# Programming Assignment

Read the paper (particularly Section 1, 2 and Appendix) about Ron Rivest's RC6 (version 1.1), which can be downloaded from: http://people.csail.mit.edu/rivest/pubs/RRSY98.pdf. Implement the RC6-w/r/b, where w = 32, and r = 20. So you can use the test vectors on page 20 to debug your program. The input of your program should be the user key and either plaintext (for encryption) or ciphertext (for decryption). The output of your program should be the ciphertext (for decryption) or plaintext (for encryption). Use a README file to explain how the program should be executed. It's OK to discuss with your classmates about the details of the paper, but you should finish programming by yourself.

## Submission guidelines

Please hand in your **source code** and a **Makefile** electronically (**please do not submit .o or executable code**). You must make sure that your code compiles and runs correctly on a Linux machine.

Write a **README** file (**text file, do not submit a .doc file**) which contains

§ Your name and email address

§ Whether your code was tested on bingsuns.

§ Your program runs as follows: "./run ./input.txt ./output.txt", where input.txt is the input file, and output.txt is the output file. The format of input.txt and output.txt is shown on the next slides.

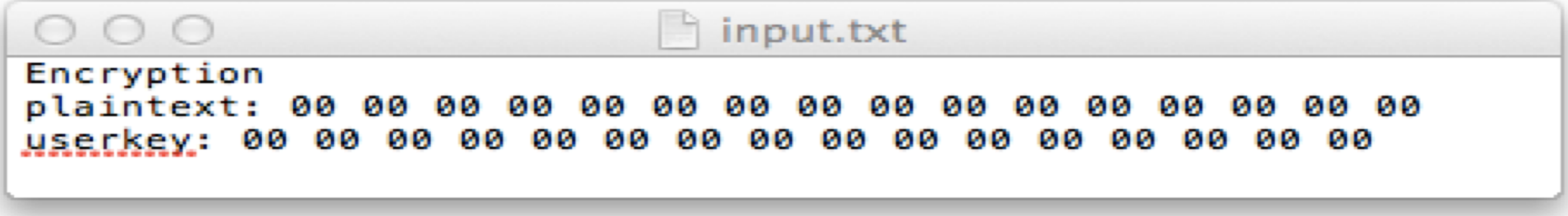
§ Briefly describe your algorithm or anything special about your submission that the TA should take note of.

Place all your files under one directory with a unique name (such as p1-[userid] for assignment 1, e.g., p1-ghyan).

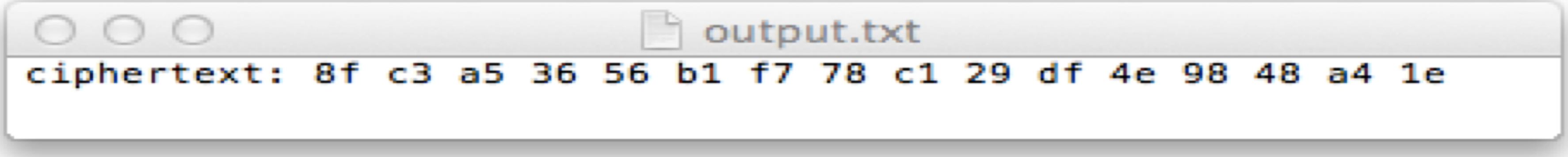
Tar the contents of this directory using the following command: **tar –cvf [directory_name].tar [directory_name]** E.g., tar -cvf p1-ghyan.tar p1-ghyan/

Use the Blackboard to upload the tared file you created above.

# Encryption

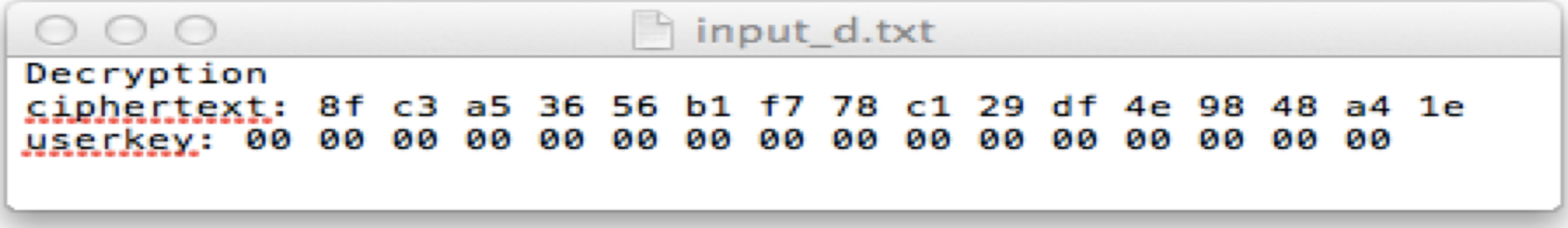


```
Encryption
plaintext: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
userkey: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

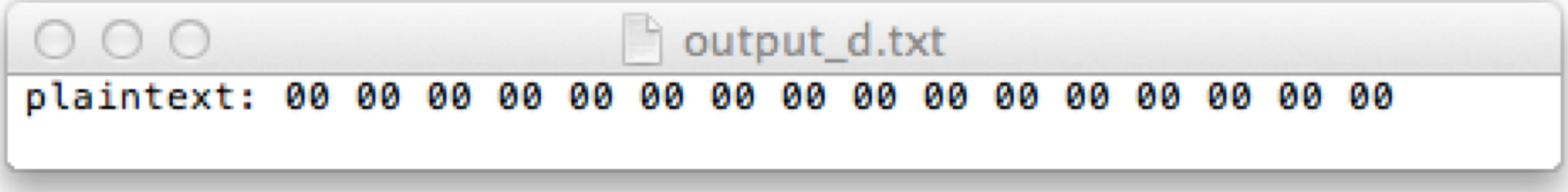


```
ciphertext: 8f c3 a5 36 56 b1 f7 78 c1 29 df 4e 98 48 a4 1e
```

# Decryption



```
Decryption
ciphertext: 8f c3 a5 36 56 b1 f7 78 c1 29 df 4e 98 48 a4 1e
userkey: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```



```
plaintext: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```