XOR and Shift Encryption Algorithm

Orkun ÇINAR   
Computer Engineering  
Dokuz Eylul UniversityIzmir, Turkey  
orkuncinar9@hotmail.com

*Abstract*—This study proposes a shifting and XOR-based encryption technique. The technique creates a series of key values using a key schedule, which are then used to both encrypt and decode plaintext messages. The Python-based technique offers robust encryption with no computational cost. The suggested algorithm gives flexible key scheduling that is simple to adjust to meet various security needs. In several applications, the algorithm may be used to protect sensitive information.

Keywords—XOR, shifting, python, encryption, decryption

# Introduction

A key component of information security is encryption, which offers a way to shield sensitive data from unwanted access. There have been many different encryption algorithms created over time, from straightforward substitution ciphers to intricate block ciphers. Shifting and XOR operations are two basic methods of encryption that make it easy and quick to convert plaintext into ciphertext.

We provide an unique encryption technique based on XOR and shifting operations in this work. The suggested technique creates a series of key values using a key schedule, which are then applied to and removed from a plaintext message. The technique is intended to offer robust encryption with little computational cost, making it appropriate for usage in contexts with limited resources.

The round number and the current key value are subjected to left shifts and XOR operations in order to create the key schedule. By conducting XOR and shifting operations on each character of the message, the resultant key values are utilized to encrypt and decode it. After that, the message is decrypted using the same key values and procedures, but in reverse.

Python is used to carry out the suggested algorithm. The implementation has tools for creating a key schedule, encrypting and decrypting messages, and publishing the outcomes. The features integrate with current software systems and are designed to be simple to use.

Considering the proposed method to current encryption techniques, there are various benefits. First off, it simply requires simple arithmetic operations and is straightforward to implement. Second, it offers reliable encryption with little computational overhead, making it appropriate for usage in contexts with limited resources. Lastly, it provides a variable key scheduling that is simple to adjust to meet various security needs.

Overall, the suggested method offers an easy-to-implement encryption solution that is both straightforward and effective. The technique may be applied to secure network communications, embedded systems, mobile devices, and other types of sensitive data. Both developers and security experts find it to be a desirable alternative due to its flexibility and effectiveness.