Homework 22, due October 27

(1) (Page 215, problem 8) Suppose you have a random 500-digit prime p. Some people want to store passwords, written as numbers. If x is the password, then the number $2^x \pmod p$ is stored in a file. When y is given as a password, the number $2^y \pmod p$ is compared with the entry for the user in the file. Suppose someone gains access to the file. Why is it hard to deduce the passwords? If instead p is chosen to be a five digit prime, why would the system not be secure?

(2) (Page 216, problem 11) In the ElGamal cryptosystem, Alice and Bob use $p = 17$ and $\alpha = 3$. Bob chooses his secret to be $x = 6$, so $\beta = 15$. Alice sends the ciphertext $(r, t) = (7, 6)$. Determine the plaintext m.

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

```
(33636257844372475419051207157963376040920028596796 7, 3,
252172251173416638407402028835377804202962741957008).
```

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

```
(30006052676088333922826892740779197199430245307595 6,
26124423472146993421032642157936494851820526624043 5)
(30006052676088333922826892740779197199430245307595 6,
14264075092686472342158267753575310682878801114797 2)
```

Eve intercepts the messages and knows that the first message $M1$ is *thisisatest*. Find $M2$.