PMAT 4282 – Cryptography — Assignment #5
Winter 2008

Instructions

- Answer each question completely; justify your answers.
- This assignment is due at: 12:00 noon on Friday 27 February 2009.

1. Solve for x by using Shanks' Algorithm:
   (a) $14^x \equiv 519 \pmod{557}$
   (b) $7^x \equiv 922 \pmod{1433}$
2. Solve for x by using the Index Calculus Method:
   (a) $14^x \equiv 51 \pmod{557}$
   (b) $7^x \equiv 92 \pmod{1433}$
3. Show that the Diffie-Hellman Problem (DHP) and the El Gamal Problem (ELGAMAL) are computationally equivalent.
4. 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?
5. Prove that each of the following numbers is composite by finding a Fermat witness:
   (a) 123
   (b) 52687
   (c) 1263739430742009409841
6. Show that 52633 is composite and also that it has no Fermat witnesses.