Exp no 3

Date:11-02-2025

ENCRYPTION CRYPTO101

PROCEDURE

1. Log in to TryHackMe

Go to https://tryhackme.com, log in or sign up if you don't already have an account.

2. Search and Join the Room

Use the search bar and type "Crypto" or "Encryption" to find rooms like:

- **"Intro to Crypto"**
- **"Cryptography"**
- **"Encryption"**
- **"RSA", "Hashing", or "Cyber Defense - Cryptography" Click on the room you want to start with and then hit "Join Room".**

3. Start the Machine (If Required)

Some rooms offer a target machine. If so, click "Start Machine" and note the IP. For most crypto rooms, you'll solve challenges without needing a machine, just using the AttackBox or your own terminal.

4. Connect to TryHackMe Network (if needed) Use either:

- **AttackBox (just launch from the browser — already connected) •**

Or connect your own VM using:

```
bash
CopyEdit
sudo openvpn your-vpn-file.ovpn
```

5. Go Through Each Task

Each task teaches a cryptographic concept. Common topics include:

Topic	Learn About
Encoding vs Encryption	Base64, Hex, ASCII
Hashing	MD5, SHA1, SHA256, Hashcat basics
Symmetric Encryption	Caesar cipher, Vigenère, AES
Asymmetric Encryption	RSA, Public/Private Keys
Steganography	Hiding messages in files/images
Frequency Analysis	Cracking substitution ciphers

6. Use Tools and Commands Learn and apply tools such as:

- **base64, xxd, md5sum, sha256sum**
- **openssl – to encrypt/decrypt messages**
- **hashcat or john – for cracking hashes**
- **Online tools like CyberChef or dcode.fr (as allowed)**
- **gpg – for key encryption Example: bash CopyEdit**

echo "Hello" | base64 # Encoding echo
"SGVsbG8=" | base64 -d
echo -n "password" | md5sum # Hashing

7. Solve Challenges & Submit Answers Each task usually ends with a question like:
"What is the plaintext message?"
"Crack this hash."
"What encryption algorithm is used?"
Use your tools, commands, and clues to figure out the answer and submit it.

8. Mark the Room as Completed
Once all answers are submitted correctly, the room will be marked as "Completed".

INTRO

Note: to actually become familiar with Linux, you need to be using it daily. Make sure you have it installed (whether that be as your host system, a dual reboot, or on a virtual machine). For pentesting, most people prefer to use Kali.

The name "Linux" is actually an umbrella term for multiple OS's that are based on UNIX (another operating system). Thanks to UNIX being open-source, variants of Linux come in all shapes and sizes, suited best for what the system is being used for.

For example, Ubuntu & Debian are some of the more commonplace distributions of Linux because it is so extensible. I.e. you can run Ubuntu as a server (such as websites & web applications) or as a fullyfledged desktop. For this series, we're going to be using Ubuntu.

The first version of Linux was released in 1991.

Basic Commands

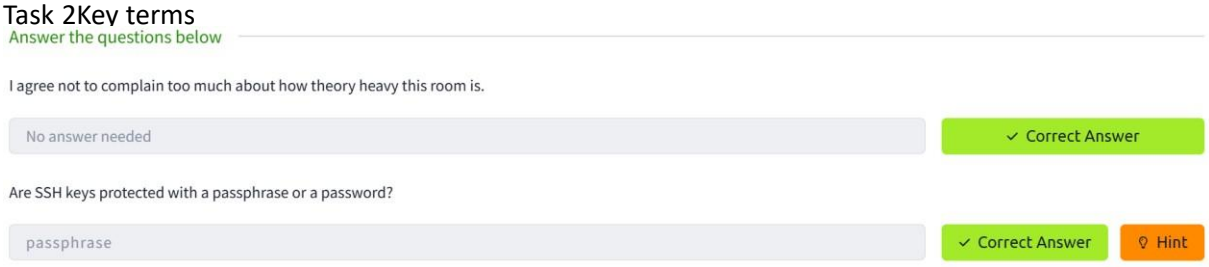
Some basic commands include pwd, ls, cd, and more.
I have listed commands and their usages in my Gitbook here.

An Introduction To Shell Operators

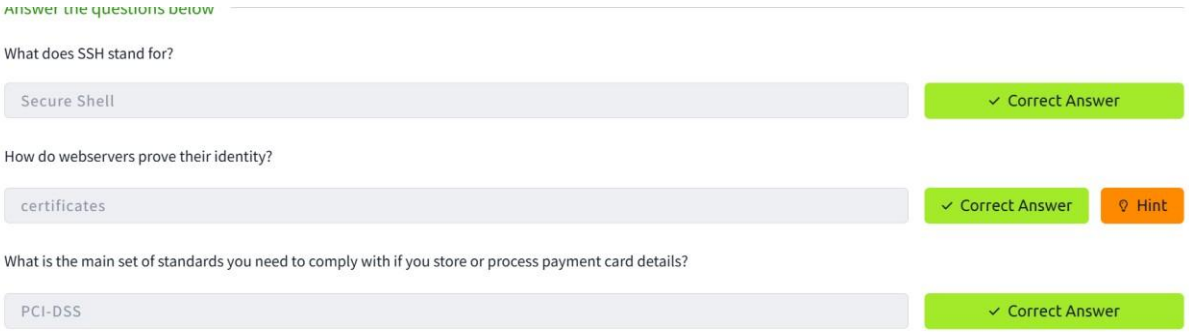
Some shell operators include &, &&, >, and >>.
I have listed commands and their usages in my Gitbook here.

TASKS

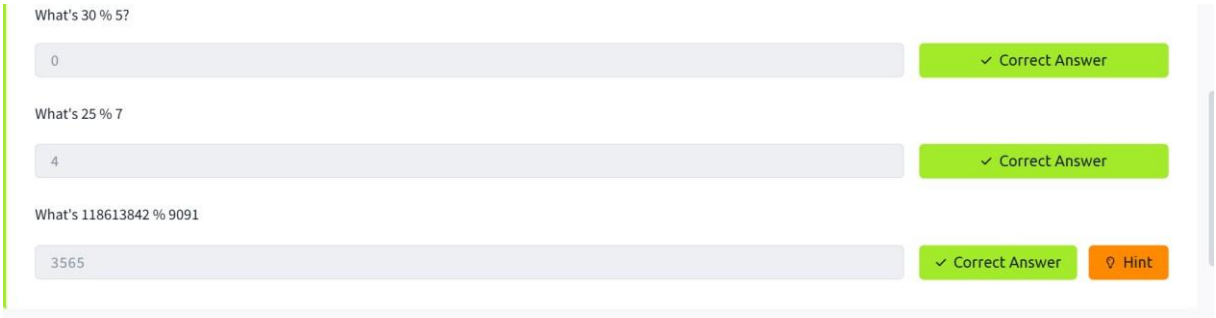
Task 2Key terms



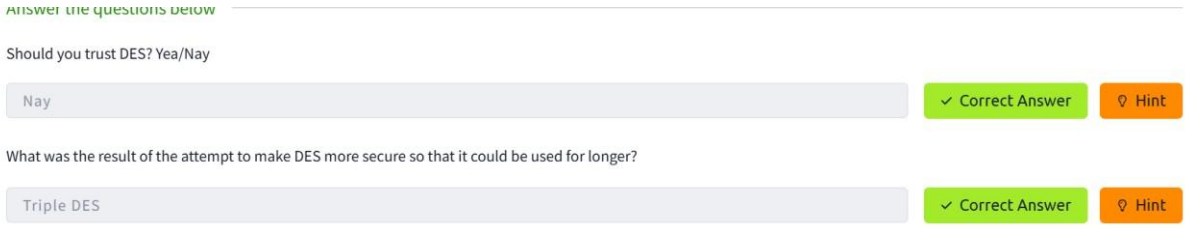
Task 3Why is Encryption important?



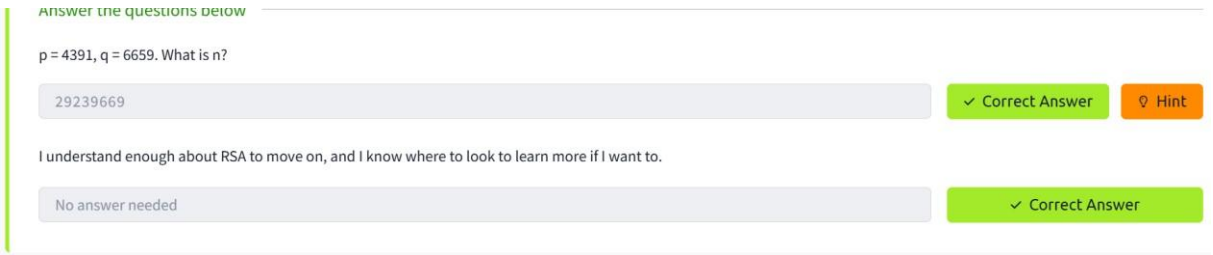
Task 4Crucial Crypto Maths



Task 5Types of Encryption

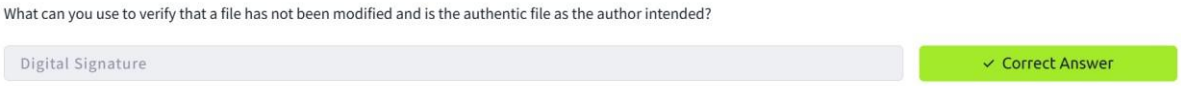


Task 6 RSA - Rivest Shamir Adleman

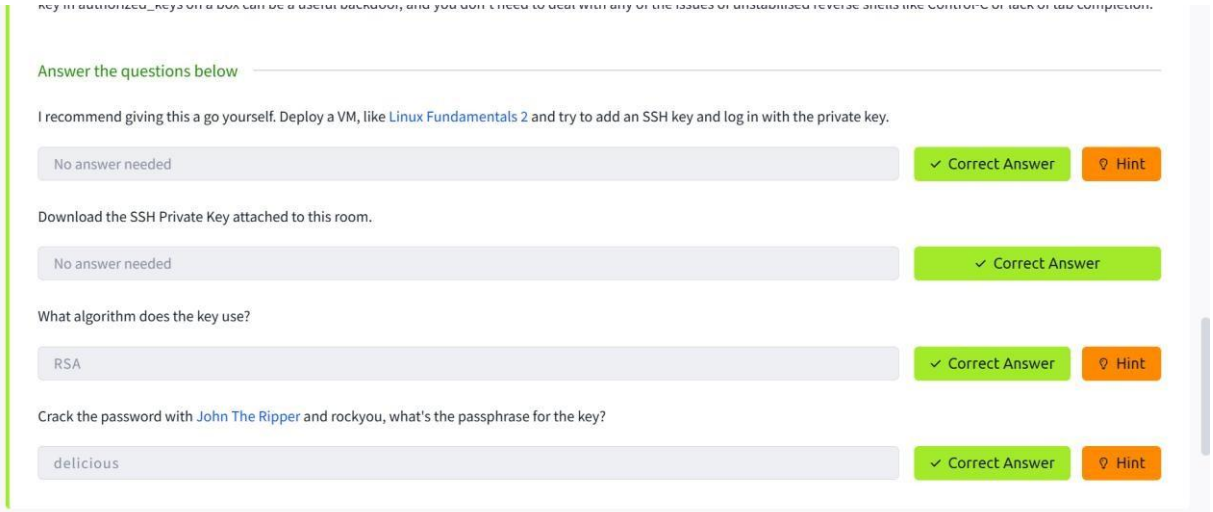


Task 7Establishing Keys Using Asymmetric Cryptography

Task 8Digital signatures and Certificates

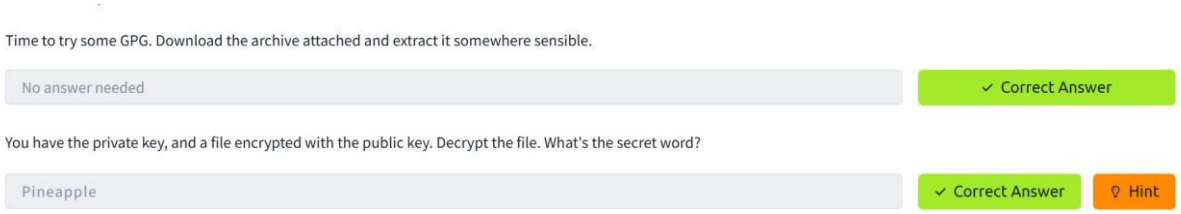


Task 9SSH Authentication



Task 10Explaining Diffie Hellman Key Exchange

Task 11PGP, GPG and AES



RESULT

Thus the introduction to Encryption crypto 101 has been sucessfully studied and implemented successfully