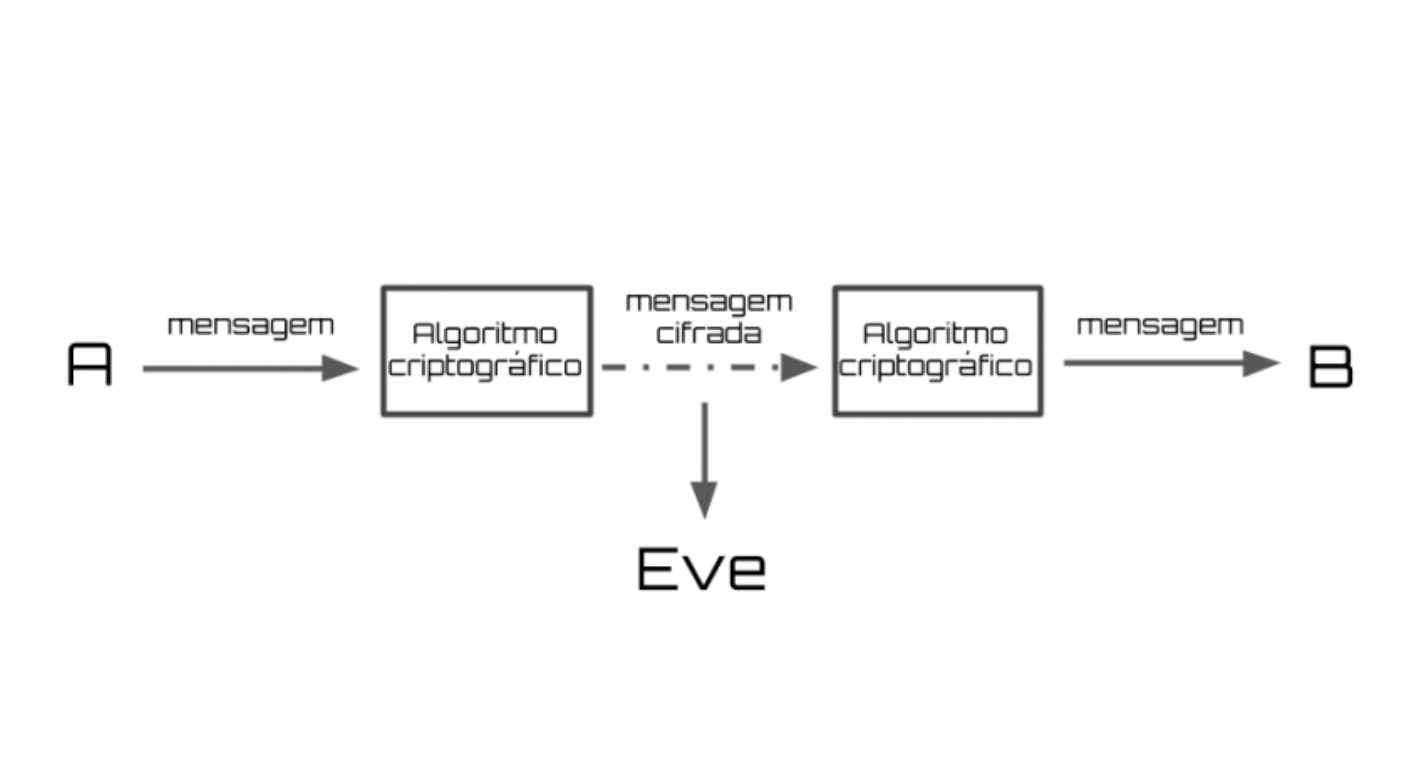
O que é criptografia?

Criptografia vem do grego *kryptós* e *graphein*, que significam "secreta" e "escrita", respectivamente. Até a era moderna, ela era sinônimo de *encriptação*, que é a conversão de uma mensagem legível para algo aparentemente sem sentido.

Para entender melhor essa ideia, digamos que **Alice** quer mandar uma mensagem para **Bob** sem que **Eve** descubra seu counteúdo.

Para isso, **Alice** usa um certo algoritmo para tornar a mensagem ilegível de forma que só **Bob** sabe como reverter a mensagem encriptada.



Assim, caso **Eve** consiga a mensagem ela, sem saber o algoritmo que **Alice** usou, não será capaz de entender a mensagem.

Ao longo da história, várias técnicas de ocultar mensagens foram desenvolvidas. Antes da criptografia pré-computacional, a **criptografia clássica** era formada por um conjunto de métodos de *substituição* e *transposição* de caracteres, porém com o advento da computação, a **criptografia moderna** se tornou amplamente embasada em teorias matemáticas e práticas de ciência da computação.

Revision #5

Created Thu, Dec 20, 2018 1:54 PM by Cainotis

Updated Mon, Jan 28, 2019 9:58 PM by

Andrew