Week 1 Submission: Ideation & Problem Definition

**Project Title:** Modular Shift-XOR Cipher (MSXC): A Lightweight Symmetric Encryption Algorithm for Secure Data Transmission

**Submitted by Group A members:**

Hamza Mohamud Ahmed

Mohamed Abdikarim Mohamud

Hussein Mohamud Hussein

Mahad Abdi Mohamud

Mohamed Hassan Mohamed

Mohamud Abdullahi Ahmed

Osman Ahmed Nur

Adnan Mukhtar Mohamud

Qali Mire Osman

Muna Dirshe Omar

Muna Isse Ali

**Course:** Information Security

**Instructor:** Eng. Adam Muhudin

**Date:** 01/06/2025

**Introduction**

Cryptography is the study of how to turn plain text, which is easy to read, into cipher text, which is hard to read. Encryption makes sure that only people with a secret key can turn the encrypted text back into its original form. This keeps communication safe. Cryptography is necessary in the digital world to ensure that traits such as integrity, confidentiality, authentication, and non-repudiation function properly.

Symmetric encryption is a simple approach to encrypt and decrypt data that uses the same secret key for both. A lot of people use it because it works well and can be used in many different ways, like keeping data safe and protecting communication connections. In symmetric encryption, there are two main ways to do it: substitution and transposition.

Substitution ciphers work by replacing the letters or symbols in the plaintext with other letters or symbols to mask the original message. The old-fashioned Caesar cipher, for instance, transfers each letter of plain text a certain number of spaces in the alphabet. Substitution does make things a little less apparent, but it doesn't modify the language's statistical features. This means that frequency analysis can be done when it's used statically.

Transposition ciphers, on the other hand, change where the letters are in the plaintext without changing who they are. This strategy makes it tougher to crack the code since the plaintext's statistical properties are spread out across the cipher text. Classic transposition ciphers break the direct link between the places of the plaintext and cipher text when you change the order of the letters or use a given key.

Symmetric ciphers have developed from fundamental classical methods, like the Caesar, Vigenère, Playfair, and Hill ciphers—each with unique benefits and drawbacks—into more sophisticated algorithms such as the Advanced Encryption Standard (AES). AES keeps data safe by using numerous layers of substitution-permutation networks. These new methods are very safe, but they might not function in areas with low resources, such embedded systems or Internet of Things (IoT) devices, because they are too hard to calculate.

As the need for encryption that works and is secure develops, especially in places with few resources, we need cryptographic solutions that are light and don't put security at risk. Encryption solutions must be secure and simple enough for teachers to use in the classroom so that students can learn basic cryptography concepts in real-life situations.

This study presents the **Modular Shift-XOR Cipher (MSXC)**, a novel symmetric encryption technique that mostly falls within the substitution cipher classification, while integrating sophisticated elements such as position-dependent transformations and modular arithmetic. **MSXC** is more complex and less predictable than typical replacement methods since it changes the mapping for each character based on its position and key-derived values all the time. **MSXC** additionally uses a special block rearranging approach that is like transposition to mix up the cipher text even more and get rid of its underlying structure. The most essential thing is that **MSXC** is harder to hack using brute-force and statistical assaults because it uses a modular ASCII masking technique to add another layer of obfuscation.

**MSXC** is a good choice for low-power devices and instructional purposes since it can incorporate the basic cryptographic notions of substitution and transposition into a design that is both lightweight and adaptable. **MSXC** intends to fill the gap between simple ciphers and the current encryption standards by developing a symmetric encryption solution that is safe, effective, and easy to use. It does this by combining ancient and new cryptographic ideas.

**1.2 Problem Statement and Gap in Existing Methods**

now are a lot of symmetric encryption systems out now, but most of them can be placed into two broad groups: current block ciphers and classical substitution ciphers. AES and other modern block ciphers are quite safe, but they take a lot of processing power since they need to do a lot of complicated key scheduling, padding, and block operations. Substitution ciphers from the past are easy to use but not very safe, and they are typically open to frequency analysis.

When employed for lightweight encryption, several symmetric ciphers still use block structures. This can make things more difficult and cost more to handle at times. AES and other block ciphers are very safe, however they don't work well when there aren't enough resources, such in embedded systems and Internet of Things devices. These systems need encryption solutions that are both quick and safe.

Another issue with typical substitution ciphers is that each character in the plaintext always matches up with a character in the cipher text. You can break this mapping with frequency analysis, which looks at linguistic patterns to figure out what the original message was. The biggest problem with these kinds of methods is that they can't dynamically replace, which lets attackers detect patterns in encrypted data that keep coming back.

The **Modular Shift-XOR Cipher (MSXC)** fixes these concerns by adding dynamic key evolution to the process of encryption. MSXC's key shifts and **XOR** operations are not the same for all characters. They rely on both the character's position and the secret key. This method makes the cipher text less predictable by employing rotating keys and modular arithmetic to make it safer. MSXC makes the cipher text more complicated and spread out without the extra work that block ciphers need, hence it is lightweight.

The new Problem Statement now explains how the **MSXC** algorithm's dynamic replacement technique works with modular arithmetic and spinning keys. This method seeks to fix the difficulties with standard substitution ciphers while still being quick enough for times when resources are constrained.

**1.3 Research Objectives and Contribution**

This study introduces and analyzes the **Modular Shift-XOR Cipher (MSXC)**, a novel symmetric encryption method aimed at overcoming the deficiencies of conventional encryption systems. The primary objectives of the inquiry are:

* To formulate a symmetric encryption technique employing modular arithmetic and position-dependent key shifts to create dynamic substitution mappings that vary according to the secret key and the location of the plaintext character.
* **To ensure the encryption process is lightweight**, enabling practical application on devices with limited resources, such as **Internet of Things (IoT) sensors** and **embedded microcontrollers**.
* **To evaluate MSXC’s security characteristics**, focusing on its resilience against **frequency analysis**, **known-plaintext attacks**, and **chosen-plaintext attacks**.
* **To validate MSXC's performance** and **efficacy** for real-world lightweight encryption tasks, demonstrating its viability through both theoretical analysis and practical implementation.

**The key contributions of this work are:**

* **The architecture and structure of MSXC**, including encryption and decryption techniques that integrate modular arithmetic and **XOR** operations with position-dependent key shifts.
* Based on **security analysis**, **MSXC** is **more resistant to typical attacks** than conventional substitution ciphers due to its dynamic substitution and key evolution.
* A functional model of **MSXC** that demonstrates its low processing power and resource requirements, making it an excellent option for light-duty and constrained scenarios.
* The examination of MSXC's potential uses, highlighting its benefits in embedded systems, educational settings, and other resource-constrained areas, laying the groundwork for further study and advancement.

**1.4 Report Organization**

This report is divided into the following sections to make it easier to read and more comprehensive:

* **Section 1: The Algorithm of MSXC** — The basic framework, mathematics, and methods for data encryption and decryption are thoroughly examined in this part.
* **Section 2: Security Analysis**, the resilience of MSXC to common cryptographic attacks is investigated, with particular focus on the system's defense against frequency analysis, known-plaintext, and chosen-plaintext attacks.
* **Section 3: Implementation and Results discusses the use of MSXC**, its effectiveness on low-resource devices (such embedded microcontrollers and Internet of Things sensors), and the evaluation's conclusions.
* **Section 4: Findings and Upcoming Projects** — This section summarizes the key findings of the study, highlights the most significant contributions made by MSXC, and offers suggestions for potential future developments and enhancements to MSXC.