)

airmon-ng start wlan0

✓ Correct Answer

What is the new interface name likely to be after you enable monitor mode?

wlan0mon

✓ Correct Answer

What do you do if other processes are currently trying to use that network adapter?

airmon-ng check kill

✓ Correct Answer

💡 Hint

What tool from the aircrack-ng suite is used to create a capture?

airodump-ng

✓ Correct Answer

What flag do you use to set the BSSID to monitor?

--bssid

✓ Correct Answer

💡 Hint

And to set the channel?

--channel

✓ Correct Answer

💡 Hint

And how do you tell it to capture packets to a file?

-w

✓ Correct Answer

💡 Hint

## Task 3:

Answer the questions below

What flag do we use to specify a BSSID to attack?

-b

✓ Correct Answer

💡 Hint

What flag do we use to specify a wordlist?

-w

✓ Correct Answer

💡 Hint

How do we create a HCCAPX in order to use hashcat to crack the password?

-j

✓ Correct Answer

💡 Hint

Using the rockyou wordlist, crack the password in the attached capture. What's the password?

greeneegsandham

✓ Correct Answer

💡 Hint

Where is password cracking likely to be fastest, CPU or GPU?

GPU

✓ Correct Answer

💡 Hint