# 

**Text Message Encryption and Decryption**

# **Requirements**

## **Introduction:**

In today's Digital world where every piece of information is sent and received through the internet or text messages (SMS or WhatsApp). It is important for the messages to be encrypted and safely delivered to and from the two (or more) using parties. There are several methods of Encrypting the given message (Public/ Private Key, Symmetric key, Diffie-Hellman algorithm, DES, etc.). These algorithms are quite difficult to break into, and provide security for the user/s.



Network security is an area of tremendous focus for companies of all sizes. Whether a corporation or a small-to-medium sized business (SMB), a target for a variety of network attacks can stop your business in its tracks.

The most common types of attacks include:

1. Malware/ Ransomware
2. Trojan horse
3. Computer Virus and Worms
4. Phishing Attacks
5. Denial of Service
6. Man in The Middle Attack
7. Spying

While most of these cases require a fire and verification wall. Many fire-walls use Secret Keys and cryptographic messages to verify the authenticity of the sender. These encrypted keys help keep the sender and receiver safe from any hacker lurking nearby. Encryption of messages helps keep the data safe from potential eavesdropping and hijacking.

## **Reason for Encryption**

[Encryption](https://en.wikipedia.org/wiki/Encryption) is the process through which data is encoded so that it remains hidden from or inaccessible to unauthorized users. It helps protect private information, sensitive data, and can enhance the security of communication between client apps and servers. In essence, when your data is encrypted, even if an unauthorized person or entity gains access to it, they will not be able to read it.

To encrypt data, an encryption key uses an encryption algorithm to translate (encode) plaintext or readable data into unreadable data or cipher text. Only the corresponding decryption key can decode the scrambled cipher text back into readable plaintext. How the encryption is done and what type of encryption is used gets much more complex.

**Symmetric Key:** Both the encryption Key and the decryption Key are the same. If any were to get their hands on the key, the data exchanged between the two parties is no longer safe and is in need of a new replacement. This encryption is fast and easy to achieve. Symmetric algorithm are commonly used for bulk data encryption.

**Asymmetric Key:** There are two separate key present. They are connected via a mathematical relationship. One is usually referred as a ‘Public Key’, while the other is referred as the ‘Private Key’. The Public Key is used for distribution while the Private Key is used for decrypting the data. The algorithm is comparatively slower a s it requires huge computation power.