TASK 4 ADVANCED ENCRYPTION TOOL

- Encryption: Encryption is the process of converting readable data (plaintext) into an unreadable format (ciphertext), while decryption is the reverse process, converting ciphertext back into plaintext. Encryption is used to protect data from unauthorized access, and decryption is used to make the data accessible to authorized users
- This process transforms data into a secret code, making it unreadable to anyone without the correct key or algorithm. This is essential for protecting sensitive information during transmission or storage

- Decryption: This process reverses the encryption, using the correct key or algorithm to convert the ciphertext back into its original, readable form (plaintext)

- Purpose: Encryption and decryption work together to ensure data confidentiality and integrity. They allow authorized parties to access and use information while preventing unauthorized individuals from doing so

- Examples: Encryption and decryption are used in various applications, including:
- Secure web browsing (HTTPS): SSL/TLS protocols encrypt data transmitted between a web browser and a website.
- Secure email: Protocols like PGP and S/MIME encrypt email content, protecting it from unauthorized access during transit.
- Data at rest: Encryption protects data stored on hard drives or cloud storage.
- Data in transit: Encryption safeguards data while it's being transmitted over networks.

TOOL USED TO PERFORM ENCRYPTION AND DECRYPTION IS:

- I am using tools to perform encryption and decryption is

- BC TEXT ENCODER
- This is the tool used for both encryption and decryption of the text files and folders
- BC Text Encoder is an open-source tool I have downloaded the tool from chrome and extracted exe
- Open BC text encoder tool and give the text file you want to encode
- Hear I am giving a text file named cyber.txt
- Then create a public key/Secrete pair by using BC Text encoder tool
- Give the required details like friend name and password and algorithm and create a secrete key pair and save the output to a text file.

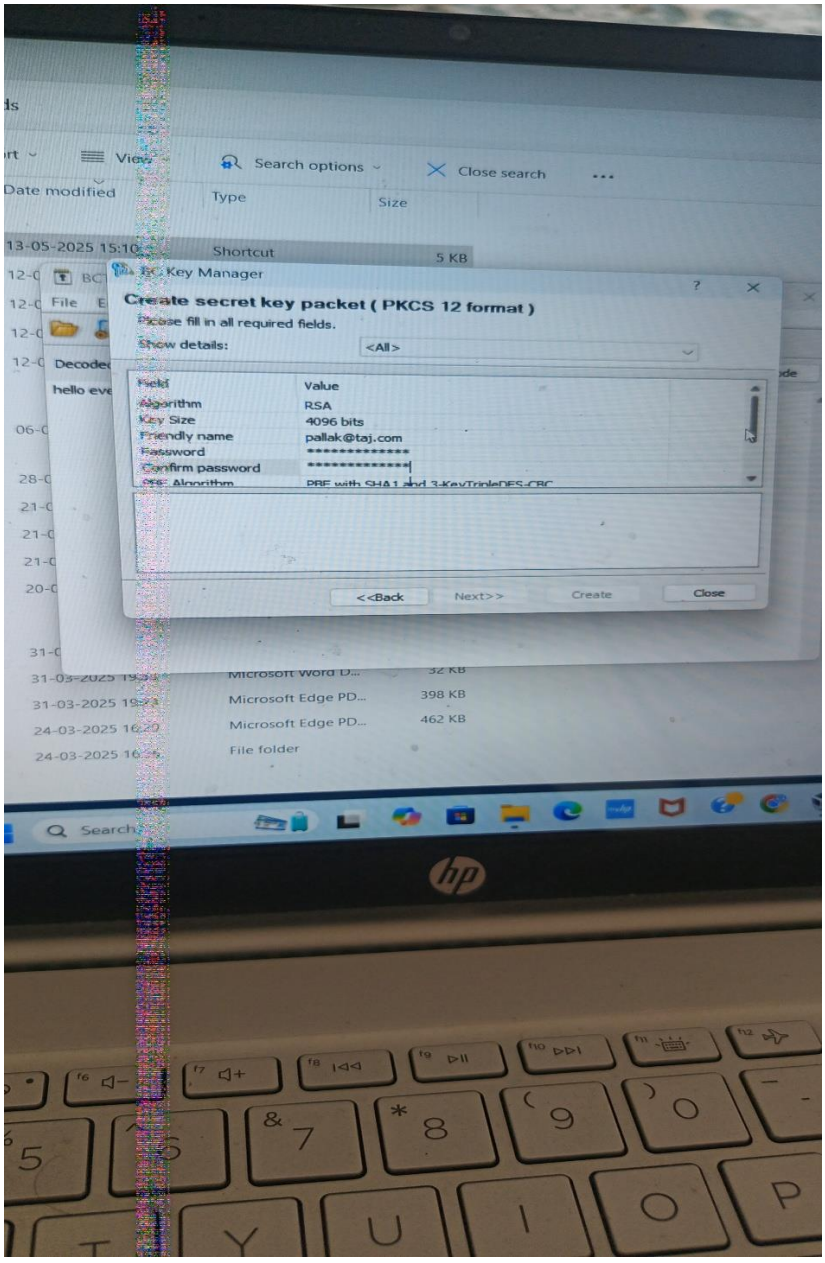

Image 4.1 shows generation of public key secret pair using BC- text encoder

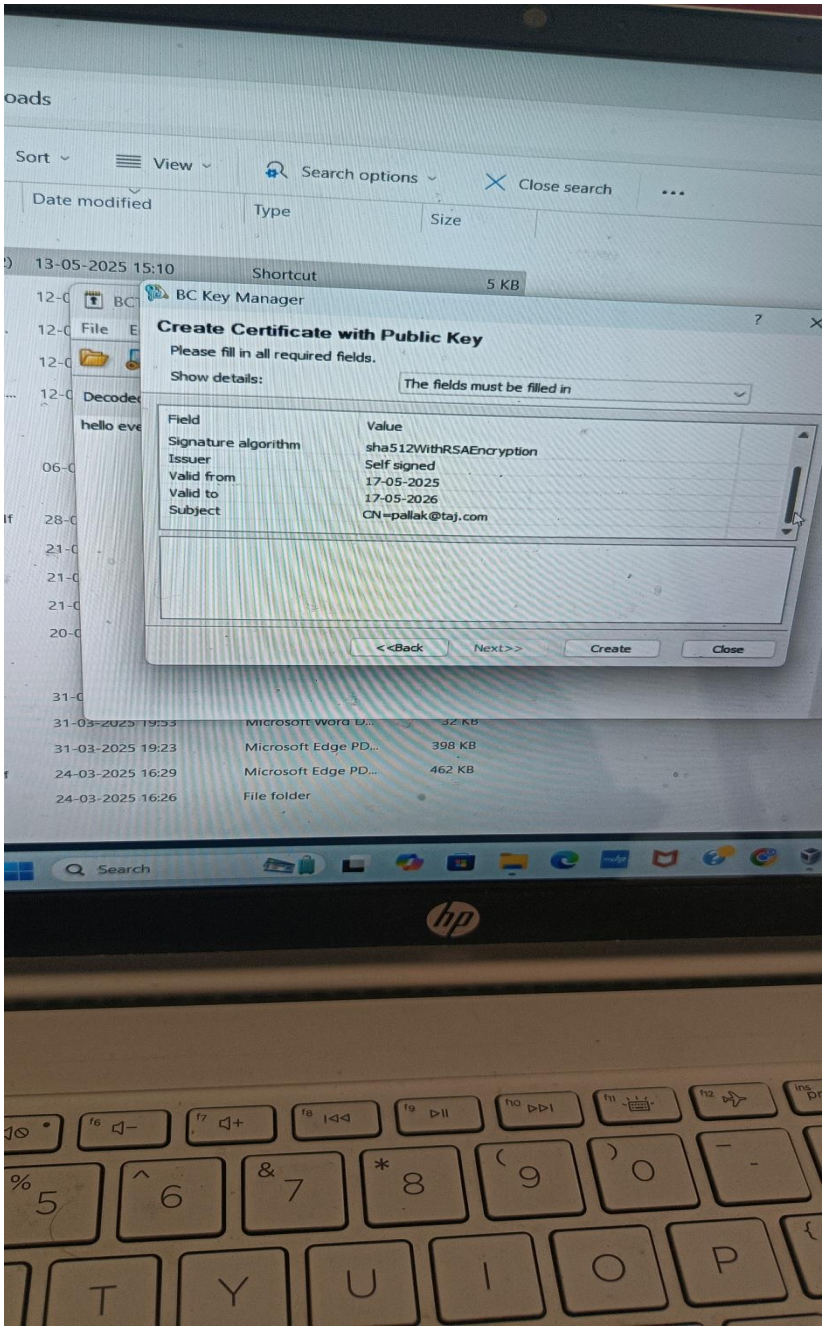

Image 4.2 shows generation of certificate with public key using BC Text encoder tool

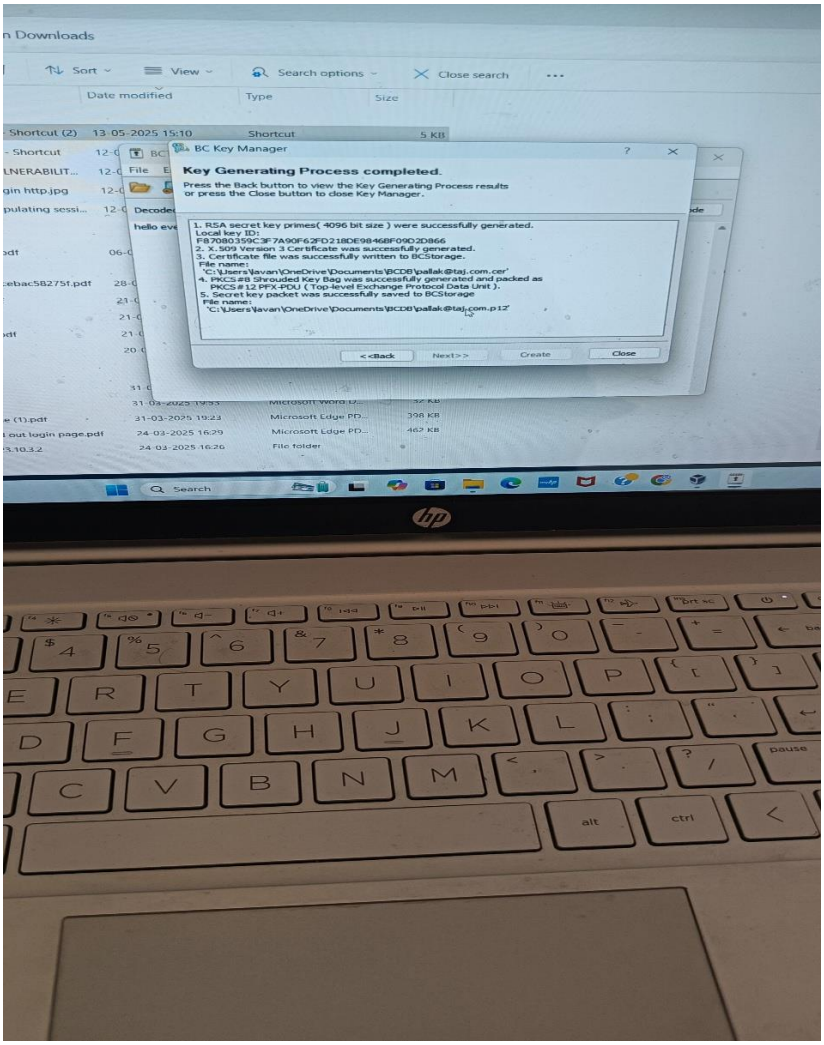

Image 4.3 show successful key generation process and its output folder path

- After public key is created by BC text encoder its out put is saved to a folder after the key generation save the output to a folder
- NOW I am going insert that file in the document

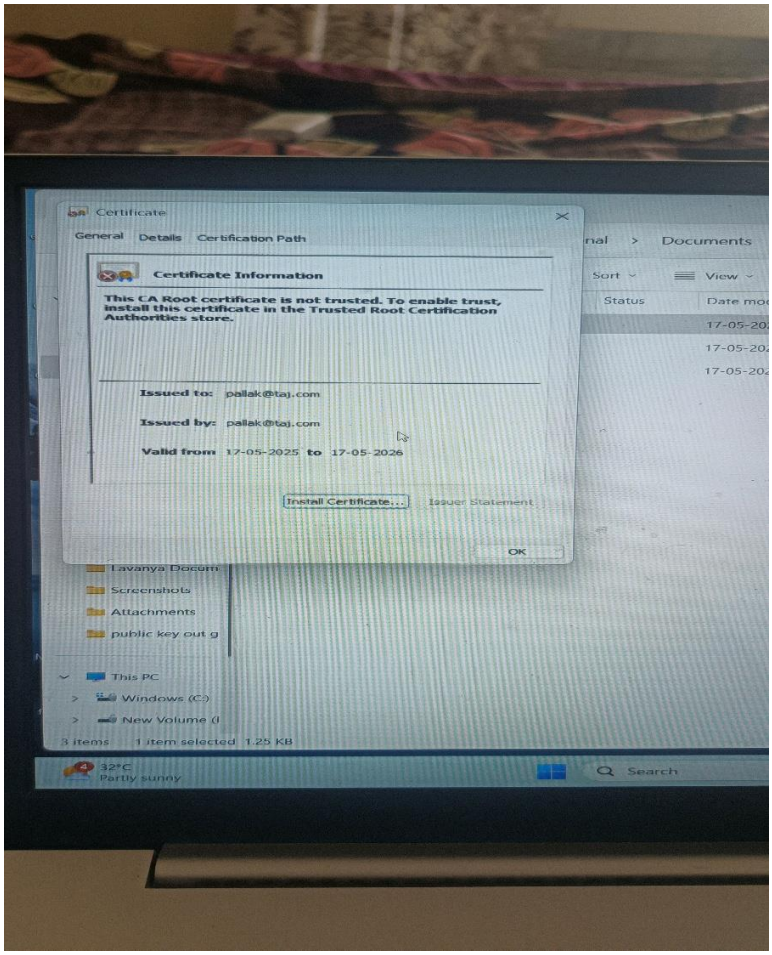

Image 4.4 shows certificate information of the created public key secret pair.

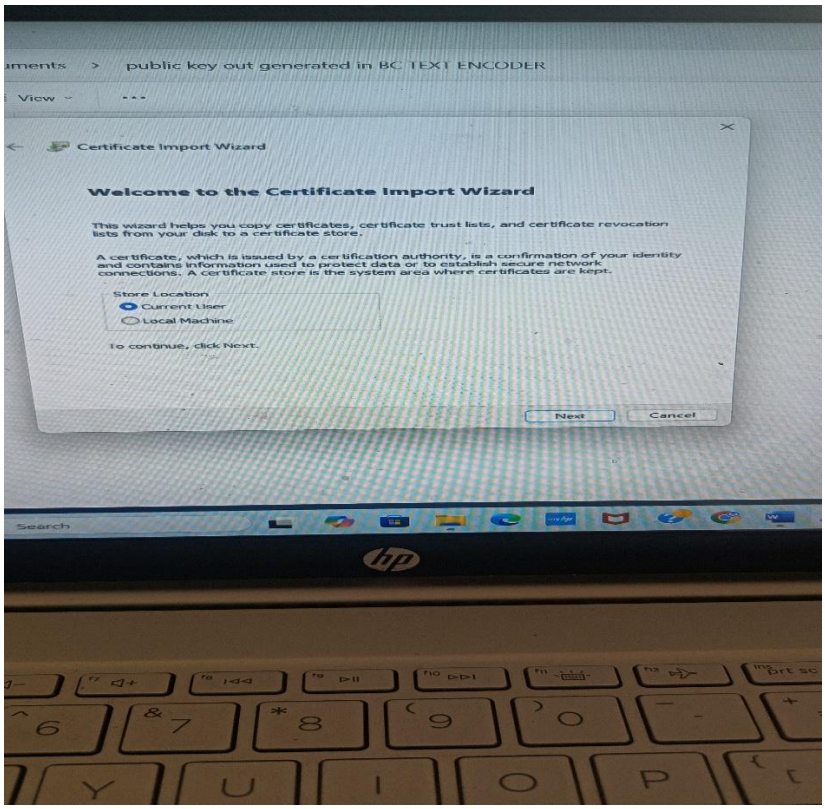

Image 4.5 shows certificate import wizard created using BC text encoder tool

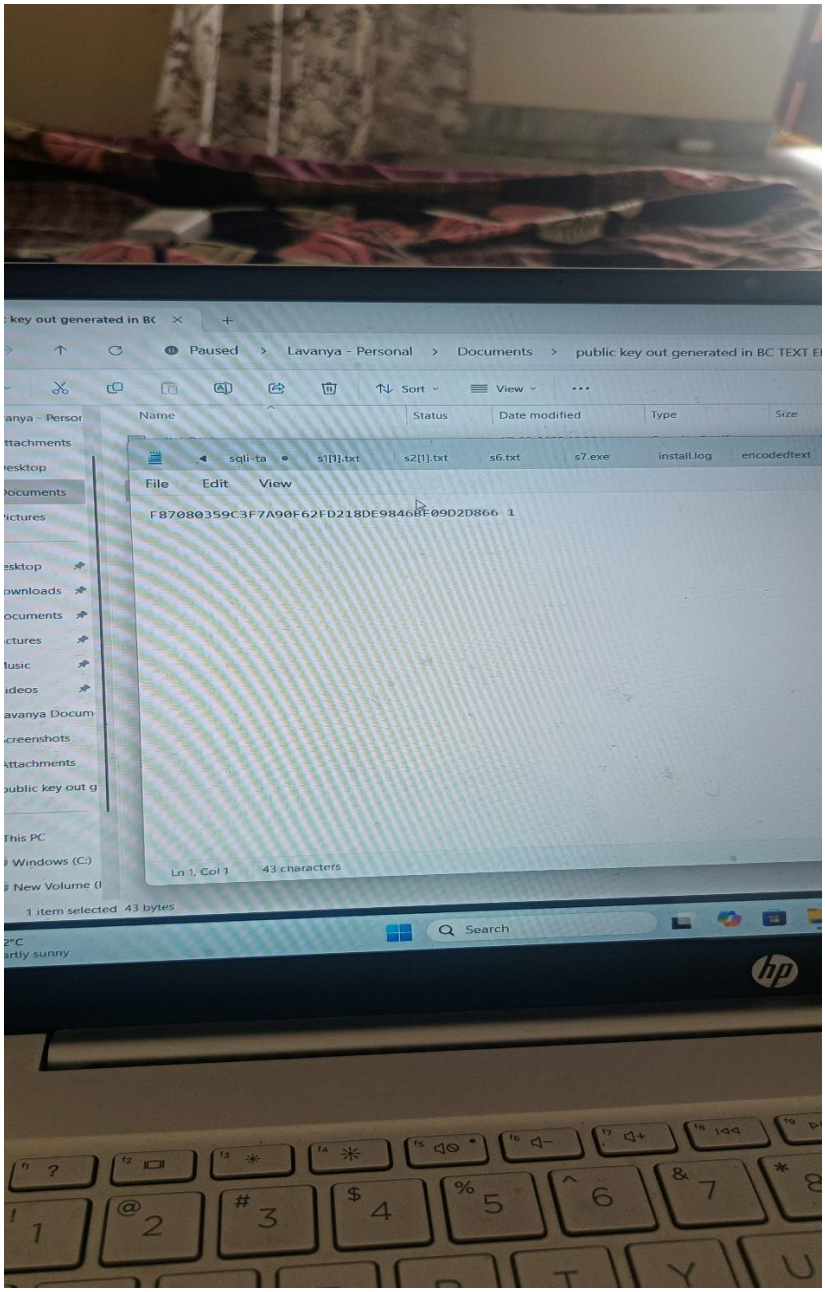

Image 4.6 shows the secret key pair generated by public key RSA algorithm using BC text encoder tool

ENCODING PLAIN TEXT USING PASSWORD

- Now I am going to encode the plain text in a file by using password
- I have encoded a text file named cyber.txt using password and save output of the encoded message to a text file

- Now I am inserting the image of encoded message file

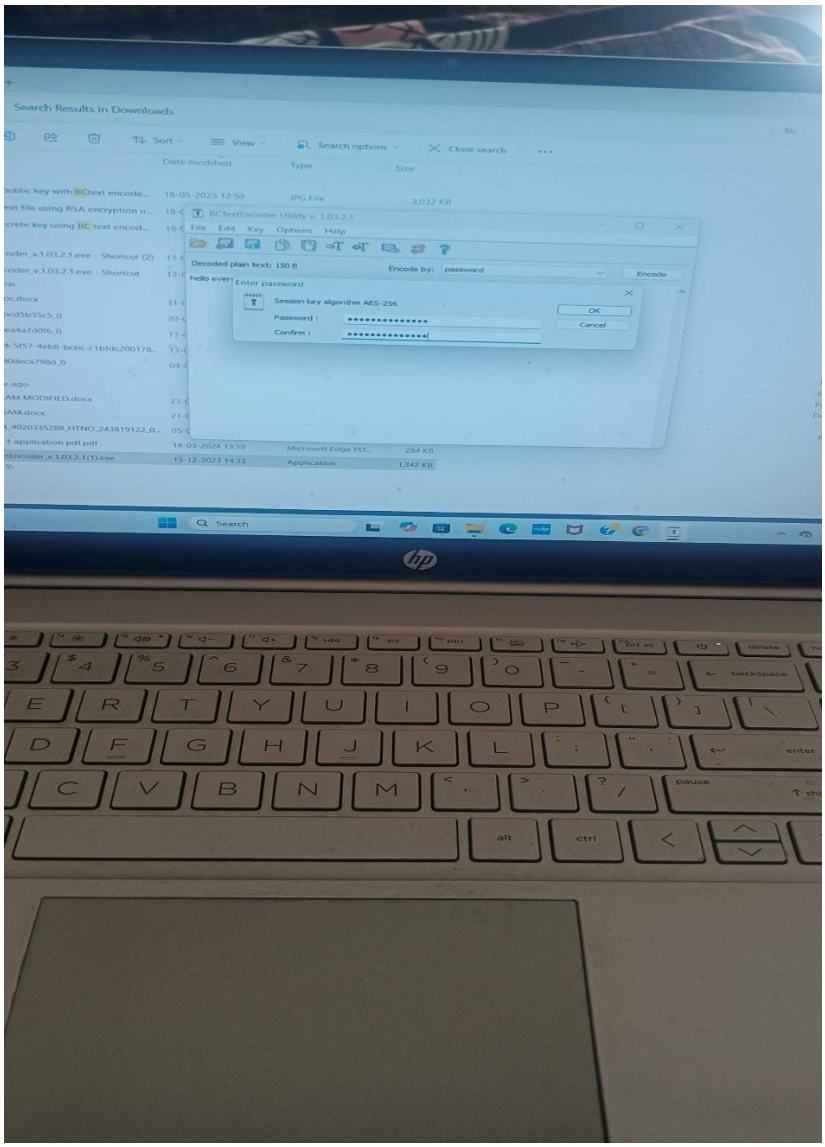

Figure 4.7 shows encoding text file using password by using BC Text encoder tool

- Now I am inserting the output file of encoded text

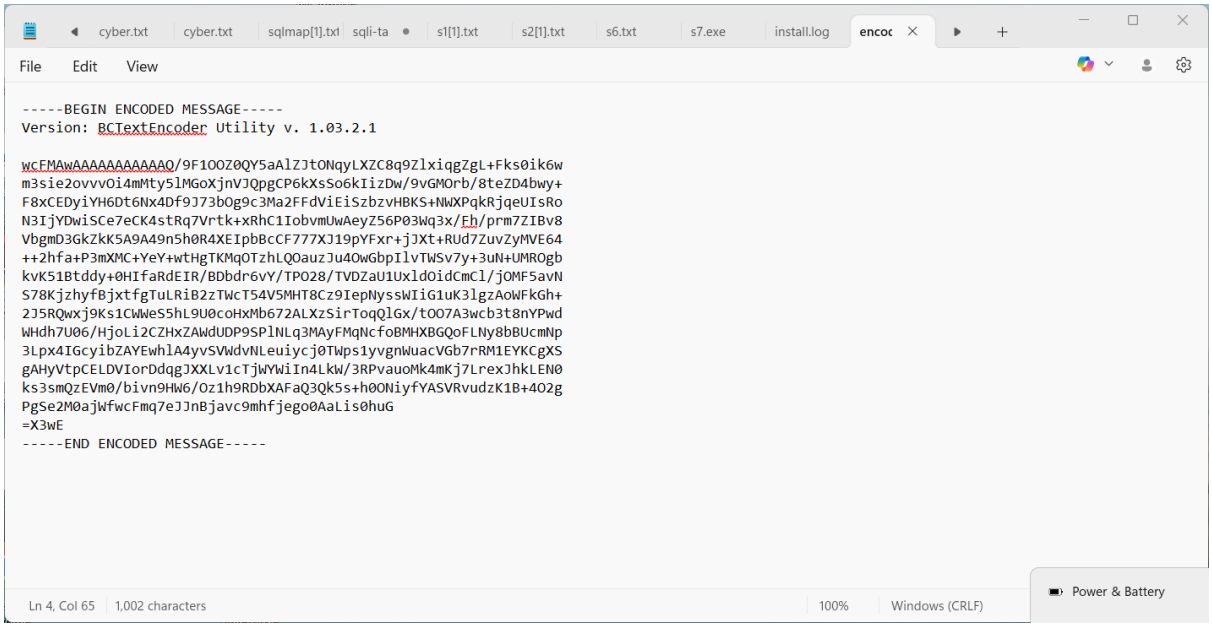

Figure 4.8 shows encrypted output of encoded text file

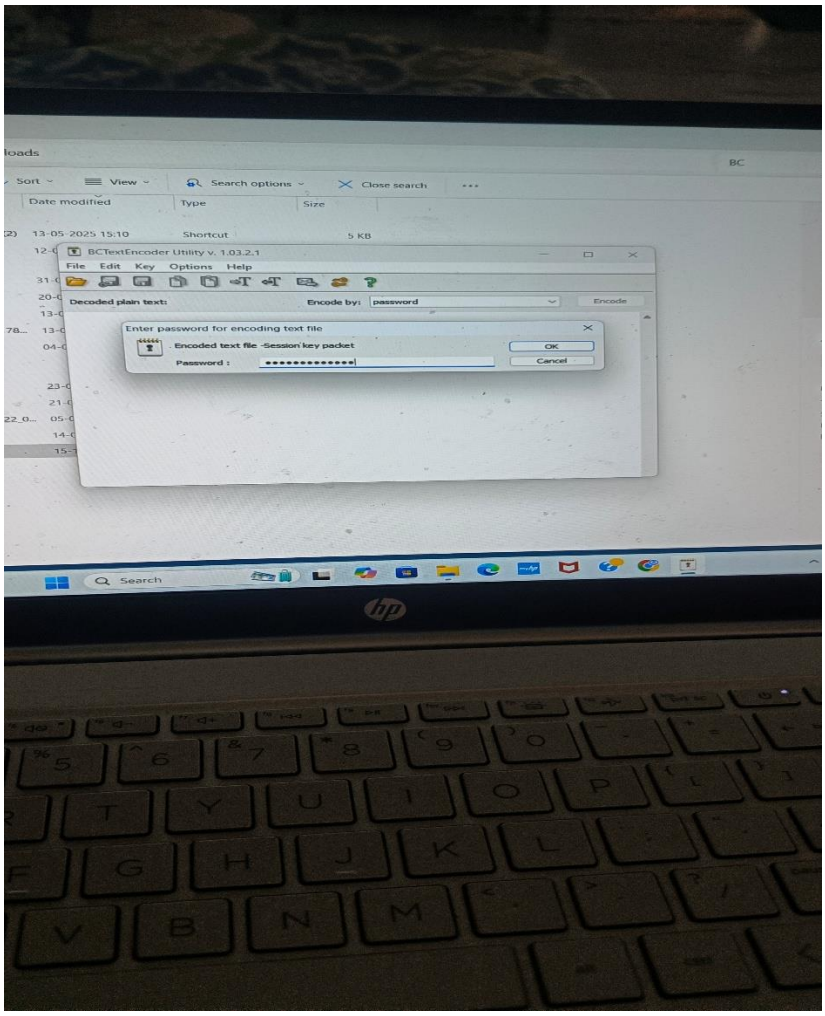

Figure 4.9 shows decrypting text file by entering password used during Encoding using BC text encoder tool

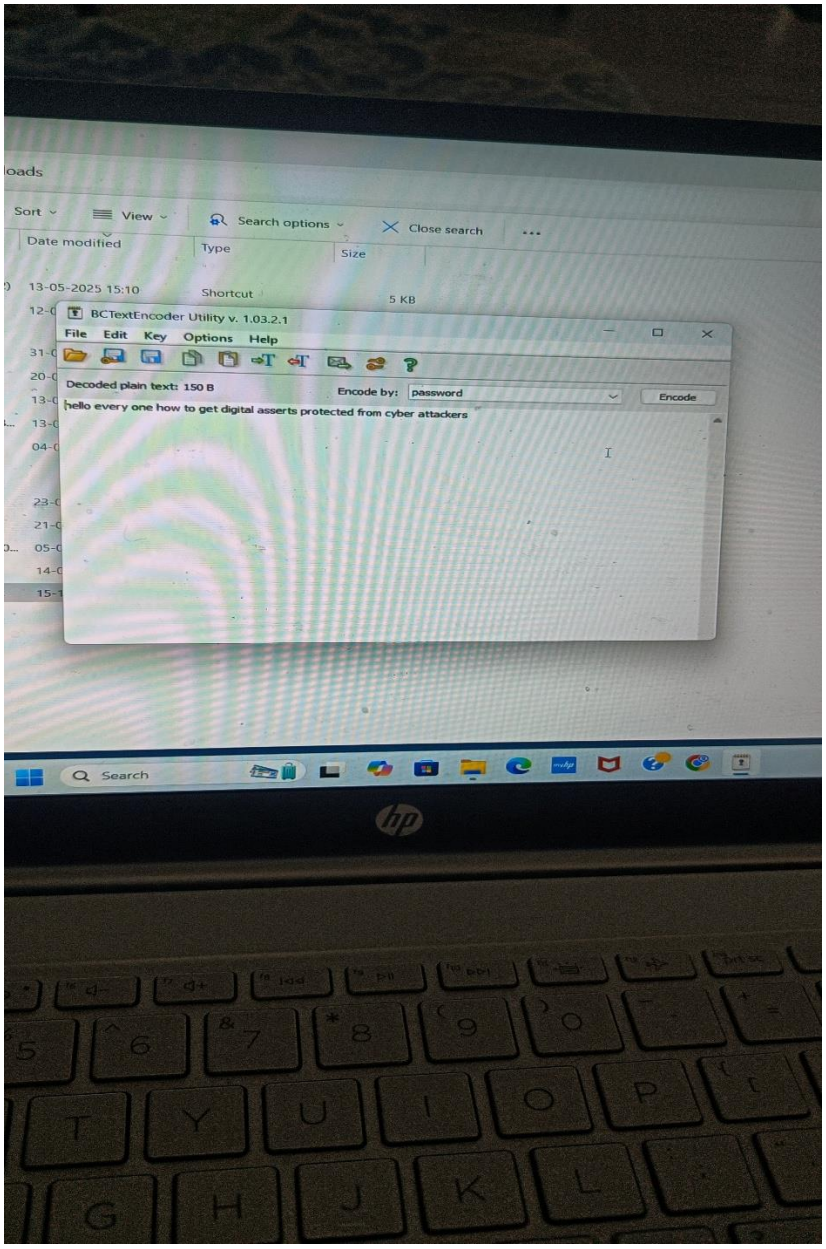

Figure 4.10 shows decoded plan text of a file using BC text encoder tool.