PMAT 4282 – Cryptography **Assignment #7**
Winter 2001

1. Show that the Diffie-Hellman Problem (DHP) and the El Gamal Problem (ELGAMAL) are computationally equivalent.

2. Suppose that Alice has published the key $(1237, 34, 383)$ for use in the El Gamal public-key cryptosystem.

   (a) You wish to send the message $m = 14$ to Alice. What do you actually transmit?

   (b) You have monitored the transmission $(94, 225)$ to Alice.

      i. Use the Index Calculus Method for solving the Discrete Log Problem to find Alice's secret key a.

      ii. What was the original message?

3. Prove that each of the following numbers is composite by finding a Fermat witness:

   (a) 123

   (b) 52687

   (c) 1263739430742009409841

4. Show that 52633 is composite and also that it has no Fermat witnesses.

5. For each of the following (a, p) pairs, determine whether $a \in QR_p$:

   (a) $(2, 17)$

   (b) $(44, 97)$

   (c) $(789, 5683)$

6. Let p be an odd prime. Prove that the equation $x^2 \equiv 1 \pmod{p}$ has exactly 2 solutions in $\mathbb{Z}_p^*$.