

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, e é esse o conceito usado em CTFs.

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

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



Assim, quando *Eve* interceptar a mensagem por meio do canal inseguro, se ela não possui o algoritmo criptográfico usado por *Alice* e *Bob*, ela 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. E com o advento da computação, a **criptografia moderna** se tornou amplamente embasada em teorias matemáticas e práticas de ciência da computação.

Para esse guia, começaremos com os métodos da criptografia clássica.

Updated Sat, Oct 6, 2018 6:45 PM by Andrew