Problem Set #3

Due Friday, February 14, 2025 @ 2:00 pm

1. Consider the Discrete Log Problem $9^x \equiv 15260 \mod 21599$

   (a) Use Shanks Babystep-Giantstep algorithm to solve the DLP.
   You can use the Mathematica notebook from November 20 last fall for the calculations.

   (b) How long are each of the lists formed by Shanks in this case?

2. Consider the same DLP in the first problem: $9^x \equiv 15260 \mod 21599$

   (a) Use Pollard's ρ algorithm to solve the DLP.

   (b) How many steps does Pollard's ρ use to solve this DLP?
   Compare to your answer from 1(b).

3. Use Pollard's ρ algorithm to solve the following DLPs, if possible.
   In each case, what is the expected value for the number of steps that Pollard's ρ will require?
   How many steps did your solution take (if you found the solution)?

   (a) $25^x \equiv 98035 \mod 137639$

   (b) $146702055^x \equiv 81868680 \mod 233280389$

   (c) $2^x \equiv 934323767785 \mod 3088621341347$

4. Decrypt the following message:

   If the prE sen ceOf ele ctR ic ityc an be made v I sib le I n a nypa rto fth ecircu it,I see n Or eas onw hy I ntel L igen ce M ayno t be tr a ns mi t te dIn st anta n eo usly b yele c tricit y-S amu el Finl eYBr eese Mor seB o rn1 79 1inC har l es town ,Ma Ss achu Set ts a n Dwasal soa pa int er asw ell

   You should turn in a one to two page writeup that explains your analysis that allowed you to find the plaintext or the different approaches you attempted if you were unable to break the cipher. In the latter case, your score for this problem will be based on the quality of your failure.