Homework 26, due November 4

(1) Alice and Bob perform a Diffie–Hellman key exchange with prime 257. They decide to ignore whether α is a primitive root, and choose $\alpha = 2$ to get a key 2^{xy}, where x and y are Alice and Bob's secret exponents. Show that if xy is divisible by 8, then the key is either 1 or 256. For randomly chosen x, y, how often does this happen? (Consider the possible $x \pmod 8$ and $y \pmod 8$.) Why does this mean that the choice of α is bad?

(2) Alice and Bob use the ElGamal cryptosystem with $p = 62501$ and $\alpha = 2$. Bob tells Alice that $\beta = 236$. Use the Pohlig-Hellman algorithm to compute Bob's secret exponent a. Next, Alice sends the ciphertext $(r, t) = (27629, 58211)$ to Bob. What is Alice's (numerical) message?

(3) Bob's ElGamal public key is $(p, \alpha, \beta) =$

`(33636257844372475419051207157963376040920028596 7967, 3, 1830).`

Alice encrypts two messages $M1$ and $M2$ and sends Bob the two messages

`(1094189891315123592 09, 108573740299231594393834269064425021470450637558918)`

`(109418989131512359209, 29527295775365383858696019846471267512874267294 0467)`

Eve intercepts the messages and knows that the first message $M1$ is "This is a test." Find $M2$.