**IMAGE ENCRYPTION USING JAVA**

**Introduction**

With the growth of technology several computing devices likes computers, laptops, or mobiles are connected with each other. New networks are being installed and connected to a global internet. A major issue for computer network is to prevent the confidential information that is transmitted over the network being disclose with the unauthorized users or illegal users. For this reason’s encryption techniques are used to prevent data from others. Most encryption techniques have an easy implementation and are widely used in the field of Information Security.

**Information Security**

Information security is a set of strategies for managing the processes, tools and policies necessary to prevent, detect, document and counter threats to digital and non-digital information. Infosec responsibilities include establishing a set of business processes that will protect [information assets](https://whatis.techtarget.com/definition/information-assets) regardless of how the information is formatted or whether it is in transit, is being processed or is [at rest](https://searchstorage.techtarget.com/definition/data-at-rest) in storage.

Infosec programs are built around the core objectives of the [CIA triad](https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA): maintaining the [confidentiality](https://whatis.techtarget.com/definition/confidentiality), [integrity](https://searchdatacenter.techtarget.com/definition/integrity) and [availability](https://searchstorage.techtarget.com/definition/data-availability) of IT systems and business data. These objectives ensure that sensitive information is only disclosed to authorized parties (confidentiality), prevent unauthorized modification of [data](https://searchdatamanagement.techtarget.com/definition/data) (integrity) and guarantee the data can be accessed by authorized parties when requested (availability).

**Cryptography**

Cryptography is an art of using mathematics to encrypt or decrypt data. It is a technique of making a cryptosystem that is capable of providing information security. It enables us to store sensitive information or transmit it across an insecure network (like Internet) so that it cannot be read by anyone except the authorized user.

While cryptography is an art of securing data, “Cryptanalysis” is an art of analysing and breaking the secure communication. Cryptology is a combination of both Cryptography and Cryptanalysis.

A cryptographic algorithm is a mathematical function used for both encryption and decryption process, it works in a combination with a key (a word, number or phrase) to encrypt the plain text to produce cipher text. The same plain text encrypts to a different cipher text with the use of different key. Therefore, the security of the data entirely depends upon two things- the strength of the cryptographic algorithm and the secrecy of the key. The combination of all the possible keys, cryptographic algorithm and all the encrypted protocols in the network forms the cryptosystem.

**Encryption**

Encryption is the method by which plaintext or any other type of data is converted from a readable form to an encoded version that can only be decoded by another entity if they have access to a decryption key. Encryption is one of the most important methods for providing data security, especially for end-to-end protection of data transmitted across networks.

Encryption is widely used on the internet to protect user information being sent between a browser and a server, including passwords, payment information and other personal information that should be considered private. Organizations and individuals also commonly use encryption to protect sensitive data stored on computers, servers and mobile devices like phones or tablets.

**Decryption**

Decryption is the process of transforming data that has been rendered unreadable through encryption back to its unencrypted form. In decryption, the system extracts and converts the garbled data and transforms it to texts and images that are easily understandable not only by the reader but also by the system. Decryption may be accomplished manually or automatically. It may also be performed with a set of keys or passwords.

One of the foremost reasons for implementing an encryption-decryption system is privacy. As information travels over the World Wide Web, it becomes subject to scrutiny and access from unauthorized individuals or organizations. As a result, data is encrypted to reduce data loss and theft. Some of the common items that are encrypted include email messages, text files, images, user data and directories. The person in charge of decryption receives a prompt or window in which a password may be entered to access encrypted information.