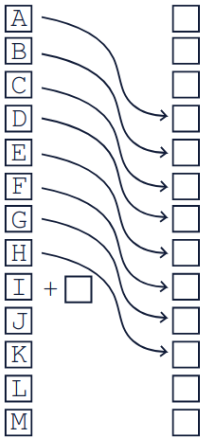
INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Professor: Macêdo Firmino
Disciplina: Segurança de Redes de Computadores
Prática 12: Criptografia (Cifra de Cesar)

Cifra de César

A Cifra de César, também conhecida como cifra de troca, é uma das mais simples e conhecidas técnicas de criptografia. É um tipo de cifra de substituição na qual cada letra do texto é substituída por outra, que se apresenta no alfabeto abaixo dela um número fixo de vezes. Por exemplo, com uma troca de três posições, A seria substituído por D, B se tornaria E, e assim por diante. O nome do método é em homenagem a Júlio César, que o usou para se comunicar com os seus generais.



As letras serão substituídas por letras ☐ posições à frente

A transformação pode ser representada alinhando-se dois alfabetos; o alfabeto cifrado é o alfabeto normal rotacionado à direita ou esquerda por um número de posições. Por exemplo, aqui está uma cifra de César usando uma rotação à esquerda de três posições (o parâmetro de troca, três neste caso, é usado como chave).

```
Normal:  ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cifrado: DEFGHIJKLMNOPQRSTUVWXYZABC
```

Para criptografar uma mensagem, deve-se simplesmente observar cada letra da mensagem na linha "Normal" e escrever a letra correspondente na linha "Cifrado". Para descriptografar, deve-se fazer o contrário.

```
Normal:  voce ganhou um ponto
Cifrado: yrfh jdqkrx xp srqwr
```

Atualmente, A cifra de César é utilizada para fins didáticos pois ela pode ser facilmente decifrada usando as mesmas técnicas usadas análise de frequência ou verificando os padrões de palavras. Por exemplo, uma vez que existe apenas um número limitado de rotações possíveis (26 em português, se desconsiderarmos o uso de cedilha e letras acentuadas), cada uma pode ser testada por turno num ataque de força bruta, ou se for um texto grande, tentar observar as letras que mais se repetem (na língua portuguesa seria a letra "a", "e", "o"e "s", por exemplo, são as quatro mais utilizadas na nossa língua).

Atividade

1. Forme duplas. Cada dupla irá criar uma mensagem secreta com no máximo 30 caracteres e colocar no quadro.

2. Quando todas as mensagens estiverem no quadro, os grupos irão tentar decifrar os códigos secretos dos outros grupos. O grupo vencedor será o que conseguir decifrar o maior número de códigos.