Name: LAKSHMINARAYANAN K

Ex. No: 1 Roll No:231901027

## **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 belowhttps://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:** 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:

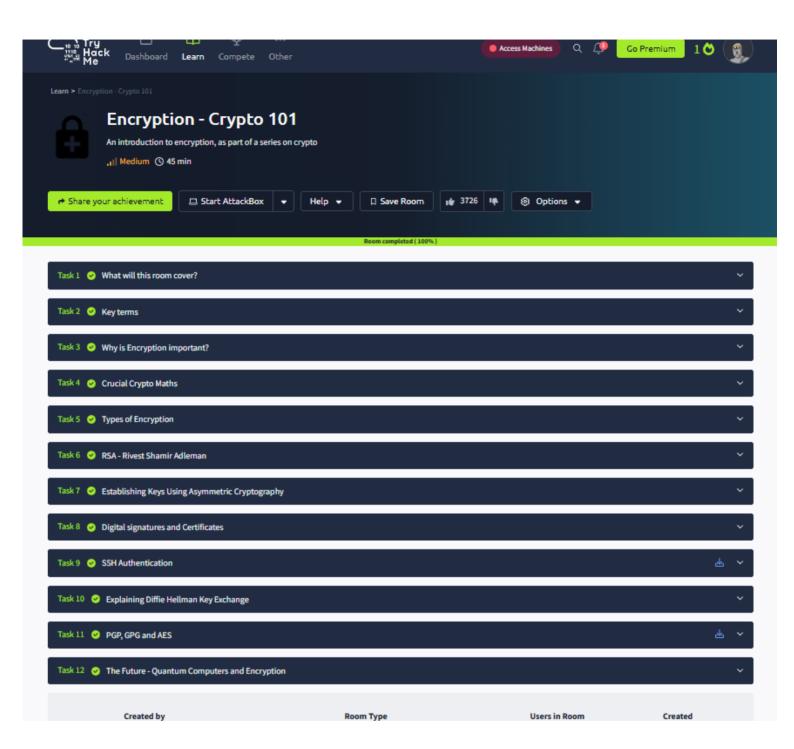
key FFA4B5252BAEB2E6: secret key imported

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.