

Ex. No.: 1**Date:** 30 . 08 . 2024**CAPTURE FLAGS-ENCRYPTION CRYPTO 101****Aim:**

To capture the various flags in Encryption Crypto 101 in TryHackMe platform.

Algorithm:

1. Access the Encryption Crypto 101 lab in TryHackMe platform using the link below-
<https://tryhackme.com/r/room/encryptioncrypto101>
2. Click Start AttackBox to run the instance of Kali Linux distribution.
3. Solve the crypto math used in RSA.
4. Find out who issued the HTTPS Certificate to tryhackme.com
5. Perform SSH Authentication by generating public and private key pair using ssh-keygen
6. Perform decryption of the gpg encrypted file and find out the secret word.

Output:

The screenshot shows the TryHackMe platform interface for the 'Encryption - Crypto 101' room. At the top, there's a navigation bar with links for 'Dashboard', 'Learn', 'Compete', and 'Other'. On the right side of the header, there are icons for 'Access Machines', a search bar, and user statistics (1 challenge completed, 100% completion rate). The main content area has a teal background featuring a large illustration of a padlock and a key.

The title 'Encryption - Crypto 101' is displayed prominently, along with a subtitle 'An introduction to encryption, as part of a series on crypto'. Below the title, it says 'Medium' difficulty and '45 min' duration. There are buttons for 'Start AttackBox', 'Help', 'Save Room', 'Options', and a like count of '3537'.

A progress bar at the bottom indicates 'Room completed (100%)'. The main content area contains six expandable sections labeled 'Task 1' through 'Task 6', each with a green checkmark icon and a question. To the right of these tasks is a small circular icon with a green and blue design, and a notification box stating '5 new notifications'.

- Task 1: What will this room cover?
- Task 2: Key terms
- Task 3: Why is Encryption important?
- Task 4: Crucial Crypto Maths
- Task 5: Types of Encryption
- Task 6: RSA - Rivest Shamir Adleman

tryhackme.com/r/room/encryptioncrypto101

Complete Beginner > Cryptography > Encryption - Crypto 101

Encryption - Crypto 101

An introduction to encryption, as part of a series on crypto

Medium 45 min

Help Save Room Options

Room completed (100%)

Your machine is initializing...
Use the AttackBox to attack machines you start on tasks
Loading (18%)

Task 1 What will this room cover?

Task 2 Key terms

```
root@ip-10-10-18-189:~# ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa): myKey
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in myKey.
Your public key has been saved in myKey.pub.
The key fingerprint is:
SHA256:mYLMN1vmJnlZgFjuatvJ+ma0mK9HcIARIe//j0dXt9s root@ip-10-10-18-189
The key's randomart image is:
+---[RSA 2048]---+
| ==   .
| o.. + .
| ... o .
| ..o.o + |
| .o+ = S .
| ..o 0 o.. |
| .+ + =. . .
| +.0+=. ..
| ++*OX.   ..E |
+---[SHA256]---+
root@ip-10-10-18-189:~# ls
burp.json    Downloads    myKey.pub    Rooms          Tools
CTFBuilder   Instructions  Pictures    Scripts        welcome.txt
Desktop      myKey       Postman    thinclient_drives  welcome.txt.gpg
```

```
root@ip-10-10-18-189:~# gpg --import tryhackme.key
gpg: /root/.gnupg/trustdb.gpg: trustdb created
gpg: key FFA4B5252BAEB2E6: public key "TryHackMe (Example Key)" imported
gpg: key FFA4B5252BAEB2E6: secret key imported
gpg: Total number processed: 1
```

```
gpg: imported: 1  
gpg: secret keys read: 1  
gpg: secret keys imported: 1
```

```
root@ip-10-10-18-189:~# gpg message.gpg
```

```
gpg: WARNING: no command supplied. Trying to guess what you mean ...  
gpg: encrypted with 1024-bit RSA key, ID 2A0A5FDC5081B1C5, created 2020-06-30  
    "TryHackMe (Example Key)"
```

```
gpg: WARNING: no command supplied. Trying to guess what you mean ...  
gpg: encrypted with 1024-bit RSA key, ID 2A0A5FDC5081B1C5, created 2020-06-30  
    "TryHackMe (Example Key)"
```

Result:

Thus, the various flags have been captured in Encryption Crypto 101 in TryHackMe platform.