Affine Cipher is a type of substitution cipher that combines two mathematical functions to encrypt plaintext messages. The Affine Cipher is considered a simple form of encryption, but it can be effective in securing messages if implemented correctly.

History

The Affine Cipher has a long history dating back to ancient civilizations, such as the Greeks and Romans, who used simple substitution ciphers to encrypt messages. However, the first known mention of the Affine Cipher specifically dates to the 9th century in the writings of an Arab mathematician named Al-Kindi.

Encryption Process

The Affine Cipher involves the use of two mathematical functions: ax + b mod m and a^-1 (x - b) mod m, where x is the value of the plaintext letter, a and b are integers chosen by the encrypter, m is the size of the alphabet being used (e.g. 26 for the English alphabet), and a^-1 is the multiplicative inverse of a modulo m.

To encrypt a plaintext message, each letter in the message is first assigned a numerical value based on its position in the alphabet (e.g. A = 0, B = 1, C = 2, etc.). The numerical value is then multiplied by the integer a, and the resulting product is added to the integer b. The result of this equation is then reduced modulo m to produce the ciphertext letter.

To decrypt the ciphertext message, each letter in the message is first assigned a numerical value based on its position in the alphabet. The numerical value is then subtracted by the integer b, and the resulting difference is multiplied by the inverse of a modulo m. The result of this equation is then reduced modulo m to produce the plaintext letter.

Security

The security of the Affine Cipher depends on the choice of integers a and b. If the integers are chosen poorly, the cipher may be vulnerable to various cryptanalytic attacks, including frequency analysis and brute-force attacks. However, if the integers are chosen randomly and kept secret, the Affine Cipher can be a relatively secure method of encryption.

Despite its vulnerabilities, the Affine Cipher is still used in some applications today, particularly in combination with other encryption techniques to provide an additional layer of security.