socrative

Name _____
Date _____

Chameleon hash functions

Score _____

1. Collision-resistant chameleon hash functions... (Multiple answers can be correct.)

(A) ...are collision-resistant for users that know the trapdoor.

(B) ...are collision-resistant for users that don't know the trapdoor.

(C) ...imply collision-resistant hash functions (existentially, i.e., if collision-resistant CHFs exist, then so do CRHFs).

(D) ...exist if the RSA assumption holds.

(E) ...exist if and only if the Discrete Logarithm assumption holds.

2. Random oracles are good chameleon hash functions.

(T) True

(F) False