Homework 1 - ENEE 456 / CMSC 456 / MATH 456 - S21

Out 1/29/21; Due: 2/5/21 11:59 pm

Problem 1

(3%) You are given a ciphertext ctext.txt encrypted with the code vigenere-enc.c. Decrypt the ciphertext without having access to the secret key. Submit both the decrypted plaintext and any code you wrote to solve this problem.

Problem 2

(3%) Alice and Bob shared an n-bit secret key some time ago. Now they are no longer sure they still have the same key. Thus, they use the following method to communicate with each other over an insecure channel to verify that the key k_a held by Alice is the same as the key k_b held by Bob. Their goal is to prevent an attacker from learning the secret key.

1. Alice generates a random n-bit value r.
2. Alice computes $x = k_a \oplus r$, and sends x to Bob.
3. Bob computes $y = k_b \oplus x$ and sends y to Alice.
4. Alice compares r and y. If $r = y$, she concludes that $k_a = k_b$, that is, she and Bob have indeed the same secret key.

Show how an attacker eavesdropping on the channel can gain possession of the shared secret key. Also show how an attacker who can do more than eavesdropping can make Alice and Bob believe they do not share the same key.