**RSA Custom Configuration – Dorough**

**Task 1:**

Here I find the value of N through multiplying (p-1) to (q-1). Next I calculate

Graphical user interface, text

Description automatically generated

Text

Description automatically generated

**Task 2:**

Here I encrypt message M by using

Text

Description automatically generated

Text

Description automatically generated

**Task 3:**

Decrypted cyphertext (c) using private key (D) , returns “password is dees”

Text

Description automatically generated

Text

Description automatically generated

**Task 4:**

Signing a message by encrypting it with your private key.

Text

Description automatically generated

Text

Description automatically generated

**Task 5:**

Here we decrypt the signed message with the sender’s public key to recover the original message which can be compared to the encrypted message sent separately to verify the message’s integrity.

Text

Description automatically generated

Text

Description automatically generated

**Task 6:**

Using the steps provided in the text, I retrieved the certificates from a web request and recovered the encryption prime value, the signed text, and the shared number. From here you verify the integrity of the message.

Text

Description automatically generated

