|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **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** |
| **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 = E(k, p) = (p + k) mod 26

P = D(k, c) = (c – k) mod 26

المود هو باقي القسمة بين رقمين:

Mod is the remaining after division between two numbers.

24 mod 10 => 24=2\*10+4=> =4

12 mod 10 => 12=1\*10+2=> =2

7 mod 10 => 7= 0\*10+7 => =7

-7 mod 10 => -7= -1\*10+3 = 3 OR (10-7 = 3)

-12 mod 10 => -12= -2\*10+8 =8

…

Let k =5:

For encryption, we change plaintext to ciphertext (produce C)

C = E(k, p) = (p + k) mod 26

C = E( 5 , p) = (5 + p) mod 26

P: the position of the letter as above.

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

H E L L O Z

H 🡪 C = (5, 7) = (5+7) mod 26 = 12 mod 26 = 12 = M (so H is encryption as M)

… (find for E L L O)

Z 🡺 C = (5, 25) = 30 mod 26 = (30=1\*26+4)= 4 = E

Or directly using the Table as:

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

For decryption:

P = D(k, c) = (c – k) mod (26)

Where c is the position of ciphertext.

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

Example: decrypt the letters (E T C I L)

E: P = D(5, 4) = (4-5) mod 26 = -1 mod 26 = 26 – 1 = 25 = Z

T: P = D (5, 19) = (19 – 5) mod 26 = 14 mod 26 = O

C: P = D (5, 2) = (2-5) mod 26= -3 mod 26 = 26-3 = 23 = X

…

**Try at class using mod formula (not the table):**

1. **Let k=18, decrypt the ciphertext: (Lzsfc qgm).**
2. **Let k=18, encrypt the plaintext: (Trust yourself)**

C = E(k, p) = (p + k) mod 26

P = D(k, c) = (c – k) mod 26

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

**Try at home:**

1. **Encrypt the plaintext (Hello there) where k= 16.**
2. **Decrypt the ciphertext ( B W N Y J ) where k = 5.**
3. **Find the result of the following:**
4. **5 mod 9.**
5. **12 mod 3.**
6. **5\*5 mod 12.**
7. **91 mod 9.**
8. **53 mod 24.**
9. **-52 mod 13.**
10. **-3 mod 4.**