CSEC 507 Homework 2

Simge Tekin

1) This implementation uses string abstraction of bits. User input is converted into a string of zeros and ones, and all the operations are performed on that string.

main.c: Contains the DES function, where the algorithm is performed.
utils.h: Contains utility functions and constants such as permutation tables.

Key(hex):0123456789abcdef
IV(hex):0123456789abcdef

Untar the files:

```
~$:tar -xzvf simge_tekin_des.tar.gz
```

Compilation:

```
~$ make
```

Run:

```
~$./des
```

Program asks for user input (max input size is 64 characters). Alternatively it can be run as ./des<input.txt (this file should end with a newline character).

2)

When “Simge Tekin” is entered as input, the following output is obtained:

Plaintext: Simge Tekin
Padded hexadecimal text: 53696d67652054656b696e8000000000
Ciphertext: 059327bf2544c0b70155b2119d4ff172
Time: 0.000481

3) 302.892374 seconds on Intel(R) Core(TM) i5-5300U CPU @ 2.30GHz

This implementation is not an efficient one it includes lots of string operations such as copying.