

Name: S RAMANITHARAN

Ex. No: 1

Roll No:231901040

## 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.

The screenshot displays the TryHackMe interface for the 'Encryption - Crypto 101' room. The top navigation bar includes links to Dashboard, Learn, Compete, and Other, along with a 'Go Premium' button and a user profile icon. The room title 'Encryption - Crypto 101' is prominently displayed, followed by a subtitle 'An introduction to encryption, as part of a series on crypto' and a difficulty level of 'Medium' with an estimated time of '45 min'. Below this, there are buttons for 'Share your achievement', 'Start AttackBox', 'Help', 'Save Room', and 'Options'. A progress bar indicates 'Room completed (100%)'. The main content area lists 12 tasks, each with a green checkmark indicating completion. The tasks are: 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, Task 7: Establishing Keys Using Asymmetric Cryptography, Task 8: Digital signatures and Certificates, Task 9: SSH Authentication, Task 10: Explaining Diffie Hellman Key Exchange, Task 11: PGP, GPG and AES, and Task 12: The Future - Quantum Computers and Encryption. At the bottom, a summary table provides room details: Created by NinjaJc01, Room Type: Free Room. Anyone can deploy virtual machines in the room (without being subscribed)!, Users in Room: 118,883, and Created: 1532 days ago.

Task	Status	Description
Task 1	Completed	What will this room cover?
Task 2	Completed	Key terms
Task 3	Completed	Why is Encryption important?
Task 4	Completed	Crucial Crypto Maths
Task 5	Completed	Types of Encryption
Task 6	Completed	RSA - Rivest Shamir Adleman
Task 7	Completed	Establishing Keys Using Asymmetric Cryptography
Task 8	Completed	Digital signatures and Certificates
Task 9	Completed	SSH Authentication
Task 10	Completed	Explaining Diffie Hellman Key Exchange
Task 11	Completed	PGP, GPG and AES
Task 12	Completed	The Future - Quantum Computers and Encryption

Created by	Room Type	Users in Room	Created
NinjaJc01	Free Room. Anyone can deploy virtual machines in the room (without being subscribed)!	118,883	1532 days ago

**Output:**

```
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.