ENEE459B: Reverse Engineering Lab
Project #1: Algorithms

Overview
You are working at a company called '**OurCompany**.' Your supervisor has come to you because he heard you took a class on Reverse Engineering.

Apparently, they found some **anomalous outbound traffic** on the network late at night. They ran **Wireshark** to capture the traffic and found **TCP connections** that **contained binary blobs** being sent to an **IP address** in an eastern European country. When they examined the machine where the traffic was coming from, **they found a binary running**. They have provided you with:

- A copy of the binary
- The payloads of a few of the binary blobs they saw
    - By payload, I mean the contents of the socket connection with all the TCP/IP information stripped (In other words, the content passed to socket APIs such as send() and recv()).

"TheBoss" wants to know what is going on. What was this program doing? What information is in these binary blobs that appear to be random data with no patterns/signatures?

Assignment
You have been provided with the files '**binary**', '**bin1**', '**bin2**', and '**bin3**.'
The '**binary**' file is the **executable**. The **other bin files** were pulled from Wireshark and **are the payloads of the communication that was viewed**.

Tasks
Please answer the following questions/perform the following tasks:

1. (**5 pts**) Use your knowledge of ELF files and provide what shared objects this binary imports (i.e., **what external libraries** are used?)
2. (**5 pts**) Examine the binary and determine how the binary blobs are being sent – what internet address are they being sent to?
3. (**10 pts**) How are the binary blobs being created?
    a. What format, if any, are they in?
    b. What is the algorithm being used to create them?
    c. What are the inputs used in the identified algorithm?
4. (**20 pts**) Write a C program that can decode these binary blobs
    a. Provide your C code with instructions on how to compile/use it – ***make sure it works on the class VMs***
    b. Provide the information that you have decoded from the binary blobs – What is it?
5. (**10 pts**) How does the program gather the data to put into the binary blobs? What mechanism is used? Are there any signatures you can look for to detect this on other hosts on your network?

Turn In
- A written report detailing all findings with the answers for the tasks – Be as complete as possible. Please use screenshots to describe important code sections.
- For Task 4, the C program that decodes the binary blobs (it should work on the class VMs).

Important

- The algorithm you find must be implemented in C! You may not use ‘system,’ ‘exec,’ or other such functions to call command line/shell utilities or pass scripting commands to various parsers.
- Please include **screenshots**/**documentation** to back up your findings.

Tips

- Don’t be afraid to start in the middle and work backwards
- Use your needle-in-the-haystack techniques to find the places of most interest in the binary
- Remember your goal – you likely do not need to understand every function to finish this assignment
- Make sure you use the ‘man’ command on any library functions you don’t recognize
    - Make sure to use ‘Google’ if you still aren’t sure
- Don’t be afraid to write small C programs (or even Python scripts if you are more comfortable, but the code you turn in MUST be C) to crunch the data you find
- Give me as much information about your thought processes as you can, especially if you are stuck – I can’t give partial credit unless I can see what you are thinking