Caesar cipher / shift by 1

Alice wants to send the plaintext

$$x = \text{“Meet at Dunkin Donuts at midnight. Come alone.”}$$

Caesar cipher / shift by 1

Alice wants to send the plaintext

$$x = \text{“Meet at Dunkin Donuts at midnight. Come alone.”}$$

Then the ciphertext is

$$y = \text{NFFU BUEV OLJO EPOV UTBU NJEO JHIU DPNF BMPO F}$$

Caesar cipher / shift by 1

Bob responds with

$$y = \text{XIJD IPOF UIFS FBSF TPNB OZ}$$

What is the plaintext?

Caesar cipher / shift by 1

Bob responds with

$$y = \text{XIJD IPOF UIFS FBSF TPNB OZ}$$

What is the plaintext?

$$x = \text{“Which one? There are so many.”}$$

1. Check 3 or 4 entries to verify that this is the multiplication table for $\mathbb{Z}_7$

$\times$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

2. Calculate the following in $\mathbb{Z}_7$
   (a) $3 - 5, \quad -2 - 3, \quad 3^{-1}, \quad 2^{-1}$
   (b) $4 \cdot 3^{-1}, \quad 2 \cdot 4^{-1}, \quad 3 \cdot 5^{-2}$
   (c) $3^2, \quad 3^3, \quad 3^4, \quad 3^5, \quad 3^6, \quad 3^{12}, \quad 3^{21}$

3. Use the table to solve for x
   (a) $3^x \equiv 5 \mod 7$
   (b) $5^x \equiv 2 \mod 7$
   (c) $2^x \equiv 3 \mod 7$