The Affine Cipher

1 Section A: General Information and Mathematics

1.1 Overview

The Affine Cipher is a type of monoalphebetic substitution cipher where each letter of the cipher text is mapped to another letter using a simple mathematical function. Each letter is assigned its equivalent numerical value and the encryption function is applied to this number to give a new number: the numerical equivalent of another letter in the alphabet. The encryption key for an affine cipher is on ordered pair of integers, commonly referred to with the letters a and b, where a is a multiplier and b is a constant as expressed in the general encryption function for a single letter using modular arithmetic:

$$E(x) = (ax + b) \bmod m \tag{1}$$

where modulus m is the size of the alphabet, 26 in this case. It is crucial that the values of a and m are coprime in order for the decryption algorithm to work. Therefore, the only valid values of a are:

$$a = 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25 \tag{2}$$

The decryption function uses the Extended Euclidean Algorithm in order to calculate modular multiplicative inverses of certain values, where each a value and its inverse a^{-1} satisfy the following equation:

$$aa^{-1} \bmod m = 1 \tag{3}$$

Hence, the general decryption algorithm for a single letter is:

$$D(x) = a^{-1}(x - b) \bmod m \tag{4}$$

Proof that the the decryption function is the inverse of the encryption function is shown in the following subsection (**1.2**)

1.2 Proof of Inverses

$$\begin{aligned}
D(E(x)) &= a^{-1}(E(x) - b) \bmod m && (1)\\
&= a^{-1}(((ax + b) \bmod m) - b) \bmod m && (2)\\
&= a^{-1}(ax + b - b) \bmod m && (3)\\
&= a^{-1}ax \bmod m && (4)\\
&= x \bmod m && (5)
\end{aligned}$$