Homework 1

In total: 30 points

1. (4 pts) How would you test a piece of ciphertext to determine quickly if it was likely the result of a simple substitution?

2. (4 pts) We assume that a household computer has a 2GHZ processor. Also we assume that a machine takes a hundred cycles per brute force (to check one possible key) against either single 56-bit DES key or 128 bit AES key. Estimate the amount of time necessary to crack a DES encryption by testing all 2^{56} possible keys. Make a similar estimate for a 128-bit AES key.

3. Bonus point (5 pts) Vignere Cipher Programming: Use Java, Python or C++ to implement the Vignere cipher.
   Your program will take in 2 inputs from the command line: 1) the key and 2) the string to encrypt. Output will be the ciphertext, and the result of decrypting the ciphertext (should be the same as input 2).
   Requirement: The key should contain English letter only (no white space or other symbols); The plaintext string should at least include English letters and white space. If you would like to include other characters in the plaintext and ciphertext, it is also fine. It is not required to distinguish capital letters and lower-case letters. If students only treat capital letters or lower-case letters, it is perfectly fine.
   Deliverable: a) program source code, b) screen shot of the result of running your program.

SEED Lab

Setup

Option 1. (local copy)
1.a Setup the environment of SEED Lab following the steps on
https://seedsecuritylabs.org/lab_env.html.
1.b Read the User Manual of the Virtual machine:
https://seedsecuritylabs.org/Labs_16.04/Documents/SEEDVM_VirtualBoxManual.pdf
Option 2. (cloud)
E.g., Microsoft Azure free credits for CPP accounts. Follow instructions at
https://github.com/seed-labs/seed-labs/blob/master/manuals/cloud/seedvm-cloud.md
Note: if connecting to the cloud server with the SSH key fails, you can choose to use password for the user instead when creating the VM.

Secret Key Encryption

4. (22 pts) Complete Task 1; Task 2; Task 3, Task 5; Task 7 in the lab description:
   https://seedsecuritylabs.org/Labs_16.04/PDF/Crypto_Encryption.pdf

The files needed can be found at
https://seedsecuritylabs.org/Labs_16.04/Crypto/Crypto_Encryption/

Deliverables on Canvas

1. A file including answers to questions 1 and 2.
2. (optional) The screen shot of the result of running your program for Bonus question 3. Source code files of Question 3 (Vignere cipher).
3. A detailed SEED lab report with screenshots, to describe what you have done and what you have observed. You also need to provide explanation to the observations that are interesting or surprising.
4. For the lab, please also turn in the source codes (if any) for each task with appropriate comments.