

Questão 149

**QUESTÃO 149**

A criptografia refere-se à construção e análise de protocolos que impedem terceiros de lerem mensagens privadas. Júlio César, imperador romano, utilizava um código para proteger as mensagens enviadas a seus generais. Assim, se a mensagem caísse em mãos inimigas, a informação não poderia ser compreendida. Nesse código, cada letra do alfabeto era substituída pela letra três posições à frente, ou seja, o "A" era substituído pelo "D", o "B" pelo "E", o "C" pelo "F", e assim sucessivamente.

|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |                           |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---------------------------|
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | Letra do texto codificado |
| ↑ | ↑ | ↑ | ↑ | ↑ | ↑ | ↑ | ↑ | ↑ | ↑ | ↑ | ↑ | ↑ | ↑ | ↑ | ↑ | ↑ | ↑ | ↑ | ↑ | ↑ | ↑ | ↑ | ↑ | ↑ | ↑ | ↑ | ↑ | ↑ |                           |
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |   |   |   | Letra do texto original   |

Disponível em: [www.codifica.ibict.br](http://www.codifica.ibict.br). Acesso em: 15 out. 2019.

Qualquer código que tenha um padrão de substituição de letras como o descrito é considerado uma Cifra de César ou um Código de César. Note que, para decifrar uma Cifra de César, basta descobrir por qual letra o "A" foi substituído, pois isso define todas as demais substituições a serem feitas.

Uma mensagem, em um alfabeto de 26 letras, foi codificada usando uma Cifra de César. Considere a probabilidade de se descobrir, aleatoriamente, o padrão utilizado nessa codificação, e que uma tentativa frustrada deverá ser eliminada nas tentativas seguintes.

A probabilidade de se descobrir o padrão dessa Cifra de César apenas na terceira tentativa é dada por

- A**  $\frac{1}{25} + \frac{1}{25} + \frac{1}{25}$
- B**  $\frac{24}{25} + \frac{23}{24} + \frac{1}{23}$
- C**  $\frac{1}{25} \times \frac{1}{24} \times \frac{1}{23}$
- D**  $\frac{24}{25} \times \frac{23}{25} \times \frac{1}{25}$
- E**  $\frac{24}{25} \times \frac{23}{24} \times \frac{1}{23}$

**RESOLUÇÃO**

**ALTERNATIVA E**

Como há um total de 26 letras, a probabilidade de escolher a letra incorreta na primeira tentativa é  $\frac{24}{25}$

Eliminando-se esta letra, a probabilidade de escolher outra letra incorreta na segunda tentativa é  $\frac{23}{24}$

Eliminando-se as duas letras das primeiras tentativas, a probabilidade de escolher a terceira letra corretamente é  $\frac{1}{23}$

Sendo assim, tem-se  $\frac{24}{25} \cdot \frac{23}{24} \cdot \frac{1}{23}$