

## 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).

$$f(p) = (p + 3) \bmod 26$$

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

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

$$f(p) = (p + k) \bmod 26$$

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

- III. **Affine Cipher:**

$$f(p) = (ap + b) \bmod 26, \text{ where } a, b \text{ are integers.}$$

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

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

a ↗ f ↗ e ↗

↓  
p+3

GJR QRW SDVV JR

Q25.

↗ ↗ ↗ ↗ ↗

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)  $(p+4) \bmod 26$   
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

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

$$\begin{array}{cccccccccccc} 328 & 345 & 260 & 277 & 277 & 260 & 209 & 269 & 362 & 345 & 158 & 260 & 243 \\ \bmod 26 \end{array}$$

16 7 0 17 17 0 1 1 24 7 2 0 9  
Q H A R R Q B B Y H C A J

Q26. Decrypt the message using Caesar cipher.

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

a) EOXH MHDQV

b) WHVW WRGDB

c) HWVW WRGDB

- 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

$$f(p) = (p + 10) \bmod 26.$$

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

- a) CEBBOXNOB XYG  
b) LO WI PBSOXN

(a) 24 11 14 23 13 14 1 23 24 6

(b-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:

$$f(p) = (ap + b) \bmod 26, \text{ where } a, b \text{ are integers.}$$

$$f(p) = (ap + b) \bmod 26 \text{ is bijection iff } \gcd(a, 26) = 1$$

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

$$x = ap + b$$

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



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

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  $15 \bmod 26$

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

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  $f(p) = (3p + 7) \bmod 26$

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

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

Inverse of  $3 \bmod 26$

$$26 \mid 3y-1$$

$$y=9$$

RTTM BXP FU MCT AHGL

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

$$9(p-7)$$

26 106 110 114 118 122 126 130 134 138 142 146 150 154 158 162 166 170 174 178 182 186 190 194 198 202 206 210 214 218 222 226 230 234 238 242 246 250 254 258 262 266 270 274 278 282 286 290 294 298 302 306 310 314 318 322 326 330 334 338 342 346 350 354 358 362 366 370 374 378 382 386 390 394 398 402 406 410 414 418 422 426 430 434 438 442 446 450 454 458 462 466 470 474 478 482 486 490 494 498 502 506 510 514 518 522 526 530 534 538 542 546 550 554 558 562 566 570 574 578 582 586 590 594 598 602 606 610 614 618 622 626 630 634 638 642 646 650 654 658 662 666 670 674 678 682 686 690 694 698 702 706 710 714 718 722 726 730 734 738 742 746 750 754 758 762 766 770 774 778 782 786 790 794 798 802 806 810 814 818 822 826 830 834 838 842 846 850 854 858 862 866 870 874 878 882 886 890 894 898 902 906 910 914 918 922 926 930 934 938 942 946 950 954 958 962 966 970 974 978 982 986 990 994 998 1000

$7(p-t)$

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.