Quiz 6

Student ID Number: Name _____
Math 173B, 1PM
Please justify all your answers March 5, 2020
Please also write your full name on the back

1. True or False?

   (a) Pollard's ρ algorithm generates two sequences of elements from a set of size N and finds a collision in $O(\log N)$ steps.

   (b) The Vigenère cipher is vulnerable to statistical analysis.

2. Alice offers to make the following bet with you. She will toss a fair coin 14 times. If exactly 7 heads come up, she will give you \$4; otherwise you must give her \$1. Would you take this bet? If so, and if you repeated the bet 10000 times, how much money would you expect to win or lose?

3. Using the Vigenère cipher, encrypt the message "HELLO WORLD" using the key "MATH."