AFFINE CIPHER

The affine cipher is a type of monoalphabetic substitution cipher, wherein each letter in an alphabet is mapped to its numeric equivalent, encrypted using a simple mathematical function, and converted back to a letter. The formula used means that each letter encrypts to one other letter, and back again, meaning the cipher is essentially a standard substitution cipher with a rule governing which letter goes to which. As such, it has the weaknesses of all substitution ciphers. Each letter is enciphered with the function (ax+b)(mod 26), where b is the magnitude of the shift.

**Examples**

In these two examples, one encrypting and one decrypting, the alphabet is going to be the letters A through Z, and will have the corresponding values found in the following table.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **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 |

**Encrypting**

In this encrypting example,the plaintext to be encrypted is "AFFINE CIPHER" using the table mentioned above for the numeric values of each letter, taking  to be 5, to be 8, and  to be 26 since there are 26 characters in the alphabet being used. Only the value of  has a restriction since it has to be coprime with 26. The possible values that  could be are 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, and 25. The value for  can be arbitrary as long as  does not equal 1 since this is the shift of the cipher. Thus, the encryption function for this example will be Y=E(X)=5X+8 (mod 26). The first step in encrypting the message is to write the numeric values of each letter.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| plaintext: | A | F | F | I | N | E | C | I | P | H | E | R |
| x: | 0 | 5 | 5 | 8 | 13 | 4 | 2 | 8 | 15 | 7 | 4 | 17 |

Now, take each value of x, and solve the first part of the equation,5X+8. After finding the value of 5X+8for each character, take the remainder when dividing the result of 5X+8by 26. The following table shows the first four steps of the encrypting process.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| plaintext: | A | F | F | I | N | E | C | I | P | H | E | R |
| x: | 0 | 5 | 5 | 8 | 13 | 4 | 2 | 8 | 15 | 7 | 4 | 17 |
| 5x+8 | 8 | 33 | 33 | 48 | 73 | 28 | 18 | 48 | 83 | 43 | 28 | 93 |
| (5x+8)\pmod{26} | 8 | 7 | 7 | 22 | 21 | 2 | 18 | 22 | 5 | 17 | 2 | 15 |

Now you have to do another table with the formula y=3x+7 and then encrypt your sentences

The final step in encrypting the message is to look up each numeric value in the table for the corresponding letters. In this example, the encrypted text would be IHHWVCSWFRCP. The table below shows the completed table for encrypting a message in the Affine cipher.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **plaintext** | A | F | F | I | N | E | C | I | P | H | E | R |
| ***x*** | 0 | 5 | 5 | 8 | 13 | 4 | 2 | 8 | 15 | 7 | 4 | 17 |
| **(5*x* + 8)** | 8 | 33 | 33 | 48 | 73 | 28 | 18 | 48 | 83 | 43 | 28 | 93 |
| **(5*x* + 8) mod 26** | 8 | 7 | 7 | 22 | 21 | 2 | 18 | 22 | 5 | 17 | 2 | 15 |
| **ciphertext** | I | H | H | W | V | C | S | W | F | R | C | P |

### Decrypting

In this decryption example, the ciphertext that will be decrypted is the ciphertext from the encryption example. The corresponding decryption function is *D*(*y*) = 21(*y* − 8) mod 26, where a−1 is calculated to be 21(because 5+21=26), *b* is 8, and *m* is 26. To begin, write the numeric equivalents to each letter in the ciphertext, as shown in the table below.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ciphertext** | I | H | H | W | V | C | S | W | F | R | C | P |
| ***y*** | 8 | 7 | 7 | 22 | 21 | 2 | 18 | 22 | 5 | 17 | 2 | 15 |

Now, the next step is to compute 21(*y* − 8), and then take the remainder when that result is divided by 26. The following table shows the results of both computations.

What is the formula for y=3x+7?

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ciphertext** | I | H | H | W | V | C | S | W | F | R | C | P |
| ***y*** | 8 | 7 | 7 | 22 | 21 | 2 | 18 | 22 | 5 | 17 | 2 | 15 |
| **21(*y* − 8)** | 0 | −21 | −21 | 294 | 273 | −126 | 210 | 294 | −63 | 189 | −126 | 147 |
| **21(*y* − 8) mod 26** | 0 | 5 | 5 | 8 | 13 | 4 | 2 | 8 | 15 | 7 | 4 | 17 |

The final step in decrypting the ciphertext is to use the table to convert numeric values back into letters. The plaintext in this decryption is AFFINECIPHER. Below is the table with the final step completed.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ciphertext** | I | H | H | W | V | C | S | W | F | R | C | P |
| ***y*** | 8 | 7 | 7 | 22 | 21 | 2 | 18 | 22 | 5 | 17 | 2 | 15 |
| **21(*y* − 8)** | 0 | −21 | −21 | 294 | 273 | −126 | 210 | 294 | −63 | 189 | −126 | 147 |
| **21(*y* − 8) mod 26** | 0 | 5 | 5 | 8 | 13 | 4 | 2 | 8 | 15 | 7 | 4 | 17 |
| **plaintext** | A | F | F | I | N | E | C | I | P | H | E | R |