

**Name: Prem Roshan P**

**Ex. No: 1**

**Roll No:231901036**

## **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:**

Dashboard
Learn
Compete
Other
Access Machines
Go Premium
0

Learn > Encryption - Crypto 101

## Encryption - Crypto 101

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

Medium 45 min

Share your achievement
Start AttackBox
Help
Save Room
3728
Options

Room completed (100%)

Task 1 What will this room cover?

Task 2 Key terms

Task 3 Why is Encryption important?

Cryptography is used to protect confidentiality, ensure integrity, ensure authenticity. You use cryptography every day most likely, and you're almost certainly reading this now over an encrypted connection.

When logging into TryHackMe, your credentials were sent to the server. These were encrypted, otherwise someone would be able to capture them by snooping on your connection.

When you connect to SSH, your client and the server establish an encrypted tunnel so that no one can snoop on your session.

When you connect to your bank, there's a certificate that uses cryptography to prove that it is actually your bank rather than a hacker.

When you download a file, how do you check if it downloaded right? You can use cryptography here to verify a checksum of the data.

You rarely have to interact directly with cryptography, but it silently protects almost everything you do digitally.

Whenever sensitive user data needs to be stored, it should be encrypted. Standards like PCI-DSS state that the data should be encrypted both at rest (in storage) AND while being transmitted. If you're handling payment card details, you need to comply with these PCI regulations. Medical data has similar standards. With legislation like GDPR and California's data protection, data breaches are extremely costly and dangerous to you as either a consumer or a business.

**DO NOT** encrypt passwords unless you're doing something like a password manager. Passwords should not be stored in plaintext, and you should use hashing to manage them safely.

Answer the questions below

What does SSH stand for?

Secure Shell ✓ Correct Answer

How do web servers prove their identity?

Certificates ✓ Correct Answer 9 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

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

Task 12 The Future - Quantum Computers and Encryption

```
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.