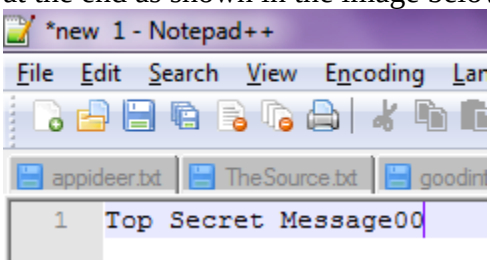
CECS 285: Lab 9

OBJECTIVES:

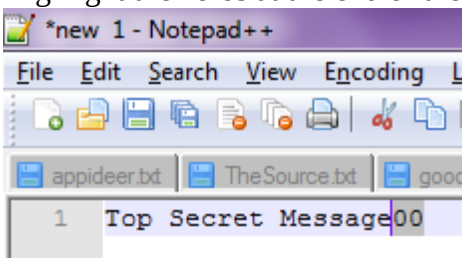
- Use Serial Communication to perform very basic symmetrical XOR encryption

ACTIVITY 1: Create a plain text file to be encrypted. The program that will be use requires a null terminating character to be contained at the end of the plain text file. This can be done in the following fashion.

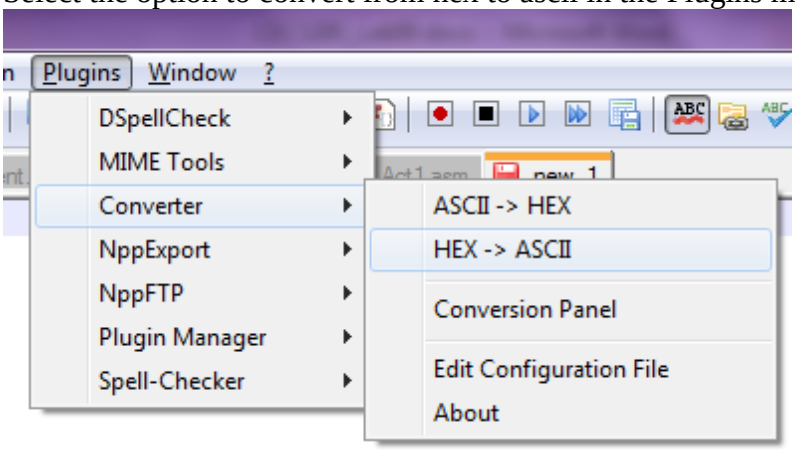
1. Use Notepad++ to create a text file with some text to be encrypted followed by two zeros at the end as shown in the image below:



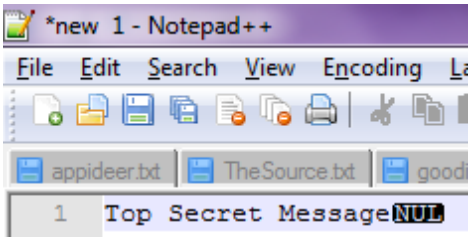
2. Highlight the zeros at the end of the message



3. Select the option to convert from hex to ascii in the Plugins menu



4. The two zeros should now become a NUL character:



5. Save your file as **Plain.txt** and it will be encrypted later in this lab.

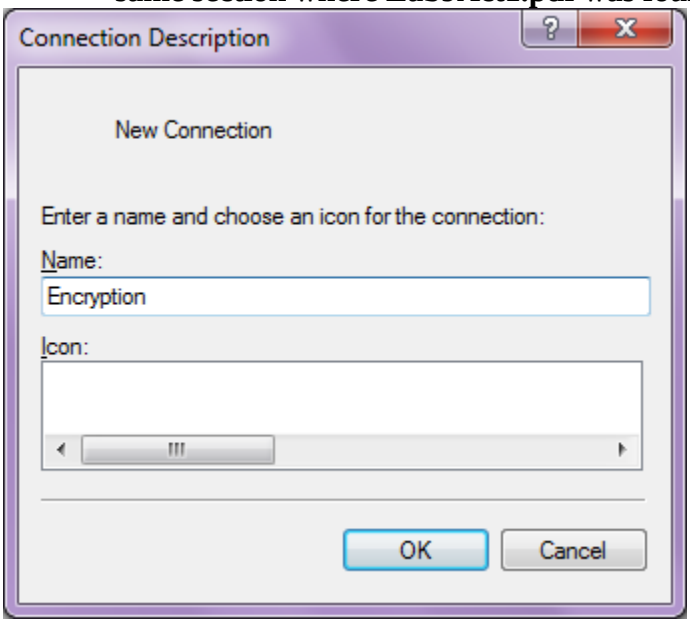
ACTIVITY 2: Use the 8051 and serial console to read a plain text file and write back encrypted 'cipher text' to the host computer. A very basic symmetrical XOR encryption program is given on beachboard which you will modify in the next activity:

Find the source code for activity 1 on **beachboard** in the **Content** section under the **Lab9_Files** subsection contained in **Lab9Act1.pdf**.

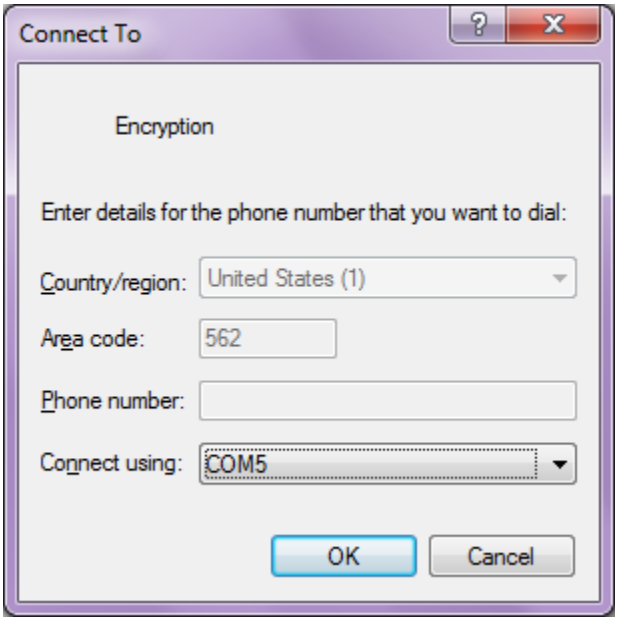
Type the program into the Keil development environment then proceed to Activity 3.

ACTIVITY 3: Run the software on your 8051 to encrypt/decrypt a plain text file. This is accomplished in the following steps.

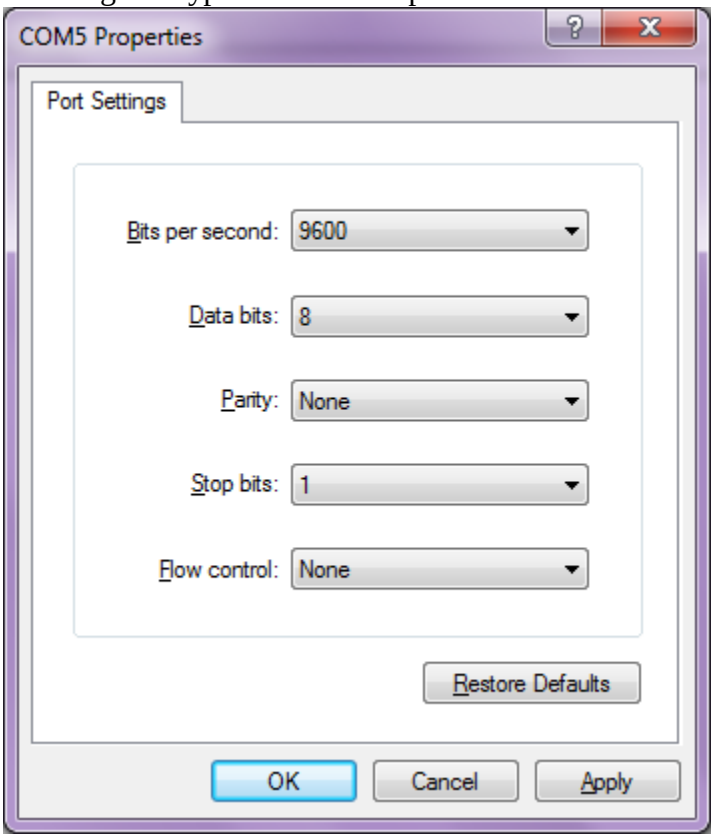
1. Use the source code referenced Lab9Act1.pdf to create a hex file.
2. Load the hex file onto your 8051.
    a. **If you are using LabPro51 and flip then close the flip application before proceeding to the next step**
3. Open Hyperterminal (if not done so already)
    a. **If you need Hyperterminal it can be downloaded from beachboard in the same section where Lab9Act1.pdf was found**



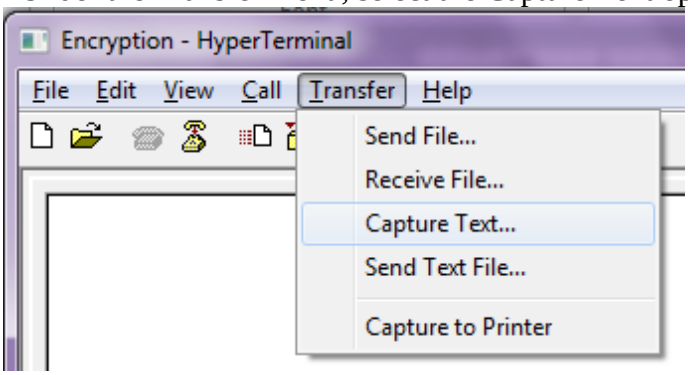
4. If your 8051 is connected to your computer through a direct serial connect then select COM 1, otherwise the highest numbered COM port should correspond to your USB/Serial Converter facilitated connection to 8051



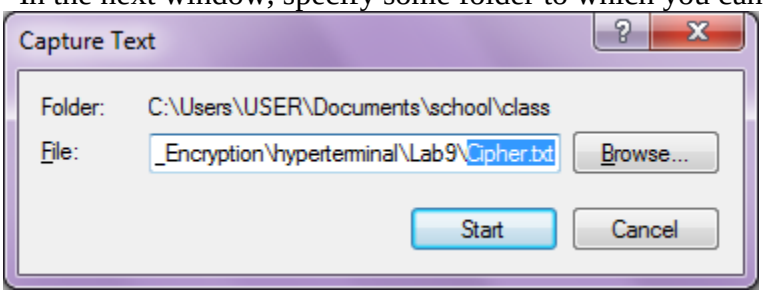
5. Configure Hyperterminal to operate with the following settings:



6. Ensure your 8051 has it's switch set to the RUN position and hit the Reset button
7. Under the Transfer menu, select the Capture Text option.

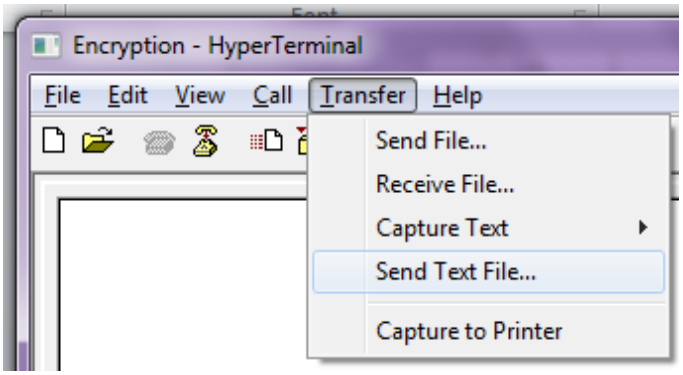


8. In the next window, specify some folder to which you can write the Cipher.txt

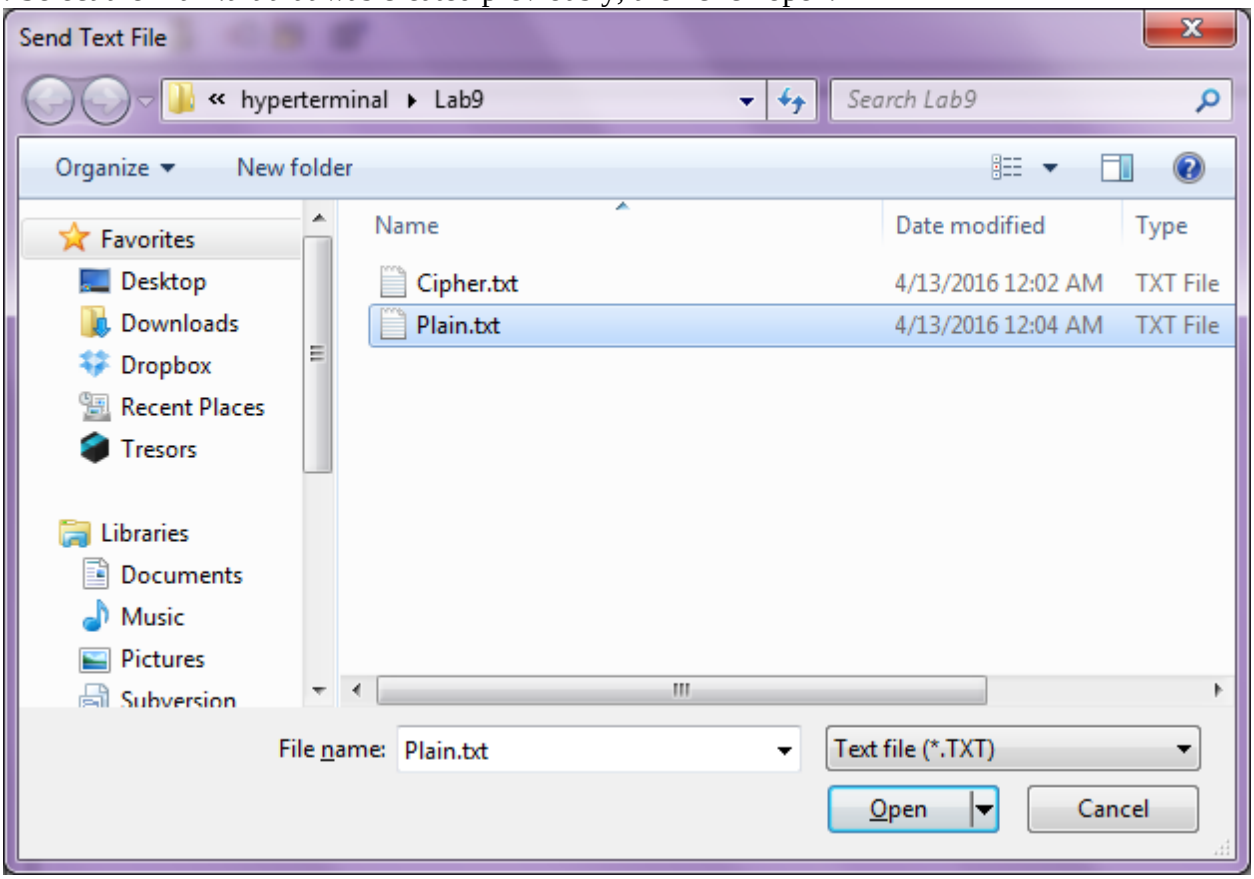


9. Press the Start button shown in the window above.

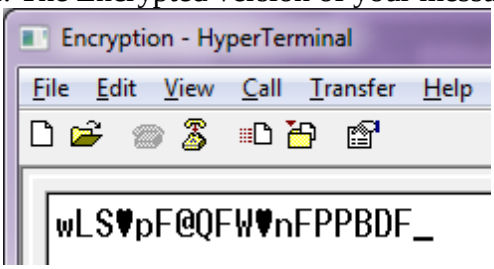
10. Click the Transfer menu and then select Send Text File:



11. Select the Plain.txt that was created previously, then click open.

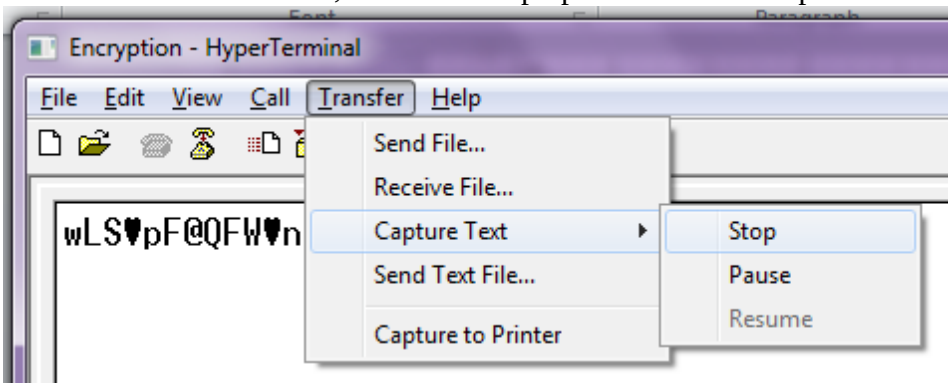


12. The Encrypted version of your message will appear in Hyperterminal:

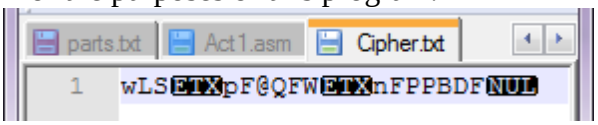


13. In the following step you will save this message

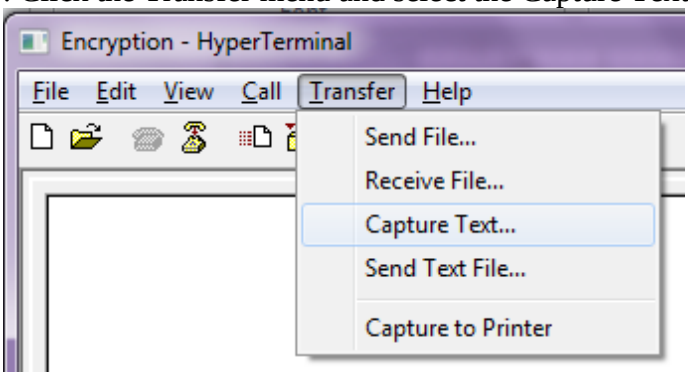
14. Click the Transfer Menu, select the Stop option under the Capture Text sub menu.



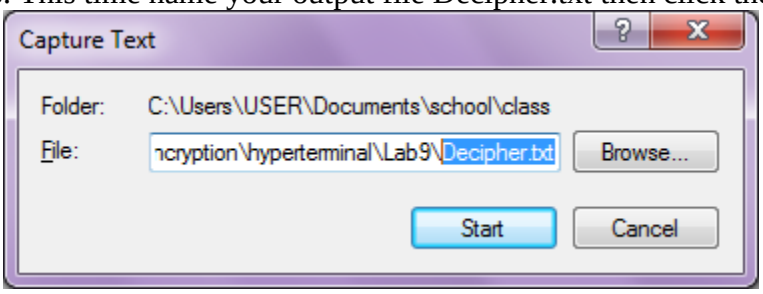
15. The encrypted message will now have been written the file named Cipher.txt, open the file to verify its contents. Note the NUL character is still at the end which is important for the purposes of this program.



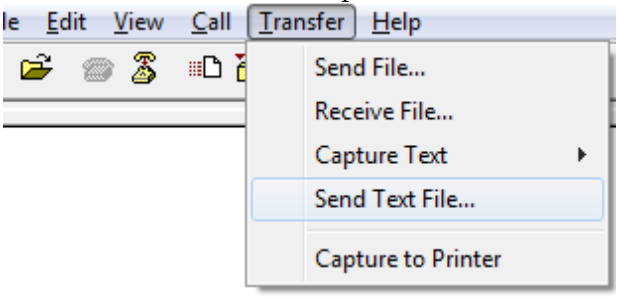
16. Now to decrypt your message, first press the reset button on your 8051
17. Click the Transfer menu and select the Capture Text option



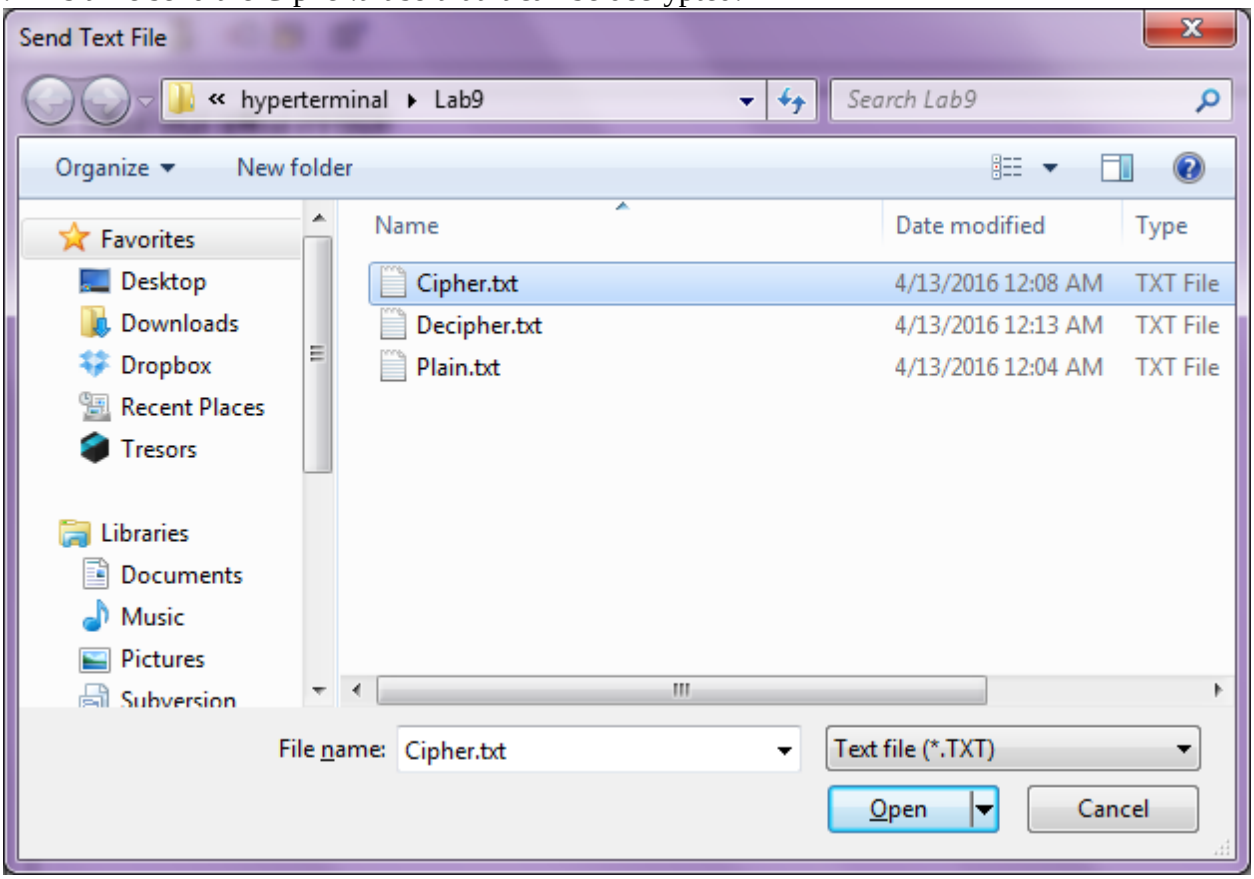
18. This time name your output file Decipher.txt then click the Start button



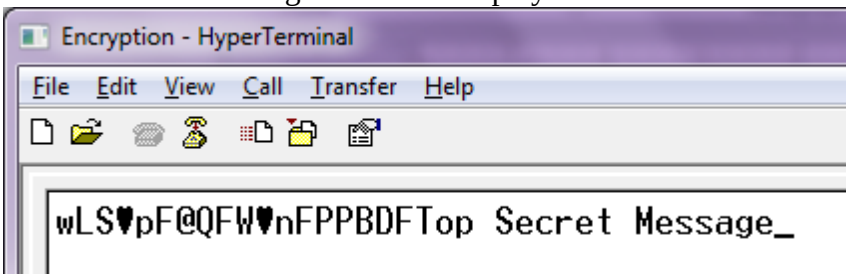
19. Select the send text file option:



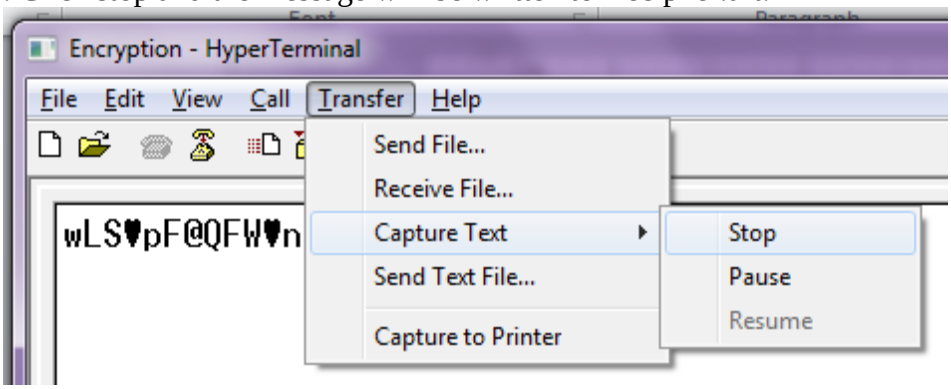
20. This time send the Cipher.txt so that it can be decrypted:



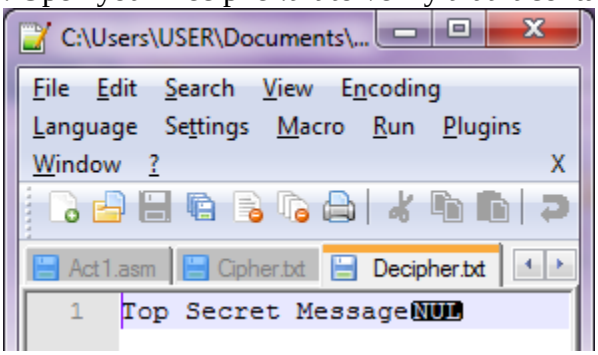
21. The Plain text message should be displayed in the console:



22. Click stop and the message will be written to Decipher.txt.



23. Open your Decipher.txt to verify that it contains the original message:



24. Proceed to the next Activity

Activity4: Repeat the process outlined in Activity3 using:

- a plain text message of your choosing which must be at least 30 characters long and must be a legitimate message i.e. song, quote, statement, haiku, … not random characters
- a keyval of your choosing (something other than 0x23 used in the example)

Take screenshots of the following steps in the process:

- a screenshot showing the contents of your plain text file with NUL character
- a screenshot showing the encrypted message displayed in Hyperterminal
- a screenshot showing the contents of your cipher text file with NUL character

Deliverables:

- The screenshots specified in Activity 4
- Manual verification that the first 4 characters of your plain text message were encrypted correctly with your key. To represent this manual verification:
  - Convert each of the first four ascii characters to hex ascii encoded value
  - Convert the raw hex of the first four characters to binary
  - Exclusive Or each binary quantity with your chosen key to produce the binary encrypted value that represents the encrypted character
  - Convert the binary encrypted value that represents the encrypted character to hex
  - Convert the hex value that represents the encrypted value to its corresponding ascii character

There is no demo portion for this lab