Cryptographic Attacks Name:_____

1. What is it called when two hashes are the same?
    A. Mathematical Error
    B. Overflow
    C. Race Condition
    D. Collision

Answer: _____

2. What is the Birthday problem?
    A. Considers the probability that in a set of N randomly chosen people, two people will have the same birthday
    B. Considers the probability that in a set of N randomly chosen people, another person will share your birthday
    C. Considers the probability that in a set of N uniformly chosen people, two people will have the same birthday
    D. Considers the probability that in a set of N randomly chosen people, 50% of the people will have the same birthday

Answer: _____

3. How are passwords typically stored within a database?
    A. Hashed
    B. Encrypted
    C. Encoded
    D. In Binary Format

Answer: _____

4. How many characters long are MD5 hashes?
    A. 16
    B. 32
    C. 64
    D. 128

Answer: _____

5. What is a brute force attack?
    A. Physically breaking into a secure repository to steal information
    B. Attempting to randomly guess based on some probability what the right answer would be
    C. Trying all possible combinations and permutations until the right guess works
    D. Use a logarithmic algorithm to reduce the numbers of potential guesses before selecting from the options available

Answer: _____

6. Which hashing algorithm was first published in 1992 and had collisions verified in 1996?
    A. MD1
    B. MD3
    C. MD5

D. MD7

Answer: _____

7. One way to help strengthen a hashed password to _____.

A. Use multiple passwords
B. Salt the password
C. Save passwords in a file
D. Encrypt passwords

Answer: _____

8. A _____ attack is when a malicious actor is able to attack a system by using older version of software.

A. downgrade
B. prehistoric
C. pen and paper
D. precursory

Answer: _____