Codebreaker Challenge

The following outlines the technical Environment that will help a student solve the problem. Additional information and updates will be provided as we get closer to attending the briefing(s).

- VMWare or VirtualBox with either a Linux or Windows VM (XP or greater), which has the following software items loaded:
  - Cygwin (if analysis and development is performed on Windows)
  - gcc version 4.5 or higher (Cygwin or Linux)
  - openssl and/or CyaSSL libraries (Cygwin or Linux)
  - The demo version of IdaPro 6.8 or higher (https://www.hex-rays.com/products/ida/support/download_demo.shtml)

    Please note, as a demo version there are usage limitations that include a limited number of analysis operations that can be performed. For example, if a student is performing a substantial number of debug code stepping they may reach this limit fairly quickly.
  - Python 2.6.* or higher, with OpenSSL and/or CyaSSL available (helpful if students want to prototype)
- We have prepared a Windows 7 VM that has a temporary usage license to help those that do not have access to their own virtual machine. However, please note there are limitations to this VM.
  - VM Link: https://drive.google.com/folderview?id=0BzhRtDqsJu_MUmhJZDFvMmxkVms&usp=sharing
  - We added some tools to this VM:
    - Please note, we added openssl (binary) to Cygwin. However, we accidently omitted the libraries to support gcc programming. Therefore, the students will need to use the Cygwin loader and add the openssl complete library.
    - Open the preinstalled Google Chrome
    - Navigate Chrome to its “Downloads” section. You should see “setup-x86.exe” for Cygwin.
    - Run setup-x86.exe
    - In the set up:
    - Select “Next”
    - “Install from Internet”
    - Select “Next” on the next 4 configuration screens to select the current values (defaults)
    - In the search window, type “openssl”
    - Install “Debug”, “Devel”, “Net” and “Python”
    - Select “Next”
    - Etc..
- It is possible to forgo the virtual machine and use a base platform (linux or windows). Even though the codebreaker challenge binary is not malware, it could possess behavior that might be aggressively identified and removed by a virus scanner implementing a heuristic engine. This can be averted by either performing the analysis in a virtual machine or temporarily shutting down the virus scanner (not the optimal choice).