Note: Plaintext is the text which you want to encrypt, and cirphertext is the resultant text after encryption

Q1. The transposition cipher aims to rearrange the letters in some way, rather than doing substitution of letters. One example is the rail-fence cipher, which encrypts encrypts the message "cryptographyiscool" by writing it in a **zig-zag** way

c . y . t . g . a . h . i . c . o .

. r . p . o . r . p . y . s . o . l

then read off the rows, giving us the ciphertext CYTGAHICORPORPYSOL .

(a) (i) Encrypt the following: “Susper is a search engine using Yacy” .

(ii) Decrypt YSHSSORCETIICRET .

(b) Another example is the columnar cipher. If we suppose that the “key” is **5**, then we will write our

message "cryptographyiscool" in **five** columns,

C R Y P T O

G R A P H Y

I S C O O L

and read it off **vertically** from left to right to get the ciphertext

CGIRRSYACPPOTHOOYL.

Without knowing the key, suggest a way to decipher the message.

2. The Caesar cipher shifts each letter in a word by a fixed number. For eg, if the number is **2**, and the shift is forward, or to the **right**, ‘a’ becomes ‘c’, ‘b’ becomes ‘d’, and so on. Hence, a Caesar shift of **3** to the right for the word “crypto” becomes “fubswr”. Sometimes when you run the Caesar cipher, one English word becomes another. For example, "COLD " becomes "FROG " if we shift everything to the right by 3. In this case we say that the shift key is +3.

Figure out which word each of the following can be encrypted to

1. FOLK
2. LATTE

3. Solve the following congruences:

(a) 7x =1 mod 17.

(b) 7x = 2015 mod 37.

(c) 7x = 2 mod 101.

4. We can use the cipher wheel (Figure 1) to encrypt/decrypt messages. Here the outer wheel is the plaintext and the inner wheel is the ciphertext.



In the example above, A is encrypted as T , G is encrypted as Z , and FUN is encrypted as YNG .

(a) Encrypt the following text,

the quick brown fox jumps over the lazy dog

(b) Decrypt the following sentence,

Rxl mabl bl max vhkkxvm tglpxk

(c) Decrypt the following sentence,

Mh ux hk ghm mh ux matm bl max jnxlmbhg