socrative

Name _____
Date _____

Chameleon hashing and chameleon signatures

Score _____

1. Collision-resistant chameleon hash functions... (choose as many options as you think apply)

(A) ...can be constructed from the discrete logarithm assumption

(B) ...can be constructed from the RSA assumption

(C) ...can be constructed from any one-time signature scheme

(D) ...imply the existence of one-time, i.e., EUF-1-CMA secure signature schemes

(E) ...imply the existence of many-time, i.e., EUF-CMA secure signature schemes

2. In a chameleon signature scheme, an ordinary signature scheme is used to sign the hash value ch(m,r) for the message m to be signed, fresh randomness r, and the chameleon hash function ch supplied by the signer.

(T) True

(F) False

3. Why is a collision-resistant chameleon hash function necessarily randomized? More formally, why is it not possible to have a collision-resistant chameleon hash function with randomness space, say, R={0}?

4. If collision-resistant chameleon hash functions exist, then so do (deterministic but keyed, i.e., with a key generation algorithm) collision-resistant hash functions.

(T) True

(F) False