Para saber mais: bytes aleatórios e pseudo aleatórios

Nessa aula, usamos o método `randomBytes()` do módulo `crypto` para gerar a chave da assinatura dos tokens. Porém, apesar do nome do método ser sugestivo, ele não gera bytes *realmente* aleatórios, mas sim, *pseudo aleatórios* (como a própria documentação do método (https://nodejs.org/api/crypto.html#crypto_crypto_randombytes_size_callback) descreve).

Um dado **pseudo aleatório** é previsível e reprodutível. Como são gerados por algoritmos, se possuírem a mesma entrada alguém poderia usar esse mesmo algoritmo e gerar o mesmo número. Por outro lado, um dado **realmente aleatório** é imprevisível, normalmente obtido de ruídos atmosféricos ou de circuitos elétricos. O Khan Academy possui um vídeo (https://www.khanacademy.org/computing/computer-science/cryptography/crypt/v/random-vs-pseudorandom-number-generators) bem didático e detalhado sobre isso.

Em geral, esses geradores de números pseudo aleatórios recebem uma entrada realmente aleatória (chamada de *seed*), que fornece a

segurança para o algoritmo. No caso do método `randomBytes()`, a documentação afirma que os valores gerados são criptograficamente seguros e a entrada é coletada da [entropia do seu computador (https://pt.wikipedia.org/wiki/Entropia_%28computa%C3%A7%C3%A3o%29)](). Assim, os bytes gerados são suficientemente aleatórios na prática.