# Encrypt and decrypt the data in image file using quick stego tool and command prompt

Encryption is the method by which information is converted into secret code that hides the information's true meaning. The science of encrypting and decrypting information is called cryptography.

In computing, unencrypted data is also known as plaintext, and encrypted data is called ciphertext. The formulas used to encode and decode messages are called encryption algorithms, or ciphers.

To be effective, a cipher includes a variable as part of the algorithm. The variable, which is called a key, is what makes a cipher's output unique. When an encrypted message is intercepted by an unauthorized entity, the intruder has to guess which cipher the sender used to encrypt the message, as well as what keys were used as variables. The time and difficulty of guessing this information is what makes encryption such a valuable security tool.

Encryption has been a longstanding way for sensitive information to be protected. Historically, it was used by militaries and governments. In modern times, encryption is used to protect data stored on computers and storage devices, as well as data in transit over networks.

Decryption is a process that transforms encrypted information into its original format. The process of encryption transforms information from its original format — called plaintext — into an unreadable format — called ciphertext — while it is being shared or transmitted

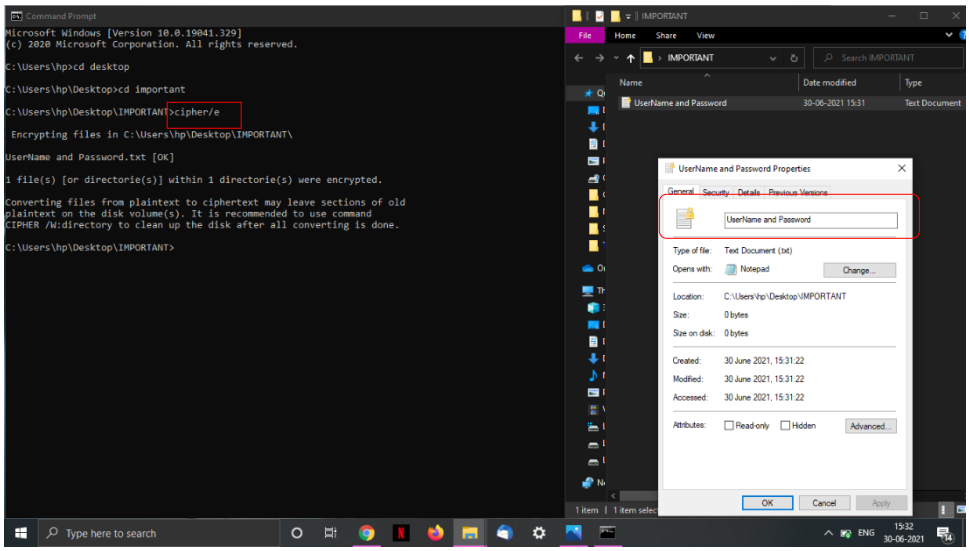
1.Opening an image in quick stego tool and opening a text to encrypt into the image.

2.This is the image where the data from a confidential document is encrypted

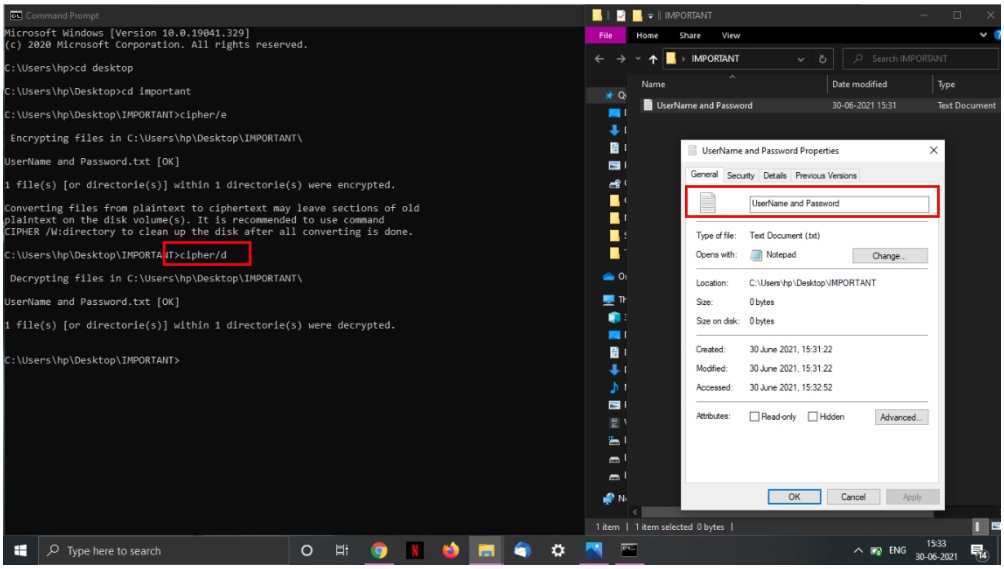
3.In this Screenshot, the data encrypted in the image is decrypted.

Encrypting confidential data in a file by using Command prompt window.

1. Opening the command prompt window and changing the directory to the “important” window and encrypting the file by using encrypt cipher command.




2.Decrpting the file by using decrypt cipher command.



**Advantages of cryptography and steganography:**

**Cryptography:**

Confidentiality − Encryption technique can guard the information and communication from unauthorized revelation and access of information.

Authentication − The cryptographic techniques such as MAC and digital signatures can protect information against spoofing and forgeries.

Data Integrity − The cryptographic hash functions are playing vital role in assuring the users about the data integrity.

Non-repudiation − The digital signature provides the non-repudiation service to guard against the dispute that may arise due to denial of passing message by the sender.

**Steganography:**

One-Way Hashing :- Used to ensure that a third party has not tampered with a sent message. This is accomplished by creating a hash of the message using a fixed character length for every item in the message, when the original items are in fact of variable character length. The hash is encrypted and sent with the message. When the recipient receives the message it is decoded. If the hash from the decoded message does not match the hash from the encrypted message, both the sender and recipient of the message know that it has been tampered with. Attaching Text to an Image: - Explanatory notes are attached to an image. In the medical profession this could be used when one medical office sends an image to another medical office. If the sending medical office needs to include explanatory notes of what the receiving medical office should be focusing on, this could be accomplished with steganography Hiding Information: - Steganography can also be used to protect identities and valuable data from theft unauthorized viewing, or potential sabotage by concealing the message within a unsuspicious image.

In conclusion, I have encrypted and decrypted data in an image file by using “Quick stego” tool and also the command prompt