

Name: MOHAMED ARSATH A

Ex. No: 1

Roll No:231901030

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 platform interface for the 'Encryption - Crypto 101' room. The top navigation bar includes links for Dashboard, Learn, Complete, and Other, along with buttons for Access Machines, Go Premium, and a user profile icon. The room title 'Encryption - Crypto 101' is prominently displayed, accompanied by a brief description: 'An introduction to encryption, as part of a series on crypto'. Below the title, the difficulty level is marked as 'Medium' and the estimated completion time is '45 min'. A row of interactive buttons includes 'Share your achievement', 'Start AttackBox', 'Help', 'Save Room', a like count of '3725', and an 'Options' dropdown. On the right side, there is a large illustration of a padlock and a key. The main content area lists twelve tasks, each with a green checkmark indicating completion: 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. A progress bar at the bottom indicates that the room is 100% completed.

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.