Comprehensive Analysis of Affine Cipher Security

Contents

Abstract:

This document provides an in-depth examination of the Affine cipher, a classical monoalphabetic substitution cipher. The focus is on its mathematical framework, encryption and decryption mechanisms, inherent vulnerabilities, and the feasibility of enhancing its security for modern applications.

A Mathematical Description of Affine Cipher

The Affine cipher operates as a monoalphabetic substitution cipher that numerically maps each letter to its equivalent in the alphabet. This cipher employs a method of modular arithmetic to transition each plaintext letter to its corresponding ciphertext letter.

Encryption Overview:

The formula used for encryption is $E(x) = (ax + b) \bmod m$, where:

- x represents the plaintext character,
- a is the multiplicative alpha key,
- b is the additive beta key,
- m is 26, reflecting the total number of letters in the alphabet.

For instance, the plaintext 'hi' translates to 'py' using keys A = 9 and B = 4:

- For 'h' (mapped to 7): 9*7 + 4 mod 26 equals 15 mod 26, which corresponds to 'p'.
- For 'i' (mapped to 8): 9*8 + 4 mod 26 equals 24 mod 26, which corresponds to 'y'.

Decryption Methodology:

The decryption formula is D(x) = (inverse a) * (y - b) mod m, which relies on the modular inverse of the alpha key a, ensuring that a and m (26) are coprime: gcd(a, m) = 1. Here, y is the ciphertext letter.

Modular Inversion via Extended Euclidean Algorithm:

The modular inverse is derived using the extended Euclidean algorithm, which resolves the greatest common divisor (gcd) as gcd(a, b) = ax + by = 1 mod 26. This process finds the modular inverse necessary for decryption. For example, to find the modular inverse of 7 under modulo 26:

- Calculation sequence: 7.x mod 26 = 1 leads to a series of reductions and substitutions starting from gcd(7, 26), breaking down as follows:
  - 26 = 7 * 3 + 5
  - 7 = 5 * 1 + 2
  - 3 = 2 * 2 + 1
  - Substituting back, we find: 1 = 3 - 2*2 = 3 - (7 - 5*1)*2 = 3*5 + 7*(-2)
- This series of substitutions ultimately shows that when 3*26 mod 26 = 0, then 7*(-11) mod 26 = 1, leading to -11 + 26 = 15. Hence, the modular inverse of 7 is 15 under modulo 26.

Brute-Force Decryption Strategy:

I cracked the cipher in AffineCipherBruteForce.c using brute-force. Initially, I asked the user to enter the 'ciphertext', which I then converted into uppercase letters to prepare it for decoding. I invoked the 'bruteforce' function, which utilized a while loop to iterate through all combinations of alpha and beta keys. This process was facilitated by a nested function within the 'while(a<26) ...decrypt(...) ... a++' loop called 'decrypt', which processed a loop of the beta

key from 0 to 25. This meant I tested every alpha key with a complete range of beta values from 0 to 25.

For example, alpha: 0, beta: 0-25, alpha: 1, beta: 0-25, alpha 2, beta: 0-25, and so on.

Using the decrypt function for each alpha and beta combination, the function executed the decryption formula d(x) = inverse(a) * (y-b) mod m and printed the deciphered text in the order of alpha: 0, beta: 0, beta: 1, beta: 2, etc.

In simpler terms, I brute-forced the ciphertext by exploring all possible key combinations in the order of alpha: 0-25, beta: 0-25. It's important to note that I also calculated the modular inverse of each alpha key to ensure the decryption formula was functional. I accomplished this by integrating an inverse function within the while loop for every iteration of the alpha key.

Vulnerabilities of the Affine Cipher:

Monoalphabetic Substitution Weakness: The Affine cipher is inherently vulnerable due to its monoalphabetic nature, which means each letter is always replaced with the same substitute. This uniform substitution makes the cipher prone to multiple types of attacks:

Brute Force Attacks: With only 12 coprime numbers for 'a' and 26 possible 'b' values, there are merely 312 possible encryption keys. This limited key space allows modern computers to quickly perform exhaustive search attacks.

Statistical Analysis: The cipher's susceptibility to frequency analysis exacerbates its weaknesses, particularly with longer texts. The frequency of letter appearance in a ciphertext can be compared to known letter frequency profiles of languages (e.g., 'e' and 't' are most frequent in English), allowing attackers to deduce likely plaintexts.

Known Plaintext Attacks: With minimal known plaintext, attackers can derive the encryption keys using simple algebraic techniques like solving simultaneous equations, making the cipher particularly weak against informed adversaries.

Security Enhancement Feasibility:

Inherent Limitations: Enhancing the security of the Affine cipher by re-encryption with different cryptographic groups might offer temporary resilience. However, layering the same type of cipher (Affine over Affine) fails to increase security due to algebraic properties that do not alter the cipher's fundamental vulnerabilities.

Conclusion on Cipher's Security for Internal Communications:

Insufficient Security for Professional Use: Despite its simplicity and ease of implementation, the Affine cipher does not provide a level of security adequate for protecting sensitive or confidential communication. Its predictable nature and vulnerability to several types of cryptanalytic attacks render it unsuitable for environments where data security is paramount.

Potential Utility: While the Affine cipher can serve educational purposes or systems where security is not a critical concern, it is ill-suited for serious applications. The simplicity of the cipher makes it accessible for non-critical uses but inadequate for securing communications within or between corporations, especially in sectors sensitive to data breaches.