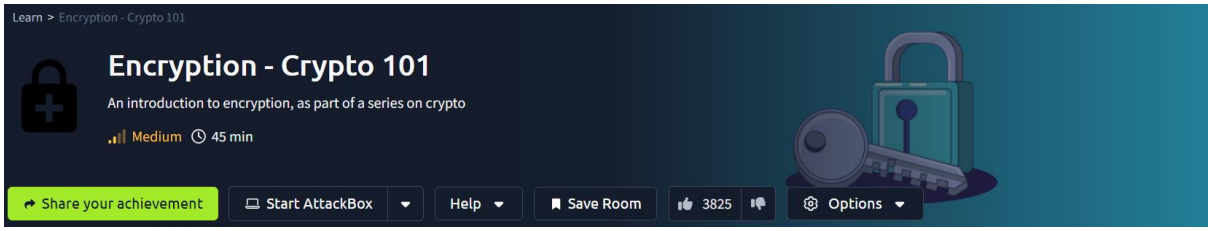

Task 2 Key terms

Answer the questions below

I agree not to complain too much about how theory heavy this room is.

No answer needed — ✓ Correct Answer

Are SSH keys protected with a passphrase or a password?

passphrase — ✓ Correct Answer — Hint

Task 3 Why is Encryption important?

Answer the questions below

What does SSH stand for?

Secure Shell — ✓ Correct Answer

How do webservers prove their identity?

certificates — ✓ Correct Answer — 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

Answer the questions below

What's 30 % 5?

0 — ✓ Correct Answer

What's 25 % 7

4 — ✓ Correct Answer

What's 118613842 % 9091

3565 — ✓ Correct Answer — Hint

Task 5 Types of Encryption

Answer the questions below

Should you trust DES? Yea/Nay

Nay ✓ Correct Answer Hint

What was the result of the attempt to make DES more secure so that it could be used for longer?

Triple DES ✓ Correct Answer Hint

Is it ok to share your public key? Yea/Nay

Yea ✓ Correct Answer

Task 6 RSA - Rivest Shamir Adleman

Answer the questions below

p = 4391, q = 6659. What is n?

29239669 ✓ Correct Answer Hint

I understand enough about RSA to move on, and I know where to look to learn more if I want to.

No answer needed ✓ Correct Answer

Task 7 Establishing Keys Using Asymmetric Cryptography

Task 8 Digital signatures and Certificates

Answer the questions below

What can you use to verify that a file has not been modified and is the authentic file as the author intended?

Digital Signature ✓ Correct Answer

Task 9 SSH Authentication

Answer the questions below

I recommend giving this a go yourself. Deploy a VM, like Linux Fundamentals 2 and try to add an SSH key and log in with the private key.

No answer needed ✓ Correct Answer Hint

Download the SSH Private Key attached to this room.

No answer needed ✓ Correct Answer

What algorithm does the key use?

RSA ✓ Correct Answer Hint

Crack the password with John The Ripper and rockyou, what's the passphrase for the key?

delicious ✓ Correct Answer Hint

Task 10 Explaining Diffie Hellman Key Exchange

Task 11 PGP, GPG and AES

Answer the questions below

Time to try some GPG. Download the archive attached and extract it somewhere sensible.

No answer needed

✓ Correct Answer

You have the private key, and a file encrypted with the public key. Decrypt the file. What's the secret word?

Pineapple

✓ Correct Answer

Hint