socrative

Name _____
Date _____

Programmable hash functions

Score _____

1. The PHF definition we have seen requires that with "decent" probability, a_{m_i}!=0 for m_1,...,m_w, but a_{m^*_j}=0 for m^*_1,...,m^*_v. Why can't we expect to have v and w both be large simultaneously?

2. A programmable hash function (with "sufficient" programmability parameters)... (choose as many options as you think are appropriate)

(A) ...is an algebraic tool that should help in enabling a security reduction.

(B) ...is collision-resistant if the DLog assumption holds in the underlying group.

(C) ...by definition requires a pairing.