Introduction to CryptographyProblem Set 1

Name: Student Name
Collaborators: Collaborators

By turning in this assignment, I agree to abide by and uphold the Honor System of Introduction to Cryptography as well as the additional policies outlined on the course website.

Transparency Note: This homework structure is modeled off of David Wu's Advanced Topics in Cryptography course. Long Answer Question 2 is taken from the text book and credit should go to Dan Boneh and Victor Shoup.

True or False (3 points each)

1. True or False: Intuition is sufficient for determining whether a cryptographic cipher is secure. Why?
2. True or False: It is important to "roll your own" (write your own) encryption. Why?

Short Answer (5 points each)

1. Does the one time pad meet the Shannon Cipher correctness requirement? Why or Why not? Please include both a mathematical explanation and an example using "real" numbers.
2. Why can you not use a one time pad more than once? Please explain a successful attack mathematically and include an example using "real" data.
3. What is the difference between a Pseudo Random Generator (PRG), Pseudo Random Function (PRF), and Pseudo Random Permutation (PRP)? When would you use each?
4. Please describe how to use a PRF to construct a MAC.
5. I have encrypted a message using a cipher we have discussed in class with a 3 character key. Decode the message and key! Please describe your attack.

nGmni akr bogpitr Fmeorcbi usxfyyr uiw

Long Answer (10 points each)

1. How does the Electronic Code Book (ECB) encryption system work? What is Chosen Plaintext Attack (CPA) security? Describe an attack game that breaks the CPA security of an ECB system (diagrams optional, but recommended).
2. A proposed system of voting would work as follows. Given t voters, a central tallying center samples a number $n_0 \xleftarrow{R} \{0, 1, 2, ..., t + 10\}$ and sends that number to voter 1. Voter 1 then adds their vote $v \leftarrow \{0, 1\}$ to the tally $n_1 \leftarrow n_0 + v$ and passes the new total to voter 2. This continues until the final voter hands back the vote to the central tallying center which

then determines who won by subtracting out the original random number they chose and determining if the vote sum is greater than or equal to half of the voters. Does this system meet the Shannon Cipher correctness property? Describe an attack that would allow two voters to collude to determine the vote of a third voter.

3. Describe an example of symmetric key cryptography being used and succesfully broken through an attack in the real world. What were the cryptographic ciphers used? What was the mechanism of attack? What were the repercussions of this attack? Bonus point: walk through an example of the attack using real world data.

Feedback (optional) (0 points each)

1. What was the hardest problem on this problem set?
2. What was your favorite problem on the problem set?
3. How long did you spend on this problem set?
4. Do you have any feedback for how I can improve either this homework set or the course in general?