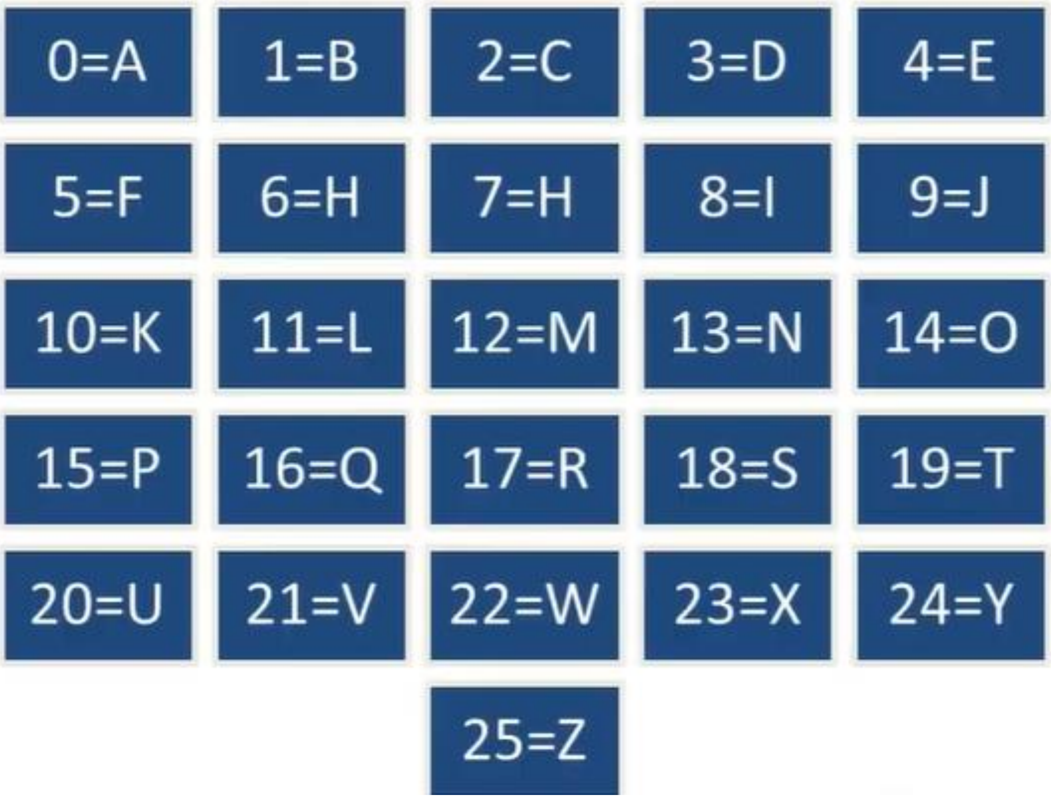
SO WHAT IS CAESAR CIPHER?

- Caesar Cipher is an encryption technique in which we replace each letter with a shift of a fixed number of letters, traditionally 3.
- For example A will be written as D, B will be written as E, C will be written as F and so on.

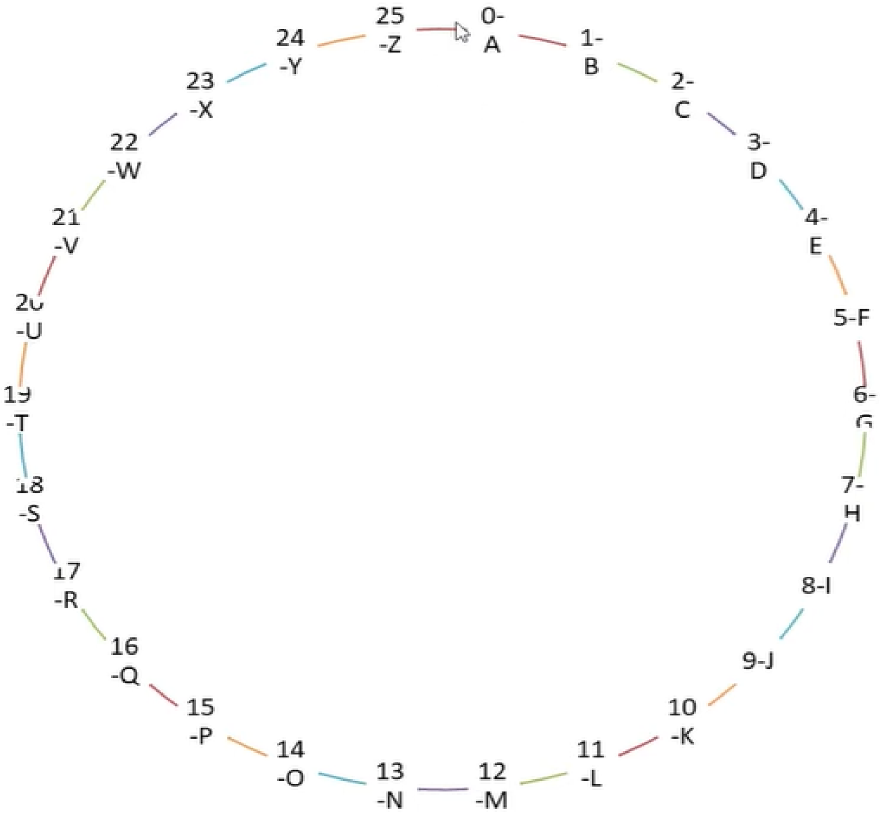
WHAT ARE THE REQUIREMENTS?

- To perform Caesar Cipher encryption you need 2 things.
- First thing is a reference table of alphabets and their numerical equivalent.
- Second the value of the shift Key.



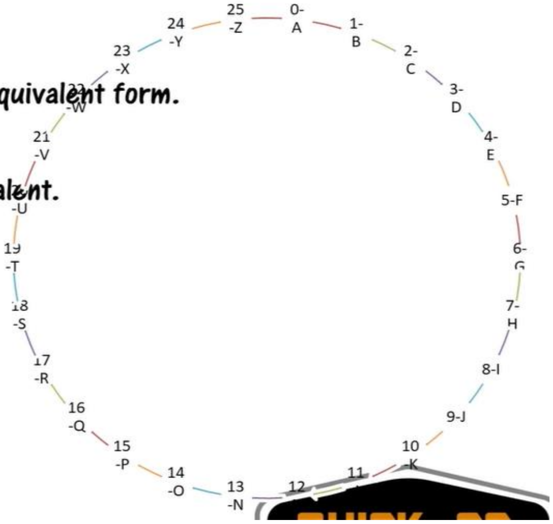
0=A	1=B	2=C	3=D	4=E
5=F	6=H	7=H	8=I	9=J
10=K	11=L	12=M	13=N	14=O
15=P	16=Q	17=R	18=S	19=T
20=U	21=V	22=W	23=X	24=Y
		25=Z		

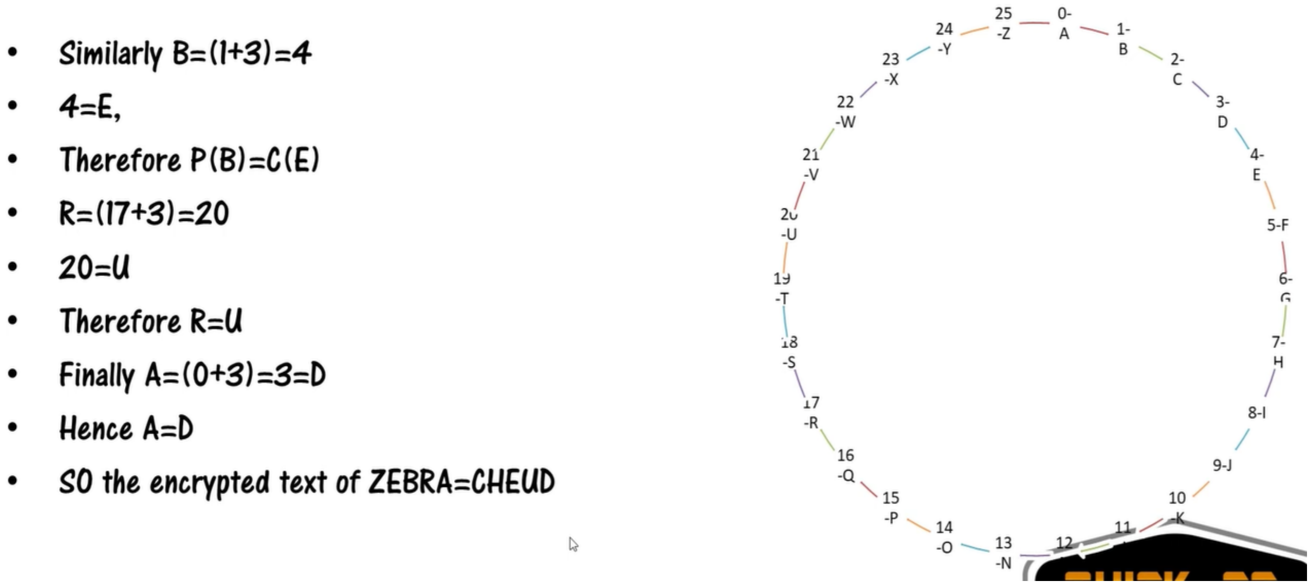
CYCLE OF LETTERS

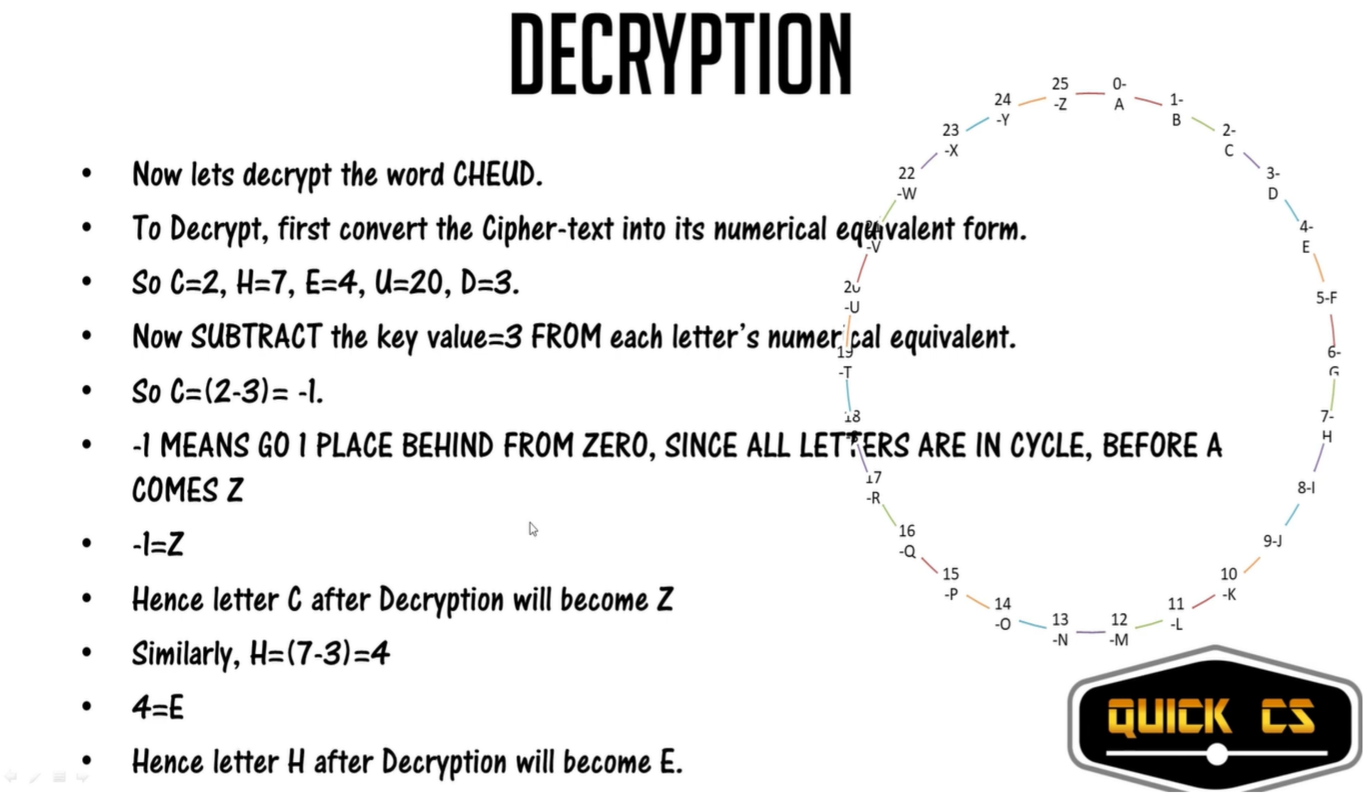


ENCRYPTION

- Now lets encrypt the word ZEBRA.
- To encrypt, first convert the Plaintext into its numerical equivalent form.
- So Z=25, E=4, B=1, R=17, A=0.
- Now add the key value=3 to each letter's numerical equivalent.
- So Z=(25+3)=28.
- 28=C
- Hence letter Z after Encryption will become C
- Similarly, E=(4+3)=7
- 7=H
- Hence letter E after encryption will become H.



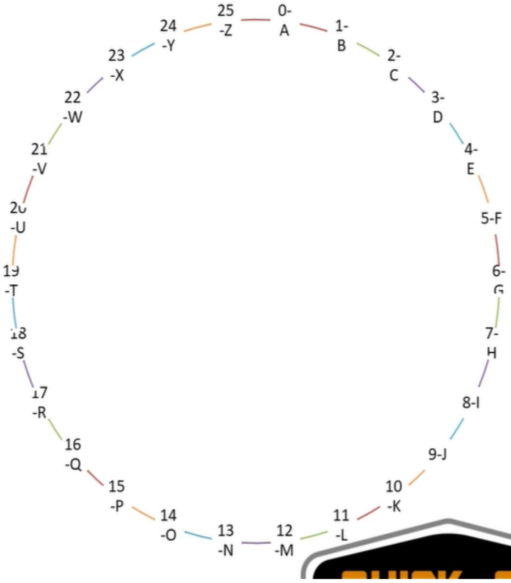

- Similarly B=(1+3)=4
- 4=E,
- Therefore P(B)=C(E)
- R=(17+3)=20
- 20=U
- Therefore R=U
- Finally A=(0+3)=3=D
- Hence A=D
- SO the encrypted text of ZEBRA=CHEUD


DECRYPTION

- Now lets decrypt the word CHEUD.
- To Decrypt, first convert the Cipher-text into its numerical equivalent form.
- So C=2, H=7, E=4, U=20, D=3.
- Now SUBTRACT the key value=3 FROM each letter's numerical equivalent.
- So C=(2-3)= -1.
- -1 MEANS GO 1 PLACE BEHIND FROM ZERO, SINCE ALL LETTERS ARE IN CYCLE, BEFORE A COMES Z
- -1=Z
- Hence letter C after Decryption will become Z
- Similarly, H=(7-3)=4
- 4=E
- Hence letter H after Decryption will become E.

DECRYPTION

- Similarly E=(4-3)=1
- 1=B,
- Therefore C(E)=P(B)
- U=(20-3)=17
- 17=R
- Therefore U=R
- Finally D=(3-3)=0=A
- Hence D=A
- SO the Decrypted text of CHEUD=ZEBRA


0-A
1-B
2-C
3-D
4-E
5-F
6-G
7-H
8-I
9-J
10-K
11-L
12-M
13-N
14-O
15-P
16-Q
17-R
18-S
19-T
20-U
21-V
22-W
23-X
24-Y
25-Z