# 

**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 protects your network and data from breaches, intrusions and other threats. This is a vast term that describes hardware and software solutions as well as processes. It even imposes the rules and configurations relate to network use, accessibility and overall threat protection. Network Security involves access control, virus and antivirus and antivirus software, application software, network analytics, firewall, VPN encryption and more.

Network Security is vital when it comes to protection of client data and information. Keeping the shared data secure, ensuring reliable access, network performance as well as protection from cyber threats is a **threat.**

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**

There have over 3,800 data breaches reported at the end of June and over 4.1 billion records exposed, 2019 was on the track to become the worst year on record for data breaches according to a report recently published by Risk Based Security. The number of breaches has increased by a staggering 54% from 2018’s midyear estimates.

Data breaches, while disastrous in themselves, never come alone. They are often followed by steep fines and customer loss of trust. Worst yet: 60% of small businesses go bankrupt within 6 months of a data breach. Companies are increasingly aware of the reality of these harsh figures and have started investing in data security strategies which aim to protect data and keep intruders out.

Encryption has emerged as a key component of these strategies and a way to secure data from malicious outsiders or the carelessness of employees. However, some organizations still hesitate when it comes to encryption due to a lack of understanding of its usefulness or the fear that its implementation may encumber networks and bring down employees’ efficiency. Encryption, however, is one of the most powerful and useful tools in the data security arsenal. Here are the most important reasons why:

1. Last line of Defense
2. Protects the data on the go
3. Helps with compliance

[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.

Encryption keys are broadly divided into:

**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.

In this project we will be using a symmetric Key Encryption. (For both the layers)

## **Defining the system:**

### **SWAT Analysis:**