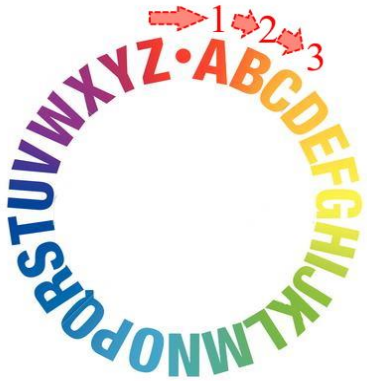
A criptografia desenvolvida é baseada no método de criptografia *zenit polar*, esse método de criptografia é bem simples e é comumente usado para passar recados simples sem que uma autoridade descubra, um caso clássico seria para passar bilhetes entre dois alunos sem que o professor descobrisse o que está escrito.

É claro que usar somente o Zenit Polar não criaria uma criptografia suficientemente forte, já que ela poderia ser resolvida até em uma folha de papel se necessário, então o grupo teve a ideia de incorporar a Cifra de Cesar no Zenit Polar para resolver esse problema.

O usuário digita um número chave e esse número dita quantas casa as letras devem pular para se tornarem novas letras, essa mudança, além de adicionar uma variável para a descoberta da criptografia, aumenta a quantidade de possibilidades que uma frase possui

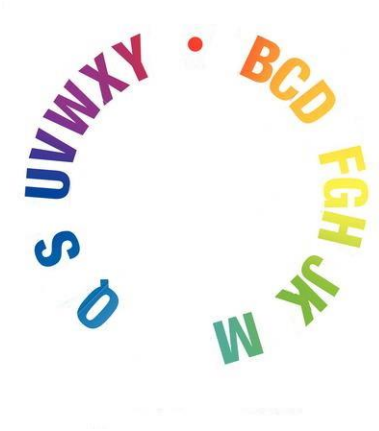
Passo 1: Vamos supor que a chave digitada pelo usuário seja ‘3’, isso significa que a nova letra será a terceira letra depois do original, essa ilustração representa o abecedário completo formando um círculo, se usarmos ele como representação, ele circularia no sentido horário.



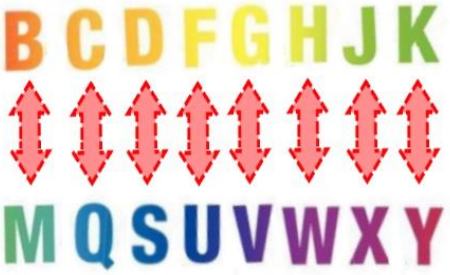
Passo 2: Vamos começar a substituir as letras por ordem, começando pela ‘Z’, acaba que a letra Z é um exemplo perfeito já que podemos representar porque é mais fácil mostrar o abecedário como círculo, quando a cifra chega ao fim do alfabeto, ao invés de parar na última letra, ela faz um loop pelo alfabeto e continua. Como mostrado na representação, a nova letra que ocupará o lugar de ‘Z’ será a letra ‘C’ se usarmos a chave 3

Isso é repetido com todas as letras da *Zenit Polar* devido ao método que a criptografia foi desenvolvida não haverá repetições de letras, então esse fator está fora do programa.

Só nesses dois processos já temos uma criptografia razoavelmente forte e totalmente definida por uma chave que é escolhida pelo usuário, mas as letras que estão fora da criptografia ainda não são alteradas, então resolvemos criar um método que exclui as letras já usada e faz basicamente uma segunda *Zenit Polar* com o resto do abecedário para assim chegarmos a possibilidades tão extremas que somente seria possível a descriptografia usando o programa criado.



Passo 3: A imagem ao lado é uma representação do resto do abecedário sem as letras que compõem o Zenit Polar, lembrando que as letras excluídas do abecedário podem variar de acordo com a chave colocada pelo usuário.
A quantidade de letras restante sempre serão 16 letras, para criarmos uma criptografia estilo o Zenit Polar, precisamos de um número par e dividi-lo em duas partes, assim ficaremos com duas partes com 8 letras cada uma.



Passo 4: se usarmos o padrão de Zenit Polar original teremos a seguinte segunda criptografia, onde a primeira metade do alfabeto faz substituição com a segunda parte do alfabeto, assim todas as letras tornam-se diferentes de sua mensagem anterior.

A criptografia agora, além de substituir as letras que foram rodadas pela cifra de Cesar junto com a zenit polar, substitui o resto das letras por seus “espelhos” e torna uma frase totalmente diferente da outra se a chave não estiver de acordo com as especificações

Um exemplo prático seria, ao digitar a frase “*OLA MUNDO*” e usar a chave 0 o programa te exibira: “*ENI BFLSE*”, mas se usar a chave 3 o programa te exibira “*QDM AWBLQ*” assim podemos deduzir que está criptografia é inquebrável, ou pelo menos, muito difícil de ser quebrada sem o uso do programa desenvolvido.

Mestrin Club