Homework 3

due by 11:59pm **on Nov 11**
Course: CS6111, Jul-Nov 2023
Instructor: Aishwarya Thiruvengadam
Teaching Assistant: Pallavi Borkar

Instructions:

1. For connecting to the binary programs, utilize the `pwn` python library and the functions: `remote, recvuntil, sendline, process`. Using these functions, you can connect to a remote or a local process.

2. Files for submission:
   - Python3 exploit script(s) (Filename format: ⟨*rollnumber_questionnumber.py*⟩)
   - Report PDF made using LaTeX(Filename format: ⟨*roll_number.pdf*⟩). It should consist of:
     – Explanations for (programming) questions 1 and 2.
     – Answers to (theoretical) questions 3, 4 and 5.

3. Any library functions (apart from those mentioned in instruction 1) should be explained in detail in the submitted report.

4. No collaboration is permitted on any of the questions for this homework.

5. Students connecting from outside IITM network should install `Zerotier` and send a request to network-id *3efa5cb78aa7d383*. The netcat IP for these students will be **192.168.194.160**. The port number remains the same.

Questions:

1. In Greek mythology, the priestess of the Temple of Apollo at Delphi was consulted on any major decisions. She came to be known as Delphi's Oracle. CS6111's very own Delphi has developed a binary program that can be accessed at **nc 10.21.236.75 8082**. It accepts an encrypted cookie and displays a user-specific password only if your cookie is accurate. Exploit a bug in the program to mount an attack and extract this password.

   The script `cookie_1.py` provides the source code of this binary program. You must submit the exploit script and your extracted password. Provide an explanation of the exploit script, screenshots of the password extraction, and the password in your report.

2. A modified version of Delphi's program can be accessed at **nc 10.21.236.75 5055**. Can you mount an attack on this program? If you can, submit the exploit script and your extracted password. Also, provide an explanation of the exploit script, screenshots of the password extraction, and the password in your report.

3. Consider an execution of Diffie-Hellman key exchange protocol in the group $\mathbb{Z}_{17}^*$ with generator 3 where Alice chooses exponent $x = 9$ and Bob chooses exponent $y = 3$.
   - What is the message that Alice sends to Bob?

- What is the message that Bob sends to Alice?
- Compute the key that Alice and Bob each derive and verify that they are equal.

4. Is the El Gamal encryption scheme CCA-secure? Prove or disprove your answer.

5. Answer the following questions with regard to the group $\mathbb{Z}_{55}^*$.

   - How many elements are in this group?
   - Define $f_3 : \mathbb{Z}_{55}^* \to \mathbb{Z}_{55}^*$ by $f_3(x) = [x^3 \mod 55]$. Compute $f_3(6)$.
   - What function computes the inverse of f_3?
   - Find x such that $f_3(x) = 2$.