CRYPTOGRAPHY MISSION 05 DOSSIER

Deadline: Thursday, 6 October 2016 at 3:05pm

This mission covers Sections 3.4, 3.6, and current issues.

Check one:

□ I received help from the following classmate(s) on this assignment:

____.

□ I did not receive any help on this assignment.

1. Graded Problems

1. (Fermat's Little Theorem and Euler's Theorem) Compute each of the following without the aid of a calculator or computer (you can double-check with some code though).

   a. $\varphi(35)$

   b. $514^{372} \mod 13$

   c. $12^{49} \mod 15$

2. (Chinese Remainder Theorem) A band of 17 pirates stole a sack of gold coins. When they tried to divide the fortune into equal portions, 3 coins remained. In the ensuing brawl over who should get the extra coins, one pirate was killed. The coins were redistributed, but this time an equal division left 10 coins. Again they fought about who should get the remaining coins and another pirate was killed. Now, fortunately, the coins could be divided evenly among the surviving 15 pirates. What was the fewest number of coins that could have been in the sack?

3. This problem will prepare you for the in-class Current Issues Debate on October 6th. **There is no write-up due for this problem, but you probably want to prepare some written notes for the in-class discussion.**

   a. You and your group are assigned a person who is invested in the topics of encryption and privacy (see next page). First, learn about this person, and, as a group, prepare a short 2-minute talk on this person's background in relation to encryption/privacy. I would recommend starting on Wikipedia. Nominate a person from your group to be the designated speaker.

   b. I will provide some relevant reading material for your character and some key words you must be familiar with (see next page). Keep in mind some of these words aren't familiar to everyone, so you might want to define them in your 2 minute intro. You might or might not personally agree with your character, but your goal for the class discussion is to bring in a fair representation of what this person would think. There might be some uncomfortable topics that come up, but they are issues that are worth discussing. Learn to be comfortable with talking about uncomfortable topics.

   c. As a group, prepare some tentative answers on the following questions, which we will debate in class. A good way to answer these is to come up with a short answer and then an example or scenario to justify your answer.
      - Who, if anyone, should have control over encryption? (Related question: who should have control over what information remains private?)
      - What level of control should a person, organization, or other entity have over encryption?
      - What does misuse of data collection mean? Is collecting information against privacy protections of the US constitute a misuse, or does it have to include actual harm to a specific person or organization?

   d. The following questions might come up based on the characters in the discussion. Read over them, and think about how your character might respond as well as how you might personally respond.

      - (Snowden) Is mass surveillance ever acceptable?
      - (Gamergate) Should online harassment count as a true threat (which is prosecutable under criminal law)?
      - (Apple vs. the FBI) Before the FBI withdrew its request, should Apple have complied with the FBI after the San Bernardino attack?
      - (WikiLeaks and Ashley Madison hack) Is it okay to expose information during a morally questionable situation?

4. Skim the last page to see who else is showing up (no need to read all the articles except for your character).

2. Characters

1. Tim Cook - Chief Executive Officer of Apple
    - Recommended Reading on Apple vs. FBI
    - Key Words: San Bernardino, backdoor, All Writs Act, privacy
2. James Comey - Director of the FBI
    - Recommended Reading on Apple vs. FBI
    - Key Words: San Bernardino, backdoor, All Writs Act, privacy
3. Richard Clarke - former National Coordinator for Security, Infrastructure Protection and Counter-terrorism for the US
    - Recommended NPR Article
    - PEW Research on Privacy vs. Security
    - Key Words: San Bernardino, counterterorrism, privacy
4. Edward Snowden - former NSA and CIA employee who leaked NSA documents to journalists
    - Recommended Reading on Snowden and the Leaked NSA Files
    - Key Words: NSA leak, mass surveillance, privacy
5. Zoë Quinn - video game developer and victim during the Gamergate controversy
    - Recommended Reading on Gamergate
    - Key Words: Gamergate, doxing, privacy, journalistic ethics
6. "Tom," a victim of the Ashley Madison hack - Ashley Madison is an online dating service for people who want to have an affair
    - Recommended Reading on the aftermath of the Ashley Madison hack
    - Key Words: Ashley Madison, data breach, internet vigilantes, hacking
7. Julian Assange - hacker and editor-in-chief for WikiLeaks
    - Recommended Reading WikiLeaks
    - Key Words: WikiLeaks, hacking, journalistic ethics, internet vigilantes
8. Jane - registered voter in the US, iPhone owner, and lover of memes
    - Recommended Summary on Clinton vs. Trump policies on Cybersecurity
    - Key Words: hacking, privacy, DNC hack, "the cyber"

3. Recommended Exercises

These will not be graded but are recommended if you need more practice.

- Section 3.13: # 9, 10, 12, 15, 20
- Section 3.14: # 6, 10