TCSS 543: Advanced Algorithms
Exam 1 Extra Credit
2/23/18
Aaron Devlin

N = # of runs of the check() function to compute the discrete logarithm, m, with Pollard's Rho Algorithm.

N = 100

1st set
p = (2^16) − 17, d = 154, n = 16339, and a = (12, 61833):
Average # of K steps to find m' = m for N random discrete logarithms: 180

2nd set
p = (2^18) − 5, d = 294, n = 65717, and a = (5, 261901):
Average # of K steps to find m' = m for N random discrete logarithms: 342

3rd set
p = (2^20) − 5, d = 47, n = 262643, and a = (3, 111745):
Average # of K steps to find m' = m for N random discrete logarithms: 676

4th set
p = (2^22) − 17, d = 314, n = 1049497, and a = (4, 85081):
Average # of K steps to find m' = m for N random discrete logarithms: 1318