Affine Cipher Definition

DS Affine Cipher

The Affine Cipher is a type of monoalphabetic substitution cipher, where each letter in the plaintext is mapped to a unique letter in the ciphertext through a simple mathematical function. The function involves modular arithmetic and is defined as: c = (a * p + b) % 26, where c is the numerical value of the ciphertext character, p is the numerical value of the plaintext character, a and b are the two keys of the cipher, and 26 is the number of letters in the alphabet. To decrypt, the inverse function can be applied using the modular multiplicative inverse of the key "a".

DS Show a simple encryption/decryption example

Sure! Let's say we have the plaintext message "HELLO" and we want to encrypt it using the Affine Cipher with keys (a,b) = (7,3). Here's how the encryption would work:

- Convert each letter in the plaintext to its numerical representation (A=0, B=1, ..., Z=25). So, "H" becomes 7, "E" becomes 4, etc.
- Apply the encryption function to each numerical representation of the plaintext:
  c1 = (7 * 7 + 3) % 26 = 10
  c2 = (7 * 4 + 3) % 26 = 25
  c3 = (7 * 11 + 3) % 26 = 8
  c4 = (7 * 11 + 3) % 26 = 8
  c5 = (7 * 14 + 3) % 26 = 5
- Convert each numerical representation of the ciphertext back to its letter representation (0=A, 1=B, ..., 25=Z). So, 10 becomes "K", 25 becomes "Z", etc.
- The resulting ciphertext is "KZZKK".

For decryption, we would use the inverse of the encryption function to obtain the original plaintext:

- p = (c - b) * a^(-1) % 26
- To find the modular multiplicative inverse of a (which is 7 in this case), we need to find an integer x such that (7 * x) % 26 = 1. In this case, x = 15.
- So, the decryption function would be: p = (c - 3) * 15 % 26
- Apply the decryption function to each numerical representation of the ciphertext:
  p1 = (10 - 3) * 15 % 26 = 4
  p2 = (25 - 3) * 15 % 26 = 11
  p3 = (8 - 3) * 15 % 26 = 11
  p4 = (8 - 3) * 15 % 26 = 11
  p5 = (5 - 3) * 15 % 26 = 14
- Convert each numerical representation of the plaintext back to its letter representation: 4 becomes "E", 11 becomes "L", etc.
- The original plaintext message is "HELLO".

DS Affine ciphers code implementation in js

Here's an implementation of the Affine Cipher encryption and decryption in JavaScript:

java Copy code

ChatGPT Jan 30 Version. Free Research Preview. Our goal is to make AI systems more natural and safe to interact with. Your feedback will help us improve.