Lab: Weak Keys in DES

Exercise 1:
The DES specification in Cryptol is provided in files `DES.cry` and `Cipher.cry`. Add a property that will allow you to find all weak keys for DES.

Definition: *weak keys of DES* are keys that result in all per-round keys being identical.

Help: in `DES.cry` there is a function called `expandKey` that takes a key as argument and produces a sequence of 16 per-round keys. All you have to do is create a function that checks whether all 16 numbers in the sequence are the same. Then create a property that compares the output of that function to something such that the comparison is `True` if and only if all 16 per-round subkeys are the same.

Exercise 2:
A key is not desirable if encrypting twice produces the original plaintext. Determine whether such keys exist for DES and, if so, provide one such.