1a) What is the size of key space for a fixed modular n? Use the notation of the Euler's totient Φ(*n*). It is defined as the number of integers that are coprime to n.

Answer:

Size of the alphabet 26 = *n*

Two prime factors of 26 are 2 and 13

**p = 2**

**q = 13**

Euler's totient function = **Φ(*n*)**

Formula for Euler's totient function Φ(*n*) for a number *n* that is the product of two distinct prime numbers *p* and *q* is:

**Φ(*n*)** = (p – 1) x (q – 1)

**Φ(n) = (2 − 1) × (13 − 1) = 1 × 12 = 12**

Key Space Size = Φ(*n*) x *n*

**Φ(n) = 12**

**n = 26**

**12 x 26 = 312 (key space)**

1c) Eve has intercepted a ciphertext “QJKESREOGHGXXREOXEO” and, through her intelligence sources, discovered that it’s encrypted using an Affine Cipher. She also has limited information about the encryption process: the letter 'T' is encrypted to 'H' and 'O' to 'E'. With this knowledge, she aims to decrypt the message. Your challenge is to help Eve by developing a method to find the decryption function of the Affine Cipher using the given information. You can do it manually or programmatically. Once the decryption function is determined, apply it to decrypt the ciphertext. Provide both the decrypted message and an explanation of your methodology.

Answer:

First, we know that the Affine Cipher follows the encryption formula c = (a \* p + b) mod 26, where *c* is the ciphertext letter, *p* is the plaintext letter, and *a* and *b* are keys.

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

In the above modular arithmetic mapping, we know that:

'T' (which is 19) encrypts to 'H' (which is 7),

'O' (which is 14) encrypts to 'E' (which is 4),

Substituting these values into the encryption formula, we get the following two equations:

For T to H: 7 = (19a + b) mod 26

For O to E: 4 = (14a + b) mod 26

Subtracting the second equation from the first gives:

5a = 3 mod 26

Finding the modular inverse of 5 mod 26 helps us isolate *a*. The modular inverse of 5 is 21 because 5 × 21 mod  26 = 1. Thus:

a = 3 x 21 = 63 -> a = 63 mod 21 -> a = 11

With a = 11, we substitute back to solve for b. Using the first equation:

7 = 19 x 11 + b mod 26

b = 7 – 209 mod 26 = 7 – 1 = 6.

The keys are a = 11 and b = 6. The decryption function inverses the encryption: p = (c – b) x a-1 mod 26, where a-1 is the modular inverse of 11 mod 26, which is 19 because 11 x 19 mod 26 = 1

Next, we decrypt the ciphertext “QJKESREOGHGXXREOXEO”:

Q = 16 -> (16 – 6) x 19 mod 26 = 8 -> plaintext = I

J = 9 -> (9 – 6) x 19 mod 26 = 5 -> plaintext = F

K = 10 -> (10 – 6) x 19 mod 26 = 24 -> plaintext = Y

E = 4 -> (4 – 6) x 19 mod 26 = 14 -> plaintext = O

S = 18 -> (18 – 6) x 19 mod 26 = 20 -> plaintext = U

Decrypted Text:

IF YOU BOW AT ALL BOW LOW

R = 17 -> (17 – 6) x 19 mod 26 = 1 -> plaintext = B

E = 4 -> (4 – 6) x 19 mod 26 = 14 -> plaintext = O

O = 14 -> (14 – 6) x 19 mod 26 = 22 -> plaintext = W

G = 6 -> (6 – 6) x 19 mod 26 = 0 -> plaintext = A

H = 7 -> (7 – 6) x 19 mod 26 = 19 -> plaintext = T

G = 6 -> (6 – 6) x 19 mod 26 = 0 -> plaintext = A

X = 23 -> (23 – 6) x 19 mod 26 = 11 -> plaintext = L

X = 23 -> (23 – 6) x 19 mod 26 = 11 -> plaintext = L

R = 17 -> (17 – 6) x 19 mod 26 = 1 -> plaintext = B

E = 4 -> (4 – 6) x 19 mod 26 = 14 -> plaintext = O

O = 14 -> (14 – 6) x 19 mod 26 = 22 -> plaintext = W

X = 23 -> (23 – 6) x 19 mod 26 = 11 -> plaintext = L

E = 4 -> (4 – 6) x 19 mod 26 = 14 -> plaintext = O

O = 14 -> (14 – 6) x 19 mod 26 = 22 -> plaintext = W

2a) Calculate the Size of the Key Space. Explain how the key space is calculated and its implications for

the cipher's security.

Answer:

For a simple substitution cipher using the English alphabet, which contains 26 letters, the key space is determined by the number of permutations of these 26 letters. This is represented mathematically by the factorial of 26, which can be written as 26!. The factorial function represents the product of all positive integers so: 26! = 26 x 25 x 24 x 23 x 22 x . . . x 2 x 1

Using a scientific calculator, we get 26! = 4.03291461 x 1026

This calculation results in an extremely large number, indicating the total number of distinct substitution mappings (or keys) that can be created.