

The Number of Possible Keys

The only multipliers that are possible are those that result in one-to-one mappings. By trying all 26 possible multipliers modulo 26, we would discover that only 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, and 25 have inverses. These are the 12 positive integers that are less than 26 and relatively prime to 26. So, there are only 12 possible multiplicative keys, and one of them is 1 which would make the ciphertext alphabet the same as the plaintext alphabet.

Let's look more carefully at multiplication modulo 26. Here is the multiplication table.

Multiplication modulo 26

| | | | | | | | | | | | | | | | | | | | | | | | | | | |
|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| | 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 | 26 |
| 1 | 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 | 26 |
| 2 | 2 | 4 | 6 | 8 | 10 | 12 | 14 | 16 | 18 | 20 | 22 | 24 | 26 | 2 | 4 | 6 | 8 | 10 | 12 | 14 | 16 | 18 | 20 | 22 | 24 | 26 |
| 3 | 3 | 6 | 9 | 12 | 15 | 18 | 21 | 24 | 1 | 4 | 7 | 10 | 13 | 16 | 19 | 22 | 25 | 2 | 5 | 8 | 11 | 14 | 17 | 20 | 23 | 26 |
| 4 | 4 | 8 | 12 | 16 | 20 | 24 | 2 | 6 | 10 | 14 | 18 | 22 | 26 | 4 | 8 | 12 | 16 | 20 | 24 | 2 | 6 | 10 | 14 | 18 | 22 | 26 |
| 5 | 5 | 10 | 15 | 20 | 25 | 4 | 9 | 14 | 19 | 24 | 3 | 8 | 13 | 18 | 23 | 2 | 7 | 12 | 17 | 22 | 1 | 6 | 11 | 16 | 21 | 26 |
| 6 | 6 | 12 | 18 | 24 | 4 | 10 | 16 | 22 | 2 | 8 | 14 | 20 | 26 | 6 | 12 | 18 | 24 | 4 | 10 | 16 | 22 | 2 | 8 | 14 | 20 | 26 |
| 7 | 7 | 14 | 21 | 2 | 9 | 16 | 23 | 4 | 11 | 18 | 25 | 6 | 13 | 20 | 1 | 8 | 15 | 22 | 3 | 10 | 17 | 24 | 5 | 12 | 19 | 26 |
| 8 | 8 | 16 | 24 | 6 | 14 | 22 | 4 | 12 | 20 | 2 | 10 | 18 | 26 | 8 | 16 | 24 | 6 | 14 | 22 | 4 | 12 | 20 | 2 | 10 | 18 | 26 |
| 9 | 9 | 18 | 1 | 10 | 19 | 2 | 11 | 20 | 3 | 12 | 21 | 4 | 13 | 22 | 5 | 14 | 23 | 6 | 15 | 24 | 7 | 16 | 25 | 8 | 17 | 26 |
| 10 | 10 | 20 | 4 | 14 | 24 | 8 | 18 | 2 | 12 | 22 | 6 | 16 | 26 | 10 | 20 | 4 | 14 | 24 | 8 | 18 | 2 | 12 | 22 | 6 | 16 | 26 |
| 11 | 11 | 22 | 7 | 18 | 3 | 14 | 25 | 10 | 21 | 6 | 17 | 2 | 13 | 24 | 9 | 20 | 5 | 16 | 1 | 12 | 23 | 8 | 19 | 4 | 15 | 26 |
| 12 | 12 | 24 | 10 | 22 | 8 | 20 | 6 | 18 | 4 | 16 | 2 | 14 | 26 | 12 | 23 | 10 | 22 | 8 | 20 | 6 | 18 | 4 | 16 | 2 | 14 | 26 |
| 13 | 13 | 26 | 13 | 26 | 13 | 26 | 13 | 26 | 13 | 26 | 13 | 26 | 13 | 26 | 13 | 26 | 13 | 26 | 13 | 26 | 13 | 26 | 13 | 26 | 13 | 26 |
| 14 | 14 | 2 | 16 | 4 | 18 | 6 | 20 | 8 | 22 | 10 | 24 | 12 | 26 | 14 | 2 | 26 | 4 | 18 | 6 | 20 | 8 | 22 | 10 | 24 | 12 | 26 |
| 15 | 15 | 4 | 19 | 8 | 23 | 12 | 1 | 16 | 5 | 20 | 9 | 24 | 13 | 2 | 17 | 6 | 21 | 10 | 25 | 14 | 3 | 18 | 7 | 22 | 11 | 26 |
| 16 | 16 | 6 | 22 | 12 | 2 | 18 | 8 | 24 | 14 | 4 | 20 | 10 | 26 | 16 | 6 | 22 | 12 | 2 | 18 | 8 | 24 | 14 | 4 | 20 | 10 | 26 |
| 17 | 17 | 8 | 25 | 16 | 7 | 24 | 15 | 6 | 23 | 14 | 5 | 22 | 13 | 4 | 21 | 12 | 3 | 20 | 11 | 2 | 19 | 10 | 1 | 18 | 9 | 26 |
| 18 | 18 | 10 | 2 | 20 | 12 | 4 | 22 | 14 | 6 | 24 | 16 | 8 | 26 | 18 | 10 | 2 | 20 | 12 | 4 | 22 | 14 | 6 | 24 | 16 | 8 | 26 |
| 19 | 19 | 12 | 5 | 24 | 17 | 10 | 3 | 22 | 15 | 8 | 1 | 20 | 13 | 6 | 25 | 18 | 11 | 4 | 23 | 16 | 9 | 2 | 21 | 14 | 7 | 26 |
| 20 | 20 | 14 | 8 | 2 | 22 | 16 | 10 | 4 | 24 | 18 | 12 | 6 | 26 | 20 | 14 | 8 | 2 | 22 | 16 | 10 | 4 | 24 | 18 | 12 | 6 | 26 |
| 21 | 21 | 16 | 11 | 6 | 1 | 22 | 17 | 12 | 7 | 2 | 23 | 18 | 13 | 8 | 3 | 24 | 19 | 14 | 9 | 4 | 25 | 20 | 15 | 10 | 5 | 26 |
| 22 | 22 | 18 | 14 | 10 | 6 | 2 | 24 | 20 | 16 | 12 | 8 | 4 | 26 | 22 | 18 | 14 | 10 | 6 | 2 | 24 | 20 | 16 | 12 | 8 | 4 | 26 |
| 23 | 23 | 20 | 17 | 14 | 11 | 8 | 5 | 2 | 25 | 22 | 19 | 16 | 13 | 10 | 7 | 4 | 1 | 24 | 21 | 18 | 15 | 12 | 9 | 6 | 3 | 26 |
| 24 | 24 | 22 | 20 | 18 | 16 | 14 | 12 | 10 | 8 | 6 | 4 | 2 | 26 | 24 | 22 | 20 | 18 | 16 | 14 | 12 | 10 | 8 | 6 | 4 | 2 | 26 |
| 25 | 25 | 24 | 23 | 22 | 21 | 20 | 19 | 18 | 17 | 16 | 15 | 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 26 |
| 26 | 26 | 26 | 26 | 26 | 26 | 26 | 26 | 26 | 26 | 26 | 26 | 26 | 26 | 26 | 26 | 26 | 26 | 26 | 26 | 26 | 26 | 26 | 26 | 26 | 26 | 26 |

Notice that only 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, and 25 have multiplicative inverses modulo 26. Here are the possible multipliers and their inverses:



| | | | | | | | | | | | | |
|-------------------------------|----------|----------|-----------|-----------|----------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|
| Number | 1 | 3 | 5 | 7 | 9 | 11 | 15 | 17 | 19 | 21 | 23 | 25 |
| Multiplicative inverse | 1 | 9 | 21 | 15 | 3 | 19 | 7 | 23 | 11 | 5 | 17 | 25 |

