# Quantum Leap: An Exploration of the Development of Computing and Cryptography

Jake Lyon and Dr. Palmer (Advisor)


## Abstract

This work aims to explore the ideas of innovation and evolution in computation within a framework of cybersecurity . To accomplish this exploration effectively, we selected three stages of computation to focus on. Circuitry, the Arduino, and quantum-based computation. The first stage is the shift cipher on physical circuity, this shows off a simple form of computation and one of the first forms of encryption. The next phase utilizes an Arduino microcontroller to highlight software and hardware interaction. The Arduino demonstrates today's encryption standard RSA at lower level of complexity to bring us to modern standards. The final phase explores quantum computing and its effects on the security of RSA. A demonstration into breaking RSA is conducted as a final experiment for this work. Through a range of theories from basic logic to quantum computation this project shows the development of computation in the subject of encryption and cyber security.


## Circuitry and Logic

Circuits which are complete electrical flow loops have lots of potential to keep track of data and perform computations.. Using electrical components to store, modify and use electrical signals and digital logic we can accomplish the first phase of this Independent Study. Digital logic is what allows us to achieve computation, through basic logical combination gates like AND, OR and NOT gates. By chaining and combining the outputs of multiple gates we can achieve tasks like addition, data storage and data representation.

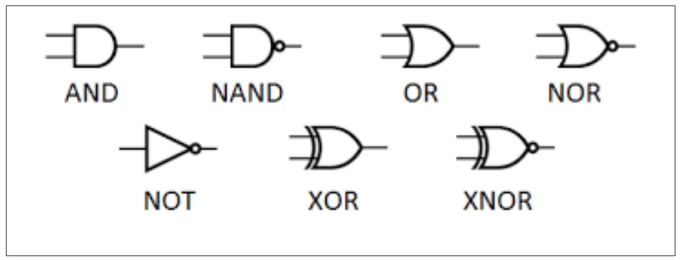


Figure 1: Digital Logic Gates

The goals of this phase was to take this early idea of computation and implement an early form of encryption, the shift cipher. This cipher is a famous example of cryptography and functions by taking the numeric representation of each letter in plain-text sentence and shifting it by a value between 0-25. This is a simple concept but serves as great starting point for this work, figure 3 in this poster shows off the fully implemented circuit that allows a user to enter in four separate values and define a shift. Each value is then able to be added with the shift to calculate the encrypted value. Then each encrypted value is decrypted back to the original input. Using seven segment displays and memory modules the letter representation of each input are visible throughout the process.

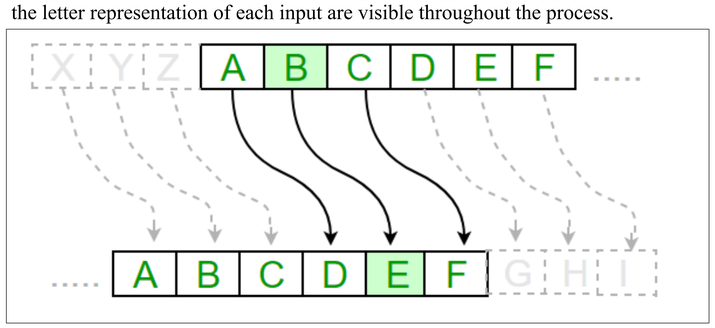


Figure 2: Operation of Shift Cipher

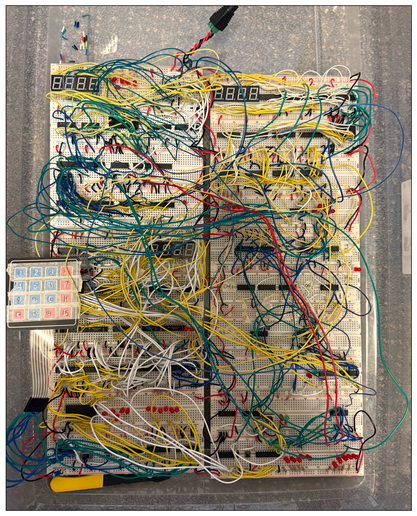

Figure 3: Full Implementation of Shift Cipher Circuit.

## Arduino

The next goal of this project was to take a step forward in both computation style and encryption. To do this we implemented today's encryption standard the Rivest-Shamir-Adleman (RSA) algorithm on the Arduino Uno R3 a microcontroller. Arduino and other examples of microcontroller and microprocessors can be considered hybrid pieces of technology, with them we are able to control physical hardware components and manipulate signals, but we are also able to upload and run code scripts to control the hardware. RSA is today's standard in data protection and functions off the use of a problem that is inefficient for classical computers to solve at a large bit size. RSA functions off the inefficient problem of factorizing large co-prime numbers to protect data [2]. This stage of the project improved many of the complicated portions of the pure circuit and demonstrates how an advancement in computation lets us become more advanced in our encryption practices. The notable advancements present here was the jump from 5 to 32 bits worth of data being encrypted, using a liquid crystal display to report our data and of course the use of a hybrid, hardware software system vs a pure hardware system.

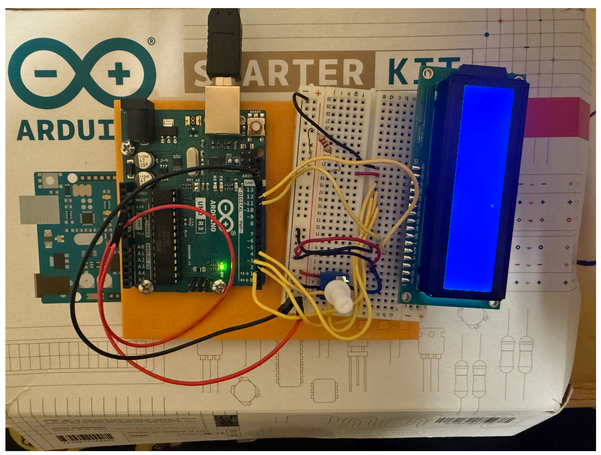

Figure 4: Arduino Hardware Used for Study

## Quantum

The final phase of this project was to explore the impact of still developing quantum computing on today's encryption standard. Quantum computing is a field of computation that is still heavily based in theory but is becoming more realistic to utilize. Based on the principles of quantum physics, quantum computers leverage the use of quantum-bits or qubits to more efficiently solve computations [1]. In the works of quantum computing exists and algorithm known as Shor's algorithm, brought forth by Peter Shor in 1994. This algorithm in theory allows a quantum computer with enough qubits that can be used effectively to make the problem of factorization more efficient than what a classical computer can accomplish. This has a huge effect on RSA as it is this factorization difficulty that is the lynch pin of RSA. To explore this, we conducted an experiment of what a hacker could potentially accomplish through the eventual use of Shor's algorithm. There exist many working implementations of the algorithm, notably by companies like IBM or Classiq. We were able to take one of these and factorize prime numbers up to 209. Python script was also developed to encrypt a message using RSA and a decryption script was also written allowing us to have a full pipeline of what a hacker could potentially implement.

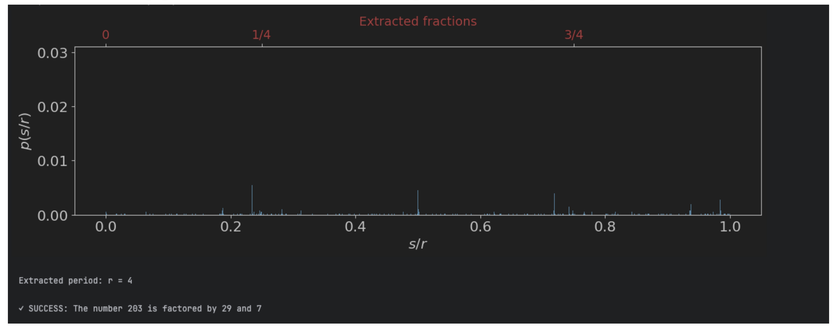


Figure 5: Graph of Potential Periods for Quantum Experiment

## Post-Quantum

As a form of discussion in the project, post-quantum encryption algorithms were investigated. There exist several viable options for algorithms that are computationally hard enough for quantum computers to solve inefficiently and allow us to secure our data after RSA is no longer safe. They include:

- **Lattice-Based Algorithms**
- **Multivariate Equation Based Algorithms**
- **Code-Based Algorithms**

## Conclusion

The exploration of each of these phases had their own unique challenges but were all exciting and fun implementations to accomplish. Consistent is the idea of continue evolution and innovation, while there are many concerns about the security of the world, there will always be developments to help, not harm.


### Acknowledgments

I would like to thank the Henry J. Copeland fund for supporting and enhancing this Independent Study.


### References


[1] Balamurugan K S et al. "Quantum computing basics, applications and future perspectives". In: Journal of Molecular Structure 1308 (2024), p. 137917. issn: 0022-2860.

[2] Kartik. RSA Algorithm in Cryptography. en-US. Section: Computer Networks.