ECE590 Enterprise Storage Architecture
Individual Homework #4: Security

Directions:

- This assignment will be completed in ***INDIVIDUALLY***. While you can discuss concepts with others both within and outside your group, actual steps and answers should not be shared!
- The solutions should be collected in a file called `ece590-<netid>-hw4.pdf`, where <netid> is your Duke NetID (sans brackets!), and submitted via Sakai. *Word documents will not be accepted*.
- *NOTE: The lab has most of the content this time, so this homework is very short.*

1 Security [30 pts]

(a) What are the inputs and outputs of a symmetric cipher? What are the inputs and outputs of an asymmetric cipher? [4pts]
Note: if you're also in my security class, you may recycle your answer from that course's Homework 1

(b) Explain the difference between "in flight" and "at rest" data encryption. What attacks can each approach mitigate? [10pts]

(c) The scenario in Homework 3's Question 2(b) describes a backup script which violates a basic tenet of security. What is it? [8pts]
(HINT: what should you never do with a password?)

(d) In Linux/UNIX, give the command(s) that would set up permissions in each of the following scenarios. For each, make *only* the change prescribed; don't change permissions/settings that aren't mentioned.

i. The "code" directory should be owned by the "developer" group, and its contents be modifiable by any member of that group. [2pt]

ii. The file "secret.txt" should be readable/writable *only* by the file's owner. [2pt]

iii. The file "do_stuff" is a script, so make it executable by anyone. [2pt]

iv. You're a hacker with root access and you're setting up a "back door" to allow unprivileged users to gain root access in the future. Set permissions on the file "innocent.sh" so that it runs as the root user. [2pt]