**Final Report**

Demo Presentation and Technical Report

Group Member:

Yash Gandhi

Jwal Ashvinkumar Patel

Claricel Ramos

Engineering Project II – EECE71030

Professor: Waleed Khan

Date: February 14, 2024

**Table of Contents**

[Introduction 4](#_Toc158676333)

[1. Project Objectives 5](#_Toc158676334)

[1.1 Implement Several Encryption / Decryption Algorithms: 5](#_Toc158676335)

[1.2 Consolidate a Sensor into the Arduino Platform to Gather Data: Use 5](#_Toc158676336)

[1.3 Investigate the Relationship Between Encryption and Sensor Data: 5](#_Toc158676337)

[2. How the Hardware and software are set up 5](#_Toc158676338)

[2.1 Hardware: 5](#_Toc158676339)

[2.2 Software: 6](#_Toc158676340)

[3. Approaches Overview 6](#_Toc158676341)

[3.1 The XOR Manipulation: 6](#_Toc158676342)

[Pros: 6](#_Toc158676343)

[Cons: 6](#_Toc158676344)

[3.2 Caesar Cipher: 6](#_Toc158676345)

[Pros: 6](#_Toc158676346)

[Cons: 7](#_Toc158676347)

[3.3 Vigenère Cipher: 7](#_Toc158676348)

[Pros: 7](#_Toc158676349)

[Cons: 7](#_Toc158676350)

[4. Insights, Obstacles, and Learning 7](#_Toc158676351)

[4.1 XOR Obstacles: 7](#_Toc158676352)

[4.2 XOR Insights: 7](#_Toc158676353)

[4.3 XOR Learning: 8](#_Toc158676354)

[4.4 Caesar Cipher Obstacles: 8](#_Toc158676355)

[4.5 Caesar Cipher Insights: 8](#_Toc158676356)

[4.6 Caesar Cipher Learning: 9](#_Toc158676357)

[4.7 Vigenère Cipher Obstacles: 9](#_Toc158676358)

[4.8 Vigenère Cipher Insight: 9](#_Toc158676359)

[4.9 Vigenère Cipher Learning: 10](#_Toc158676360)

[5. Potential Future Features 10](#_Toc158676361)

[5.1 Key Management System: 10](#_Toc158676362)

[5.2 Integration with Cloud Services: 10](#_Toc158676363)

[Conclusion 11](#_Toc158676364)

# **Introduction**

Protecting the integrity of data transmission and storage has become urgently important in today’s quickly changing digital environment, when information is shared everywhere, and our electronic devices are more interconnected than ever. Encryption, which is essential to protecting private data from illegal access and interception, is at the foundation of this project.

Our report investigates the combination of encryption methods and technology for sensors, proposing fresh approaches to strengthening data protection and maintaining privacy. This is done in recognition of the fact that data security is of the utmost importance.

Our primary focus is on the incorporation of encryption methods into Arduino-based sensor systems. Our objectives are not only to improve the integrity of the data, but also to provide illuminate the complex link that exists between encryption techniques and the data that is created by sensors. By utilizing the adaptable features of Arduino boards and a variety of sensors, we aim to apply, assess, and showcase the efficiency of various encryption/decryption algorithms in real-life situations.

## **Project Objectives**

For Arduino-based systems, the following are the primary objectives we have established: to enhance data security and operational efficiency.

* 1. **Implement Several Encryption / Decryption Algorithms:** Explore and implement various encryption techniques to improve data security and confidentiality.
  2. **Consolidate a Sensor into the Arduino Platform:** Integrate sensor technologies into the Arduino platform to capture real-time data, leading in a seamless connection between sensory inputs and encryption systems.
  3. **Investigate the Relationship Between Encryption and Sensor Data:** Examine the connection of encryption methodologies and sensor data to gain valuable insight into methods of enhancing data security and maintaining privacy.

## **How the Hardware and software are set up**

The process of configuring the hardware and software components for this project comprises many crucial stages to guarantee proper operation and seamless integration.

### **2.1 Hardware:**

* Arduino board (e.g. Arduino Uno)
* Sensor (e.g. soil moisture sensor, air flow sensor)
* Connecting wires

### **2.2 Software:**

* Arduino IDE
* Libraries for encryption and decryption algorithms

## **Approaches Overview**

This section, we’ll explore the different encryption methods employed in this project, along with their specific merits and downsides.

* 1. **The XOR Manipulation:** XOR is an operation system that generates a return bit by comparing two bits and determining their difference.

##### **Pros:**

* Simple and fast to follow.
* It is utilized in symmetric ciphers such as AES.

###### **Cons:**

* It is not safe against the decryption methods used of today.
* Unprotected against attacks using known plaintext.
  1. **Caesar Cipher:** The most straightforward method of encryption is known as the Caesar Cipher. The letters in the plaintext message are moved by a finite number of positions for it to function properly. “Shift” or “Key” is what it is known as.

###### **Pros:**

* Straightforward and simple to comprehend.
* Quick implementation

###### **Cons:**

* Insufficient protection from brute force attacks.
* Lack of Authentication
  1. **Vigenère Cipher:** When it comes to encoding text, the Vigenère cipher is a plain-text kind of encoding that employs alphabetical substitution.

###### **Pros:**

* Significantly more secure than the Caesar cipher.
* Resists analysis based on frequency.

###### **Cons:**

* It is necessary to use a longer key.
* Compatibility with cloud-based infrastructure.

## **Insights, Obstacles, and Learning**

Several significant insights, obstacles, and lessons have surfaced throughout the duration of our project.

### **XOR Obstacles:**

**Bit Manipulation:** Regarding this matter, we are having difficulty obtaining a specific bit at a certain index and then successfully adjusting the result bit in accordance with the key value.

### **XOR Insights:**

**XOR is a fundamental building block for encryption:** XOR manipulation is a fundamental component of encryption methods. The simplicity and effectiveness of this technique make it an essential component for constructing more complex encryption schemes. Through comprehending the concepts of XOR manipulation, we get significant knowledge about the internal mechanisms of encryption systems.

### **XOR Learning:**

**Cryptography Fundamentals**: Decrypting XOR ciphers covers essential concepts in cryptography, including symmetric encryption and the features of XOR operations.

### **Caesar Cipher Obstacles:**

**Rolling of character from both end:** The ACSII value alphabets shifts based on the key modification, but frequently the border character goes beyond the range o alphabets, therefore maintaining it in the range is one of the most difficult challenges.

**Making char in uppercase:** In the Arduino code, if the message comprises lowercase alphabets, it is necessary to convert them to uppercase. However, this caused an issue at the start of the encryption process.

### **Caesar Cipher Insights:**

**Caesar Cipher is suitable for beginners:** however, it lacks security: While the Caesar Cipher is commonly employed as an initial encryption method due to its simplicity, it lacks security. Caesar Cipher works by changing characters in a plaintext message by a set number of places, known as the “shift” or “key”. However, renderer ability to brute force assaults and lack of authentication measures renders it ineffective for protecting critical information in current settings.

### **Caesar Cipher Learning:**

**C Programming Fundamentals:** Programming fundamentals such as variables, loops, conditionals, and functions are strengthened by the implementation of the decryption method in the C library.

**Algorithm Analysis:** Enhancing one’s grasp of algorithm analysis and optimization may be accomplished by doing an examination of the effectiveness and efficiency of encryption and decryption algorithms.

### **Vigenère Cipher Obstacles:**

**Complexity of Vigenère Cipher:** When compared to the Caesar Cipher, the Vigenère Cipher incorporates a key phrase for the purpose of encryption, making it more complicated. Perhaps significant study and meticulous preparation are required to successfully implement this complexity on Arduino.

**String Manipulation:** When compared to high-level language, string manipulation in C can be slightly more difficult to do. In Order to successfully implement decryption logic, it may be necessary to handle strings and characters with caution.

### **Vigenère Cipher Insight:**

**Vigenère Cipher Balances Security and Efficiency:** The Vigenère Cipher is an encryption compromise that balances both safety and accessibility. Unlike the Caesar Cipher, the Vigenère Cipher uses a keyword to shift letters in the plaintext message, which adds an extra degree of protection. This increases its resistance to frequency analysis, a popular cryptanalysis approach, However, the Vigenère Cipher still requires a longer key for maximum security, and its compatibility with cloud-based systems may provide issues in some cases.

### **Vigenère Cipher Learning:**

**String Manipulation in C:** Building an enhanced understanding of string manipulation methods, arrays, and loops in the C programming language can be achieved by implementing the decryption techniques in C.

**Data Structure:** A greater understanding of the application of data structures in cryptographic algorithms can be achieved by storing the key phrase in arrays or other data structures and performing encryption and decryption operations on them.

## **Potential Future Features**

* 1. **Key Management System:** The objective is to create an encryption key management system that is both user-friendly and secure. By limiting access to sensitive data to authorized personnel, an additional level of security will be implemented.
  2. **Integration with Cloud Services:** Investigating the feasibility of integrating the system with cloud service. Implementing this will facilitate the smooth and efficient storage, retrieval, and examination of sensor data, hence improving the capacity and adaptability of the systems.

# **Conclusion**

In culmination, the study on combining encryption techniques with Arduino-based sensor systems is a major step towards strengthening data security and improving operational efficiency. The Arduino ecosystem has established a strong framework for enhancing the protection of sensitive information and improving data processing capabilities by seamlessly integrating encryption methods with real-time sensor data collecting. This focused endeavor highlights a dedication to providing innovative approaches that effectively combine strong security measures with excellent performance. In the future, next steps will continue to pioneer innovations that prioritize both the integrity of data and the flawless running of systems.