601.445/601.645: Practical Cryptographic Systems January 27, 2020

Weekly Homework 1

Instructor: Matthew Green *Due: 11:59pm, February 3*

Name: _____

The assignment should be completed individually. You are permitted to use the Internet and any printed references.

Please submit the completed assignment via Blackboard.

Problem 1: Suppose we are told that the Vigenere ciphertext `CCWEKHBSJIR` decrypts to `CHICKENSOUP`. Determine the cipher key.

Problem 2: The following ciphertext has been encrypted using the Permutation Cipher. See `https://www.nku.edu/~christensen/1402%20permutation%20ciphers.pdf` for a description of the cipher.

```
HESWAOLGLOTTONHDENEWASHELGFILH
FINTRENCAWASHELGFILHTONTHASEES
ONDACSANEWASHELGFILHTWITHWROGI
OGCNNEIDFNNEACDWROGITGSNRTNGEH
HNTIEWIRAELHASLEEFDNROUDINLASD
     THAWETERVHSCOETBAYME
```

Find the permutation key and describe what techniques you used.

Problem 3: Answer the following questions:

1. Describe (in your own words) what the *Index of Coincidence* is.
2. What is the IoC value for uniformly random text, assuming a standard 26-letter alphabet. Explain why.
3. Take two piece of (relatively long) English-language text and calculate the IoC value for those texts. You should feel free to use an online app for this. List the texts you used.
4. Give two vulnerabilities with the Permutation Cipher.
5. Explain what happens to the security of a cryptosystem if one combines two ciphers by first encrypting with one and then "super-encrypting" the resulting ciphertext with the other. For this specific example, consider the Vigenere cipher and the substitution cipher. Does this make the system more difficult to attack?

6. Give an argument for why the Vigenere cipher is unbreakable *if we assume a perfectly random key*, that's as long as the message and used only one time.

7. Give an argument for why your argument above (in the general setting) does not hold if the key is re-used to encrypt multiple messages.