Homework1

Cryptography and Network Security (2019 Spring)

Introduction

- 3 handwriting problems and 6 programming problems.
    - For programming problem, any programming language is acceptable.
- Topic includes: Lecture2 (3/5) ~ Lecture5 (3/26)
    - Security requirements, basic cryptography knowledges, hash functions, D-H key agreement, authentication, digital signature and other related topics.

Submission Guidelines

- Submit your homework to CEIBA.
- You need to put all of them in **a single folder** named by your student ID, and then **zip** them before upload to CEIBA.
- For example: **hw1_r07922xxx.zip.**

Submission Guidelines

- The folder should include all the contents listed below.
  - Your report, including:
    - your **answers** for handwriting problems.
    - your **write-up** for programming problems to explain how you solve them, also **the flag** for each problem if required.
  - Your codes for programming problems if required.
  - A **readme.txt** file to provide a brief usage of your code. (e.g., how to compile, if needed, and execute)
    - You may lose points if TAs can't run your code.

Submission Guidelines

- For example, the file layout in your folder should look like this:
    - report.pdf
    - code{X}.py
    - code{Y}.c / .cpp
    - …
    - readme.txt
    - (other required files.)

Submission Guidelines

- **Submission deadline: 2019/4/7 23:59 (about 3 weeks)**
- Late penalty: 10% penalty per day, up to 2 days. You will not receive any credit if delayed for more than 48 hours.

Collaboration policy

- Discussion is encouraged, but you must acknowledge.
- **You must write your own answer and code.** Violation of this policy will lead to serious consequence.

Others

- You may encounter new concepts that haven't been taught in class, and thus you're encouraged to discuss with your classmates, search online (Google is your friend!), ask TAs, etc.
- The challenge server only allow connections from 140.112.0.0/16, 140.118.0.0/16 and 140.122.0.0/16. VPN is your friend.

TA Hours

- 毛偉倫
  - 星期二 1100 - 1200，資307
- 江緯璿
  - 星期三 1030 - 1130，資217
- 蕭乙蓁
  - 星期二 1720 - 1820，資217

TA Hour Location may change, please refer to ceiba.

Email: cns@csie.ntu.edu.tw
Subject: [CNS]HW1_{X} eg: [CNS]HW1_10

Recommended Tools

Linux command -- nc

- $ nc [server-ip] [port]

pwntools - installation

```
apt-get update
apt-get install python2.7 python-pip python-dev git libssl-dev libffi-dev build-essential
pip install --upgrade pip
pip install --upgrade pwntools
```

Example code

```
from pwn import *

r=remote(“140.112.31.96”,10150)

print r.recv()

r.send(“HAHA”)

r.interactive()
```

Reference

https://pwntools.readthedocs.io/en/stable/tubes.html

Q & A

- **Any questions?**

END

- **Start your homework early.**
  - **Or you will GG.**