socrative

Name _____
Date _____

RSA-based signatures 1

Score _____

1. The RSA assumption states that every PPT adversary A has at most negligible success in...

(A) ...given N and e, to compute d = e^{-1} mod phi(N)

(B) ...given N, e, and d, to compute phi(N)

(C) ...given N, e, and y (randomly chosen from Z_N), to compute x with x^e = y mod N

(D) ...given N, to compute the factors P and Q of N

2. Even if the RSA assumption holds, the textbook RSA scheme allows a PPT attacker...

(A) ...given pk, a random message m^*, and two signatures for self-chosen messages m_1,m_2 != m^* (that may depend on m^*), to compute a signature for m^*

(B) ...given pk, a random message m^*, and one signature for a self-chosen message m != m^* (that may depend on m^*), to compute a signature for m^*

(C) ...given pk, and a random message m^*, to compute a signature for m^*

(D) ...given only pk, to compute the corresponding secret key sk

(E) ...given only pk, to compute a signature for a self-chosen message m^*