MAT-260 Milestone One: The Affine Cipher

Gary Hobson

Southern New Hampshire University

May 20, 2025

Cipher Selection

For this project, I have selected the Affine Cipher, a classical encryption method that combines elements of both the multiplicative and shift (Caesar) ciphers. As a senior studying mathematics and cryptography, I chose this cipher because it provides a solid bridge between basic substitution ciphers and more mathematically complex systems. Its use of modular arithmetic introduces key concepts that recur in modern cryptographic systems, such as key space constraints and the necessity of invertibility. The Affine Cipher is not only historically relevant but also mathematically rich, making it an ideal subject for deeper analysis in Milestone Two and the Final Project. By exploring this cipher, I aim to build a foundation for understanding how mathematical principles underpin encryption, which I will expand upon in later stages of this project.

Historical Background

The Affine Cipher belongs to the family of monoalphabetic substitution ciphers, which have origins dating back to ancient times. It evolved from the Caesar Cipher, famously used by Julius Caesar to protect military messages around 50 BCE. While the Caesar Cipher applied a fixed shift to each letter, the Affine Cipher generalized this concept by incorporating multiplication into the encryption process, thus adding a layer of complexity. Although there is no record of widespread historical deployment of the Affine Cipher, it represents an important theoretical advancement in the development of cryptographic techniques. It gained academic interest in the 19th and 20th centuries as researchers formalized encryption methods using number theory. Today, the Affine Cipher serves as an introductory example in cryptographic education due to its simplicity and its ability to introduce fundamental concepts like modular inverses and key management (Trappe & Washington, 2017; Singh, 1999). This historical context sets the stage for analyzing its mathematical properties and vulnerabilities in the upcoming milestones.

Properties and Mathematical Foundations

The Affine Cipher transforms each letter x of the plaintext using the formula:

$$E(x) = (a \cdot x + b) \mod 26$$

Here, x represents the numerical position of the letter in the alphabet (with $A = 0$, $B = 1$, ..., $Z = 25$), a and b are the keys, and 26 is the modulus for the English alphabet. The value of a must be coprime to 26 to ensure the existence of a modular inverse, which is essential for decryption. Specifically, $\gcd(a, 26) = 1$, meaning a must be one of the 12 values relatively prime to 26 (e.g., 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25).

Decryption uses the inverse function:

$$D(y) = a^{-1}(y - b) \mod 26$$

where a^{-1} is the modular inverse of a modulo 26, satisfying $a \cdot a^{-1} \equiv 1 \pmod{26}$. The total key space is calculated as the number of valid a values times the possible values of b (0 to 25), giving $12 \times 26 = 312$ possible key combinations.

The Affine Cipher illustrates core ideas in modern encryption, including modular arithmetic, invertibility, and key management. Its mathematical elegance lies in its reversibility, which depends entirely on choosing appropriate keys. However, it also reveals a critical limitation of monoalphabetic ciphers: despite the added mathematical complexity, they remain vulnerable to frequency analysis, as the substitution remains fixed across the entire message (GeeksforGeeks, n.d.). This vulnerability will be a focal point for Milestone Two, where I will explore attack methods.

Conclusion

The Affine Cipher is a valuable cipher to study because it introduces key mathematical structures while remaining accessible for analysis. Its use of modular arithmetic and the requirement for a coprime key provide a practical introduction to concepts that are

foundational to modern cryptography. In Milestone Two, I plan to explore the cipher's vulnerabilities through manual analysis and simulation in MATLAB, focusing on techniques like frequency analysis to break the cipher. For the Final Project, I will extend this work to compare the Affine Cipher to modern systems like AES, demonstrating why stronger methods are necessary for real-world applications. This initial exploration sets a strong foundation for the subsequent phases of the project, allowing me to build a comprehensive understanding of cryptographic principles.

References

- Trappe, W., & Washington, L. C. (2017). *Introduction to Cryptography with Coding Theory* (3rd ed.). Pearson.
- Singh, S. (1999). *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography.* Anchor Books.
- GeeksforGeeks. (n.d.). Affine Cipher Explained. Retrieved from `https://www.geeksforgeeks.org/affine-cipher-explained/`