P = 29   Q = 31

N = (29)(31) = 899

Z = (28)(30) = 840

E = 29

D = 29

Public key = (N, E) ,   Private Key = (N , D)

Letter	m	m^e	
G	7	7^{29} = 3,219,905,755,813,179,726,837,607	C = 7^{29} mod 899 = 877

877^{29} =
22232495220053313238550319156403346297406109462146681372806532712898863498678648395037

877^{29} Mod 899 = 7

Sign/Encrypt Files - Kleopatra

? **✕**

Sign / Encrypt Files

Prove authenticity (sign)

☑ Sign as: ✅ Mohammad Alhourani <C00227505@itcarlow.ie> (certified, created: 22/03/2021) ⌄

Encrypt

☐ Encrypt for me: ✅ Mohammad Alhourani <C00227505@itcarlow.ie> (certified, created: 22/03/2021) ⌄

☑ Encrypt for others: ✅ Cliona Hayden <C00225401@itcarlow.ie> (certified, OpenPGP, created: 22/03/2021) ⌫

👥 Please enter a name or email address...

☐ Encrypt with password. Anyone you share the password with can read the data.

Output

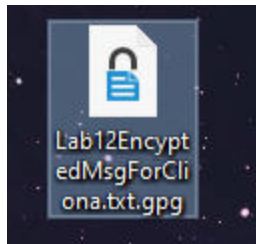☐ Encrypt / Sign each file separately.

🔒 C:/Users/neron/OneDrive/Desktop/Lab12EncyptedMsgForCliona.txt.gpg ⌫ 📁

Sign / Encrypt **Cancel**

📝 Lab12EncyptedMsgForCliona.txt - Notepad

File Edit Format View Help

This is an encrypted message For Cliona Hayden

These are screenshots from cliona decrypting my message

Lab12EncyptedMsgForCliona.txt - Notepad

File   Edit   Format   View   Help

This is an encrypted message For Cliona Hayden

Lab12Encypt
edMsgForCli
ona.txt

Decrypt/Verify Files - Kleopatra   ?   ×

Output folder: C:/Users/Cliona/Downloads

All operations completed.

100%

Lab12EncyptedMsgForCliona.txt.gpg → Lab12EncyptedMsgForCliona.txt: **The data could not**   Show Audit Log
be verified.

Signature created on Monday 22 March 2021 11:40:49
With certificate:
Mohammad Alhourani <C00227505@itcarlow.ie> (2985 4FE1 FBE3 2FFF)
The used key is not certified by you or any trusted person.

Save All   Discard