Lecture 42

09 December 2021 11:06

Cryptography

The subject of transforming information so that it cannot be easily recovered without special knowledge.

A to Z → 0 to 25 <

Most commonly used Encryption and Decryption transformation

I. **Caesar Cipher:** This approach shifts each letter three letters forward in the alphabet (sending the last three letters of the alphabet to the first three).

$$f(p) = (p+3)\ mod\ 26 \qquad f^{-1}(p) \equiv (p-3)\ mod\ 26$$

II. **Shift Cipher:** This approach shifts each letter by k steps.

$$f(p) = (p+k)\ mod\ 26 \qquad f^{-1}(p) \equiv (p-k)\ mod\ 26$$

III. **Affine Cipher:**

$f(p) = (ap+b)\ mod\ 26$, where a, b are integers.

$f(p) = (ap+b)\ mod\ 26$ is bijection iff $\gcd(a, 26) = 1$

Q24. Encrypt the message DO NOT PASS GO using Caesar cipher.

↓

$p+3$

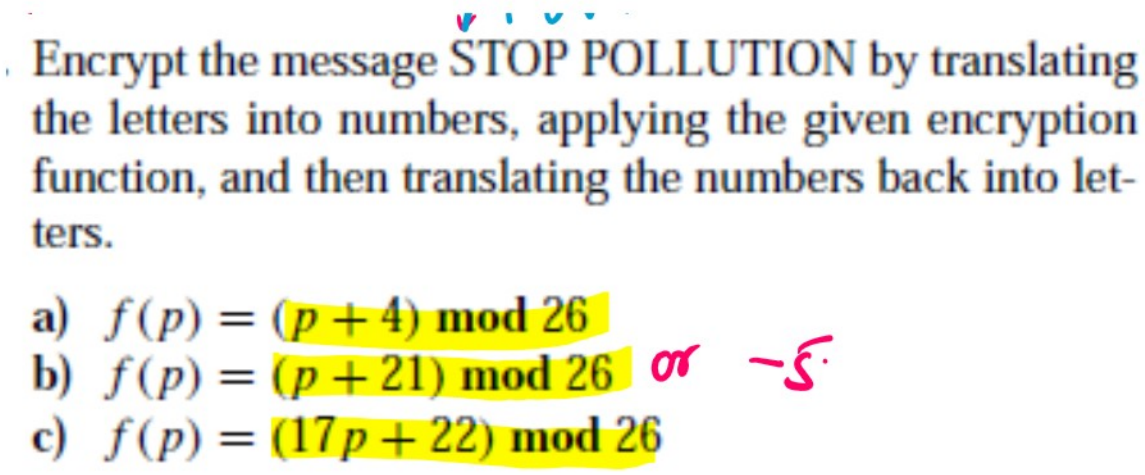
G F E

GR QRW SDVV JR.

Q25.

T U V W

Encrypt the message STOP POLLUTION by translating



Encrypt the message STOP POLLUTION by translating the letters into numbers, applying the given encryption function, and then translating the numbers back into letters.

a) $f(p) = (p + 4) \bmod 26$

b) $f(p) = (p + 21) \bmod 26$ or -5.

c) $f(p) = (17p + 22) \bmod 26$

(a) $(p+4) \bmod 21$

WXST TSPPYXMSR

(b) S T O P P O L L U T I O N

N O J K K J G G P O D J I

(c) S T O P P O L L U T I O N

18 19 14 15 15 14 11 11 20 19 8 14 13

$f(p) = (17p+22)$

328 345 260 277 277 260 209 209 362 345 158 260 243

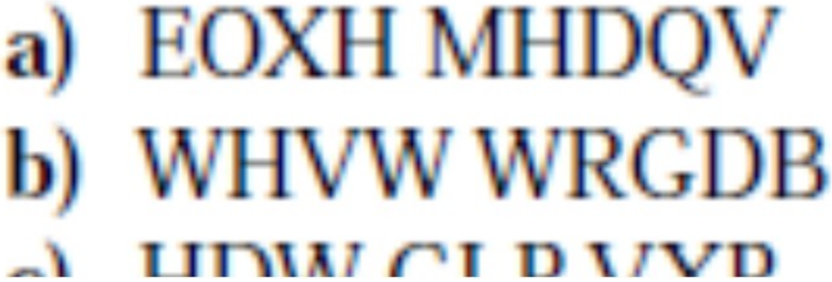
mod 26

16 7 0 17 17 0 1 1 24 7 2 0 9

Q H A R RQBB YHCAJ

Q26. Decrypt the message using Caesar cipher.

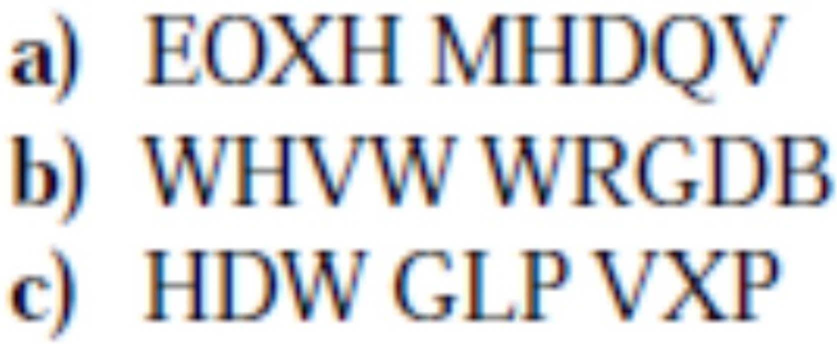
$f^{-1}(p) = (p-3) \bmod 26$



a) EOXH MHDQV

b) WHVW WRGDB

c) HDW GLP VXP



a) EOXH MHDQV

b) WHVW WRGDB

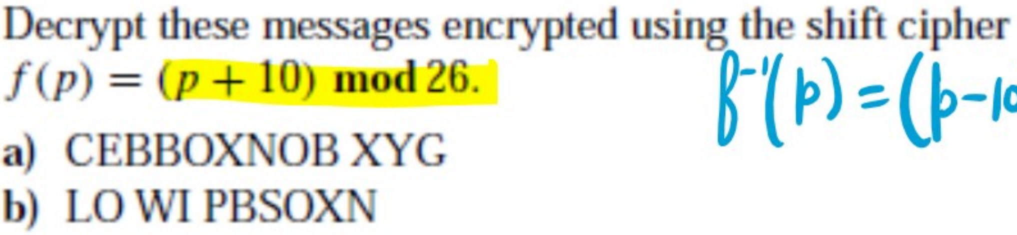
c) HDW GLP VXP

(a) BLUE JEANS

(b) TEST TODAY

(c) EAT DIM SUM

Q27.



Decrypt these messages encrypted using the shift cipher $f(p) = (p + 10) \textbf{ mod } 26.$

a) CEBBOXNOB XYG

b) LO WI PBSOXN

$f^{-1}(p) = (p-10) \bmod 26$

(a) 2 4 1 1 14 23 13 14 1   23 24 6

(p-10)

-8 -6 -9 -9 4 13 3 4 -9   13 14 -4

18 20 17 17   17   22

S U R R E N D E R   N O W

(b) BE MY FRIEND

Affine Cipher:

$f(p) = (ap + b) \; mod \; 26$, where a, b are integers.

$x = ap + b$

$p = \frac{x-b}{a}$

$f(p) = (ap + b) \; mod \; 26$ is bijection iff $\gcd(a, 26) = 1$

$f^{-1}(p) = a^{-1}(p-b) \bmod 26$

$f(p) = a(p - b) \bmod 26$

Q28.

What is the decryption function for an affine cipher if the encryption function is $c = (15p + 13) \bmod 26$?

$f^{-1}(p) = 15^{-1}(p-13) \bmod 26$

$f^{-1}(p) = 7(p-13) \bmod 26$

Relative Prime

Inverse of 15 mod 26

$y = 7,\ 26 \mid 15y - 1$

or use Bezout's Identity

$26 = 15(1) + 11 \quad 1 = 15(7) - 26(4)$

$15 = 11(1) + 4 \quad 1 = 15(3) - 11(4)$

$11 = 4(2) + 3 \quad 1 = 4(3) - 11(1)$

$4 = 3(1) + 1 \quad 1 = 4 - 3(1)$

$1 = 15(7) + 26(-4)$

Q29. Decrypt the message RTTM BXP FU MCT AHGL if the encryption function is $f(p) = (3p + 7) mod\ 26$

$f^{-1}(p) = 3^{-1}(p-7) \bmod 26,$

$f^{-1}(p) = 9(p-7) \bmod 26$

Inverse of 3 mod 26

$26 \mid 3y - 1$

$y = 9$

RTTM BXP FU MCT AHGL

17 19 19 12 1 23 15 5 20 12 2 19 0 7 6 11

$9(p-7)$

90 108 108 45 -54 144 72 -18 117 45 -45 108 -63 0 -9 36

$9(p-7)$

90 108 108 45, −54 144 72, −18 117, 45 −45 108, −63 0 −9 36

mod 26

12 4 4 19, 24 14 20, 8 13, 19 7 4, 15 0 17 10

Answer

MEET YOU IN THE PARK.