Assignment 1

1) You are given a ciphertext encrypted under Caesar cipher: "ibbiks eqbp nctt nwzkm ia awwv ia bpm acv zqama". Recover the key and the plaintext.

2) Ceasar cipher: suppose that Alice and Bob generates three keys and uses triple encryption. That is, they encrypt the message using the first key, then encrypt the result using the 2nd key, then encrypt the result again using the 3rd key using a Ceasar cipher. Is this secure? Show a way to break it.

3) Vigenere cipher: what if key length equals message length? Can you still break it? Why or why not?

4) Compute 3292213^41 mod 100. How many multiplications did you require? How many digits did the numbers (which you had to multiply) had? Try to make it as efficient as you can.

5) Compute Discrete log of y=6 with respect to base g = 5 and modulas N = 7.

6) (no need to submit): Read and understand notions of digital signatures, public key encryption, and key exchange. Understand the differences between these.

ddl: 12am, Thursday, Jun. 2 (BJT).

https://www.cs.cmu.edu/~goyal/handouts/

Professor Email: Vipul@cmu.edu