CS558 Assignment 4
Due: 11:59pm June 28 (Sunday)

This assignment is done individually.

Choice I: Password management (10 points extra credit)

In this assignment, you need to write two programs: genpass and verifypass (you can give different names).

genpass is used to generate a file ***password*** which has the following format:

<user ID> <encrypted password>

where <encrypted password> is computed by encrypting the password using a key and a symmetric encryption algorithm (e.g. AES, 3-DES). **You can either hardcode the key in your program, or randomly generate a key and save the key in a file. You can use the existing implementation of 3-DES, or AES (e.g. the implementation provided in java.security, openssl, etc.) in this assignment**.

When genpass is invoked, it prompts the person who invokes genpass to enter each user's ID and password. Your program then encrypts the password using the key, and saves the ID and the encrypted password in a file password. You can assume that the ID entered each time is different (i.e. your program does not need to check whether the ID is already in the file).

verifypass is used to verify the ID and the password of a user. When verifypass is invoked, it prompts the user to enter his/her ID and password. If the ID does not exist in file password, then print "ID does not exist". Otherwise, your program will retrieve the encrypted password ep of the user from file password. Your program then decrypt the password ep and compare the password entered by the user against the decrypted password. If they are the same, then print "the password is correct"; otherwise print "the password is incorrect".

Submission guideline:

- Create a directory with a unique name (e.g. p4-[userid]), which contains the source code, the key (if the key is saved in a file), and a README file.
- **README** file (text file, please do not submit a .doc file) contains
  - Your name and email address.
  - Whether your code was tested on bingsuns or remote.cs.
  - How to compile and execute your program.
  - (Optional) Briefly describe your algorithm or anything special about your submission that the TA should take note of.
- Tar the contents of this directory using the following command.

  tar –cvf p4-[userid].tar p4-[userid]

  E.g. tar -cvf p4-pyang.tar p4-pyang/
- Upload the tared file you create above to mycourses.

Choice II: Rootkit (10 points extra credit)

Download a rootkit that enables attackers to hide files and processes, and demonstrate how to do it. You will need to first install a **virtual machine** (e.g. virtualbox) and then download and execute the rootkit inside the virtual machine.

The following link may be helpful: https://github.com/topics/rootkit.

Submission guideline:

Please record a video that shows how to use PGP to provide confidentiality and digital signature, upload the video to google drive, and email me (pyang@binghamton.edu) a link to the video.

Choice III: Scam Websites

Using google to search for "tennis rebound net", "trampoline", "lego mind storm", or other popular expensive items, identify at least three websites that are scam websites, and explain why they are scam websites.

Submission guideline:

You need to hand in your assignment through mycourses.binghamton.edu, which contains: 1) Your name and email address; and 2) Solution to the problems. Your assignment must be in **.pdf** format.