CS 355, Fall, 2019, Homework 5

1. Chuck uses RSA and accidentally revealed the Euler phi function of his public modulus. His modulus is $n = 4386607$ and he revealed $\phi(n) = 4382136$. Solve a quadratic equation to find the prime factors of n.

2. Alice uses $n = 2581$ and $e_A = 107$ for her public RSA key. How would Bob encipher $M = 1619$ to send to Alice? Decipher the cipher text $C = 1674$, which Chuck sent to Alice.

3. Alice and Bob use a toy version of the Diffie-Hellman key exchange protocol with common prime modulus $p = 11$ and common base $a = 2$. An eavesdropper who knew p and a noted that the number Alice sent to Bob was $y_A = 9$ and the number Bob sent to Alice was $y_B = 3$.

a. What was Alice's secret random number x_A?

b. What was the common secret key K generated for Alice and Bob by the protocol?

4. Alice uses the Pohlig-Hellman cipher with prime modulus $p = 2591$ and enciphering exponent $e = 13$ to encipher her diary. She enciphers two-letter blocks as units. The largest possible block would be 2525, meaning `ZZ`, and this is less than p. Decipher the cipher text `1213 0902 0539 1208 1234 1103 1374`.

5. A toy version of the ElGamal cipher uses the public common modulus $p = 97$ and the primitive root $g = 5$. Alice participates in this ElGamal system and uses $e_A = 37$ as her secret key and $b_A = g^{e_A} \bmod p = 56$ as her public key. What is the cipher text when Bob enciphers $M = 82$ to send to Alice if he chooses $k = 75$ for the random number? Show how Alice would decipher the cipher text $(7, 84)$, which she received from Chuck.

6. Your friend has a secret file you would like to read. The file contains ordinary text in English. However, you cannot read it because it is enciphered with a Vernam cipher. Each ciphertext byte is the **exclusive or** of a plaintext byte and a key byte. You have made a copy of the entire ciphertext.

One day your friend remarks that the "T" key on his keyboard sticks so that sometimes he types "TT" by mistake when he means "T". He says that this happened once when he was typing the plaintext of his secret file and that he has just corrected this typo. You suspect that he re-enciphered the file with the same key stream. You make a new copy of the entire ciphertext. Sure enough, it is one (1) byte shorter than the old copy. When you compare

the old and new copies you find that the first nine (9) bytes are the same and that the two files differ after that.

How much of the secret file can you decipher? Explain exactly what you would do to decipher the part that you can decipher. Define notation for the characters in the plaintext and the two ciphertexts. Give explicit formulas and pseudocode for your answer. Don't say that anything is "obvious" or "computed similarly".