

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 2 Key terms

Answer the questions below

I agree not to complain too much about how theory heavy this room is.

No answer needed

✓ Correct Answer

Are SSH keys protected with a passphrase or a password?

passphrase

✓ Correct Answer

💡 Hint

Task 3 Why is Encryption important?

Answer the questions below

What does SSH stand for?

Secure Shell

✓ Correct Answer

How do web servers prove their identity?

certificates

✓ Correct Answer

💡 Hint

What is the main set of standards you need to comply with if you store or process payment card details?

PCI-DSS

✓ Correct Answer

Task 4 Crucial Crypto Maths

What's $30 \% 5$?

0

✓ Correct Answer

What's $25 \% 7$?

4

✓ Correct Answer

What's $118613842 \% 9091$?

3565

✓ Correct Answer

💡 Hint

Task 5 Types of Encryption

Answer the questions below

Should you trust DES? Yea/Nay

Nay

✓ Correct Answer

💡 Hint

What was the result of the attempt to make DES more secure so that it could be used for longer?

Triple DES

✓ Correct Answer

💡 Hint

Task 6 RSA - Rivest Shamir Adleman

Answer the questions below

$p = 4391$, $q = 6659$. What is n ?

29239669

✓ Correct Answer

🔍 Hint

I understand enough about RSA to move on, and I know where to look to learn more if I want to.

No answer needed

✓ Correct Answer

Task 7 Establishing Keys Using Asymmetric Cryptography

Answer the questions below

I understand how keys can be established using Public Key (asymmetric) cryptography.

No answer needed

✓ Correct Answer

Task 8 Digital signatures and Certificates

What can you use to verify that a file has not been modified and is the authentic file as the author intended?

Digital Signature

✓ Correct Answer

Task 9 SSH Authentication

Key management keys on a box can be a useful backdrop, and you don't need to deal with any of the issues of unauthenticated reversal arena the controls of lack of the completion.

Answer the questions below

I recommend giving this a go yourself. Deploy a VM, like [Linux Fundamentals 2](#) and try to add an SSH key and log in with the private key.

No answer needed

✓ Correct Answer

🔍 Hint

Download the SSH Private Key attached to this room.

No answer needed

✓ Correct Answer

What algorithm does the key use?

RSA

✓ Correct Answer

🔍 Hint

Crack the password with [John The Ripper](#) and [rockyou](#), what's the passphrase for the key?

delicious

✓ Correct Answer

🔍 Hint

Task 10 Explaining Diffie Hellman Key Exchange

Answer the questions below

I understand how Diffie Hellman Key Exchange works at a basic level

No answer needed

✓ Correct Answer

Task 11 PGP, GPG and AES

Time to try some GPG. Download the archive attached and extract it somewhere sensible.

No answer needed

✓ Correct Answer

You have the private key, and a file encrypted with the public key. Decrypt the file. What's the secret word?

Pineapple

✓ Correct Answer

🔍 Hint

RESULT

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

220701256

220701256