socrative

Name _____
Date _____

Pairings

Score _____

1. Which of the following properties does a pairing e: G_1 x G_2 → G_T have? (Mark as many options as you think are correct.)

(A) Bilinearity

(B) Collision-resistance

(C) Non-degeneracy

2. How many evaluations of a pairing e: G x G → G_T does each party have to perform in Joux's 3-party key exchange protocol to compute a shared key?

3. (Requires knowledge about common cryptographic assumptions in cyclic groups.) Intuitively, a pairing allows one "multiplication in the exponent", at the cost of moving to another group G_T. Why is a pairing with G_1=G_2=G_t (and e(g,g)=g) probably not very useful?

In the lecture, we asked this question without the e(g,g) = g requirement. The answer for the case e(g,g) ≠ g stays the same, but requieres a more complex argument (see solution file).