Assignment question

1. This question is about the third generation of fully homomorphic encryption scheme GSW. This is a FHE from Learning with Errors which is conceptually simpler, asymptotically faster and attribute based.
   Suppose we have a ciphertext C is a $N \times N$ matrix. The secret key v is a N-dimensional vector. We say C encrypts μ when $C \cdot v = \mu \cdot v + e \ mod \ q$ where e is a small error vector and q is some modulus.
   a. If we use $C \cdot v = \mu \cdot v \ mod \ q$, it's already homomorphic, why are we still using $C \cdot v = \mu \cdot v + e \ mod \ q$? Try to explain in two to three sentences.
      By adding the error, it is one-wayness that it is hard to decrypt.
   b. Given that e is a small error vector, what range should e be in?
      0<e<<q
   c. Let $C_1 \cdot v = \mu_1 \cdot v + e_1 \ mod \ q$, and $C_2 \cdot v = \mu_2 \cdot v + e_2 \ mod \ q$
      Calculate the new error of $C_1 + C_2$
      $e_1 + e_2$
      Calculate the new error of $C_1 \times C_2$
      $\mu_2 \cdot e_1 + C_1 \cdot e_2$
      Will addition or multiplication make the error grow faster?
      multiplication
2. Before moving on to Q3, let's take a short review on Diffie-Hellman Key Exchange. Suppose that Alice and Bob are trying to simulate DHKE. Show your steps on how to calculate the shared key.
   p = 97, g = 5
   Alice: a = 9
   Bob: b = 11

   $$A = g^a \ mod \ p = 5^9 \ mod \ 97 = 30$$

   $$B = g^b \ mod \ p = 5^{11} \ mod \ 97 = 71$$

   $$k = A^b \ mod \ p = B^a \ mod \ p = 28$$

3. Take a look at the dhke.py. Here's a message that's encrypted by Alice using DHKE. Use the provided information in the file to decrypt the message. Paste the decrypted message below:
   I LOVE CSC427! The Encryption Overview Presentation is the best presentation I have ever had! :)