Homework 18, due November 6

(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 $(p, \alpha, \beta) =$

`(336362578443724754190512071579633760409200285967967, 3, 1830).`

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

```
(109418989131512359209, 108573740299231594393834269064425021470450637558918)
(109418989131512359209, 295272957753653838586960198464712675128742672940467)
```

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

(4) Consider the following hash function. Let n be a large integer. Messages are in the form of a sequence of integers $(a_1, a_2, \ldots, a_s)$, where each a_i satisfies $0 \leq a_i < n$. The hash function h is computed as $a_1 + a_2 + \ldots + a_s \pmod n$. Which of the requirements for a good hash function from section 8.1 are satisfied by h? Explain.