

## Find Weak Keys of DES

The DES specification in cryptol is provided in  
<http://gauss.ececs.uc.edu/Courses/c6021/labs/DES.cry> and  
<http://gauss.ececs.uc.edu/Courses/c6021/labs/Cipher.cry>  
Add a property that will allow you to find weak keys for DES.  
Find all of them and submit your modified DES.cry.

**Definition:** *weak keys of DES*: 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` iff all 16 per-round subkeys are the same.

Submission instructions: <http://gauss.ececs.uc.edu/Courses/c6021/labs/submit.html>