Programming assignment 1

1 Problem

Implement DES as specified in the FIPS 46-3 standard in a scripting language such as Perl, Python, Tcl etc. All else failing, Java, C, C++, C# are also OK. Your programs should build and execute on **sunfire.comp**. The deadline for submission is October 11.

2 Submission

Your submission must include a README file that describes the contents of all the files in your submission. You must also include a Makefile that builds your program and any needed environment by just typing **make**. The executable built on typing "make" should be called **des**. Collect all the files in a tarred compressed archive (**.tgz**) and submit this single file. Instructions on how to submit this file will be made available later.

The input/output interface of **des** should be as follows:

des k=0000000000000000 t=1234567812345678

must generate an output approximating[1] the following:

```
t=1234567812345678
k=0000000000000000
c=4A438AC15D8074B5
  Round Key  |    Left  | Right    |
000000000000 | ccff6600 | 00aa8855 |
000000000000 | 00aa8855 | a0baa620 |
000000000000 | a0baa620 | e08b57d9 |
       ..............
000000000000 | acc01507 | 5bd0d09a |
```

There are sixteen round keys, and the left and right denote the L_i and R_i register values for each round.

3 For extra pizazz (but not extra credit)

Write a procedure that generates data to drive a graphical library, for e.g., **graphviz** (although graphviz is not really suitable for this purpose because you can't finely control the layout of graphical elements) that will display the entire structure of the DES computation in a scrollable (both LR & TB) widget. Java 2D might be a good candidate. There's also SVG that might be appropriate. Posterity will thank you for it and it'll look great on your resumé.

[1] Very closely.