
# Hajee Mohammad Danesh Science and Technology University,Dinajpur-5200

**Department of Computer Science and Engineering**
**Level : 3, Semester : II**

## A Report on A Cryptography Algorithm

**Course Code:** CSE 361
**Course Title:** Mathematical Analysis for Computer Science

**Prepared By**
Fariha Tasneem Feya
ID: 2102006

**Submitted To**
Pankaj Bhowmik
Lecturer
Department of Computer Science and Engineering

**Submission Date:** 4 July 2025

# Algorithm Name: Mod-X Cipher

## 1. Introduction

This is a simple symmetric encryption algorithm that combines modular arithmetic and bitwise XOR operations to provide basic confidentiality. It uses a single numeric key K shared between the sender and receiver to perform both encryption and decryption which makes it a symmetric algorithm. This algorithm operates on the ASCII values of characters.

## 2. Notations

P: Plaintext (original message)
C: Ciphertext (encrypted message)
K: Secret key (a positive integer, $0 \leq K \leq 255$)
P[i]: i-th character of plaintext
C[i]: i-th character of ciphertext
ord(x): ASCII value of character x
chr(x): Character corresponding to ASCII value x

## 3. Encryption Algorithm

**Input:**
A string P (plaintext)
An integer key K

**Output:**
A string C (ciphertext)

**Procedure:**
1. Initialize empty string C ← ""
2. For each character P[i] in P:
a. val ← (ord(P[i]) + K) mod 256
b. val ← val XOR K
c. C ← C + chr(val)
3. Return C

## 4. Decryption Algorithm

**Input:**
A string C (ciphertext)
An integer key K

**Output:**

A string P (recovered plaintext)

**Procedure:**
1. Initialize empty string P ← ""
2. For each character C[i] in C:
a. val ← ord(C[i]) XOR K
b. val ← (val - K + 256) mod 256
c. P ← P + chr(val)
3. Return P

# 5. Flowchart

## 5.1 Encryption

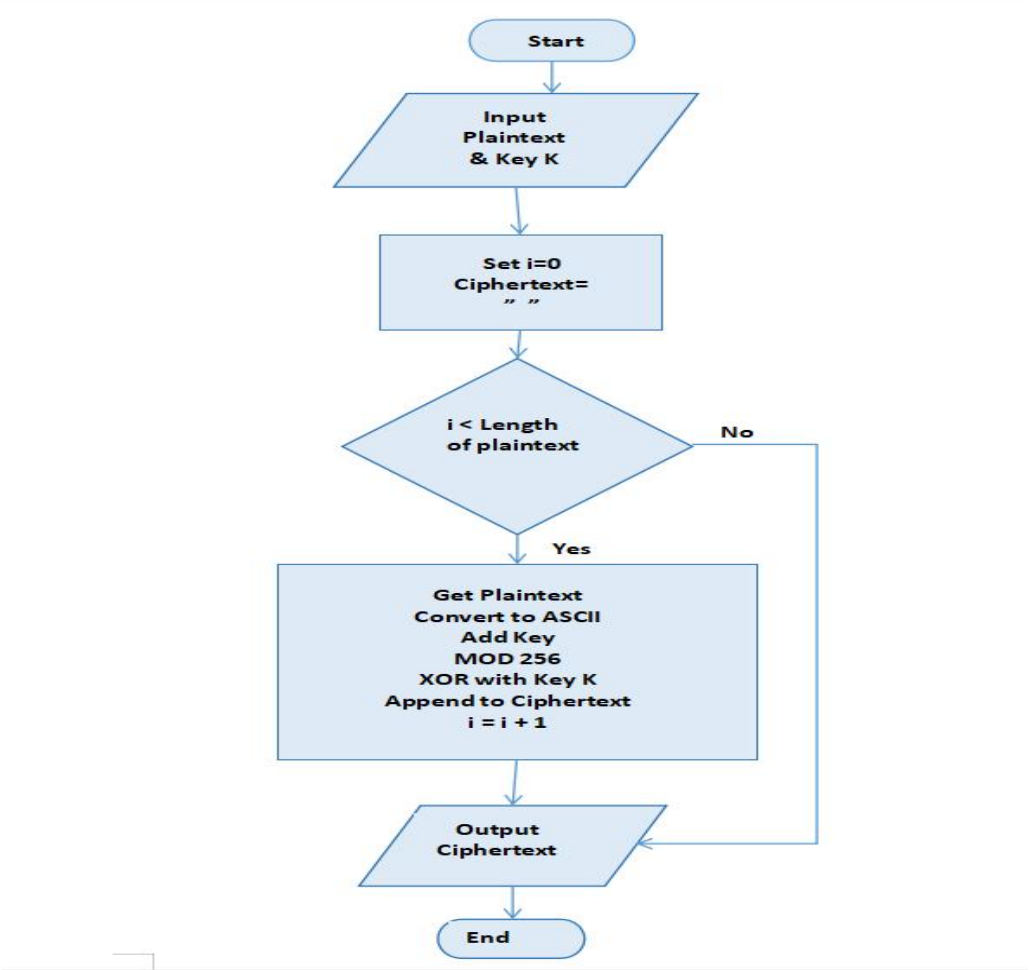


**Figure 5.1: Encryption Algorithm Flowchart**

### 5.2 Decryption

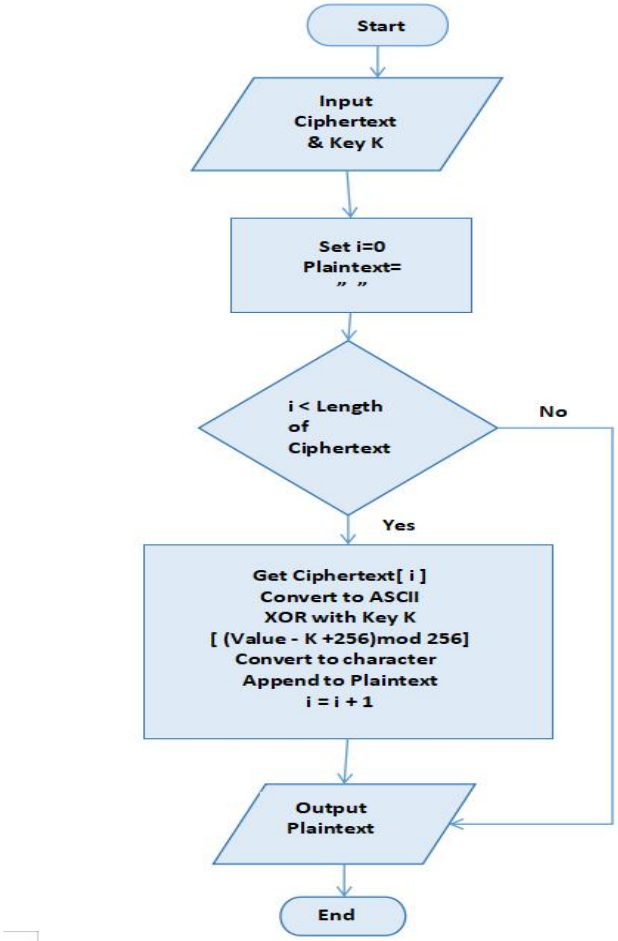


**Figure 5.2: Decryption Algorithm Flowchart**

## 6. Example Test Case

Input:
Plaintext: "HELLO"
Key: K = 23

Encryption (step-by-step for 'H'):
ord('H') = 72
(72 + 23) mod 256 = 95
95 XOR 23 = 72
chr(72) = 'H'

Final Output:
Encrypted text: "HKttq"
Decrypted text: "HELLO"

## 6. Conclusion

The Mod-X Cipher is symmetric, the same key is used for both encryption and decryption. It ensures reversibility by applying XOR and modular arithmetic. It can encrypt all standard ASCII characters (0–255).