Implementations of 30+ Cryptography Algorithms in Rust

Saurabh Gupta

June 2024

Abstract

This is the abstract of your document. It should provide a brief summary of your work, typically in about 150-300 words. The abstract gives readers a quick overview of your paper's main points and conclusions.

Contents

1 Introduction

Cryptography is the practice of secure communication

2 Simple Substitution

Simple substitution ciphers are basic encryption techniques where each letter in the plaintext is replaced by another letter or symbol in the ciphertext.

2.1 Additive

The additive cipher, also known as Caesar cipher, shifts each letter of the alphabet by a fixed number of positions.

$$E(x) = (x + k) \bmod 26 \tag{1}$$

Where $E(x)$ is the encrypted letter, x is the original letter (as a number from 0-25), and k is the shift key.

2.2 Multiplicative

In a multiplicative cipher, each letter is multiplied by a fixed number (modulo 26).

$$E(x) = (ax) \bmod 26 \tag{2}$$

Where a is the multiplication key, which must be coprime to 26.

2.3 Affine

The affine cipher combines both additive and multiplicative methods:

$$E(x) = (ax + b) \bmod 26 \tag{3}$$

Where a and b are the keys, and a must be coprime to 26.