PROF. SUNAR, ECE-673. SPRING 2014

ASSIGNMENT #1

ADVANCED CRYPTOGRAPHY

Due Date: February 11

1. Using a software package with big integer arithmetic support (e.g. Maple, Sage, Python/NumPy, C/GMP) develop a program to compute a discrete logarithm in Z_p^* using **Pollard's Rho method**. You may use the large number arithmetic functions including modular exponentiation, however you are (obviously) not allowed to use built-in discrete logarithm functions.

   Find the discrete logarithm $x = \log_\alpha \beta$ for

   (a) (40 bits) $p = 1933545007397$, $\alpha = 3$, and $\beta = 1046577355951$.

   (b) (60 bits) $p = 1223495743193500397$, $\alpha = 3$ and $\beta = 824260262947116620$,

   (c) (80 bits) $p = 1354408229903035206774829$, $\alpha = 17$, and $\beta = 812263064505936197143084$.

   (d) (100 bits)
   $p = 2408947440748783129141614766463$,
   $\alpha = 13237$, and
   $\beta = 660143456330023897106854342109$.

   (e) (120 bits)
   $p = 2397238908184939483393471607358782131$,
   $\alpha = 1337$, and
   $\beta = 1572038877384608709536972395832362653$.

   In your answer include your implementation. For each case indicate how much time was spent to complete the attack. Also indicate the platform information (MHz speed, memory, chip type, number of machines etc.).