Homework #3

You must submit your work to your instructor before midnight on due date. Failure to do so will result in late penalties, [see the syllabus for grading detail](#).

Submit your work on the Blackboard before midnight the day the homework is due. Here are the requirements for your Blackboard submission:

- Attach the assignment as a compressed archive file (.zip, .tgz, .tbz2, .rar) Include in the archive a copy of any code you've written in order to get the assignment done.
- The name of the file should be: *firstName-lastName-HW-assignmentNumber.extension* (e.g. Jane-Doe-HW-3.zip)
- Include your e-mail address in the Comment field when submitting the assignment through the Digital Drop Box
- If for any reason you are submitting the assignment more than once, indicate this in the Comment field by including the word COMPLEMENT

The purpose of this homework is to give you a chance to better understand encryption.

Here is what you have to do:

- Download and install FOSS symmetric encryption software, such as [aescrypt](#).
- Download a story from the [Gutenberg Project](#). For purposes of this project you should download a plain text story that has at least 500,000 characters.
- Measure the letter frequency in the plain text.
- Encrypt the story using the software you just downloaded. If the software you're using may output the cyphertext in both binary and ascii formats, then choose ascii.
- Measure the letter frequency in the cyphertext.
- Measure the time it takes to encrypt your story. Make multiple measurements such that you have a statistically significant sample; include in your report the average, median and standard deviation of your measurements.
- Repeat the previous three bullet points using GnuPG, the software you installed on your computer for HW#2.
- Create a report that includes your findings and comments on those findings. Don't forget to mention relevant statistics about the story you've used in your work, a link to the story you've used, the name and version of the encryption software, the operating system you're using, a description of how you measured the letter frequency, etc. Don't forget to compare and contrast the running times between the two encryption softwares.

$Id: hw3.html,v 1.2 2008/09/08 00:15:38 virgil Exp $