EN650.658 Lab Assignment 1 - Pseudo Random Number Generation

In this lab, you will apply your knowledge learnt in class to find out some interesting facts and do some experiments on crypto programming. You need to complete all the five tasks in this lab and submit a detailed lab report, with screenshots, to describe what you have done and what you have observed. You also need to provide explanation to the observations that are interesting or surprising.
Please also list the important code snippets followed by explanation. Simply attaching code without any explanation will receive no credits. And you may complete this lab with a group up to 3 people.

The lab is one of the exercises in SEED Project. It provides a Virtual Machine (VM) image in order to simplify setups of experimental environment. We are using the Ubuntu 16.04 image for this lab. Load the VM image with your VirtualBox or VMware (whichever you prefer). Please read the User Manual carefully before you start working on the labs.

Additional Instructions

The lab manual has step-by-step walkthrough and detailed instructions. Please carefully read the following tips and notes:

- The VM image is an archive of vmdk files. VirtualBox users can follow the instruction in the User Manual to import those files. For VMware user, please refer to this video for lab setup.
- In Task 2, you need to implement an AES-128-CBC program to perform encryption. Python is recommended here since you may use libraries like *Crypto, pycrypto* or *cryptography* to simplify the task. However, it is also acceptable to use any other languages. Just remember to attach the code with enough explanation.
- The plaintext, ciphertext and IV provided in Task 2, together with the key you generate in Task 1, are all hexadecimal codes. Conversion may be applied to handle them in your program.
- The question at the end of Task 4 is a bonus question, and you may receive extra credits (up to 5 points) for this question.
- The 256-bit key in the last step of is supposed to be a binary string (sequence of 0s and 1s of length 256).
- Take screenshots periodically and include it in your report. They not only serve as evidences of completion but also help grader understand what you're trying to achieve.
- Attach your code with explanation for each task in your report to receive full credits.

Points Breakdown

This lab has 40 points in total. Task 1 through Task 5 are worth 5, 15, 5, 5, 10 points respectively.