**Affine Cipher**

**Aim – To design an Affine Cipher in Java**

**Description**

The Affine cipher is a monoalphabetic substitution cipher that uses mathematical functions to encrypt and decrypt messages. In this cipher, each letter in the plaintext is first mapped to a number (usually A=0, B=1, C=2, ..., Z=25), and then encrypted using a simple mathematical function (of the form ax + b, where “a” and “b” are constants). The result is a ciphertext consisting of numbers, which can then be converted back to letters to obtain the final encrypted message. To decrypt the message, another simple mathematical function is applied to the ciphertext numbers, which returns the original plaintext numbers, which can then be converted back to letters. The security of the Affine cipher relies on the secrecy of the values of the two constants “a” and “b”.

The ‘key’ for the Affine cipher consists of 2 numbers, we’ll call them a and b. The following discussion assumes the use of a 26 character alphabet (m = 26). “a” should be chosen to be relatively prime to m (i.e. “a” should have no factors in common with “m”).

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

**Encryption**

This function is used to encrypt the plain text. It takes the plain text PlainText, the encryption key “a”, the encryption offset “b”, and the size of the character set “m” as inputs. The encryption process is simply a linear transformation of the form (a \* PlainText + b) % m. The result of this transformation is the encrypted cipher text.

Working of Encryption function –

* Map each letter in the plaintext to a numerical value (e.g. A=0, B=1, C=2, ..., Z=25).
* Apply the following mathematical function to each numerical value: (ax + b) mod 26, where “a” and “b” are constants and “mod 26” means the result is taken modulo 26. This results in a new numerical value for each letter.
* Convert the new numerical values back to letters to obtain the final ciphertext.

Encryption Formula –

(a \* PlainText + b) % m

a and b: key of the cipher

m: size of the series of alphabets

N.B. – a must be chosen such that a and m are co-primes

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| C | J | Q | X | E | L | S | Z | G | N | U | B | I | P | W | D | K | R | Y | F | M | T | A | H | O | V |

**Decryption**

This function is used to decrypt the cipher text. It takes the cipher text CipherText, the encryption key “a”, and the size of the character set “m” as inputs. The decryption process is to reverse the encryption process, which can be done by first finding the modular inverse of “a” with respect to “m” and then transforming the cipher text back to the original plain text using the equation (inv \* (CipherText - b + m)) % m.

Working of decryption function –

* Map each letter in the ciphertext to its corresponding numerical value (e.g. A=0, B=1, C=2, ..., Z=25).
* Apply the inverse function to each numerical value. The inverse function is of the form (y = a^-1 \* (x - b)) mod 26, where “a^-1” is the modular inverse of “a” (modulo 26), “x” is the numerical value of the ciphertext letter, and “b” is the same constant used in the encryption.
* Convert the new numerical values back to letters to obtain the original plaintext.

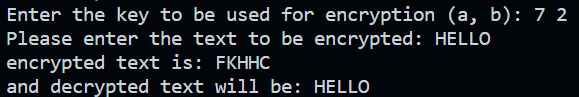
Decryption Formula –

(inv \* (CipherText - b + m)) % m

inv: modular multiplicative inverse of “a” modulo “m”

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| C | J | Q | X | E | L | S | Z | G | N | U | B | I | P | W | D | K | R | Y | F | M | T | A | H | O | V |
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |

**Output**

****

**N.B. –** Keys of the following Affine Cipher are “a” = 7 and “b” = 2

**Encryption Output**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| PlainText | H | E | L | L | O |
| x | 7 | 4 | 11 | 11 | 14 |
| ax + b % 26 | 25 | 4 | 1 | 1 | 22 |
| Encrypted | F | K | H | H | C |

**Decryption Output**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Encrypted | F | K | H | H | C |
| x | 25 | 4 | 1 | 1 | 22 |
| inv\*(x-b)%m | 7 | 4 | 11 | 11 | 14 |
| PlainText | H | E | L | L | O |

**Name: Dinanath Dash**

**Registration Number: 2241004161**

**Section: 2241026**