socrative

Name _____
Date _____

Parameter choices

Score _____

1. The best known attack on the RSA encryption scheme consists of...

(A) ...guessing N uniformly

(B) ...guessing the factors P and Q of N uniformly

(C) ...factoring N using the general number field sieve

(D) ...factoring N using the special number field sieve

(E) ...factoring e using the special number field sieve

2. Time/success tradeoffs: which of the following statements are true?

(A) Every algorithm that succeeds with probability p>0 in time t can be turned into an algorithm that always succeeds and runs in expected time t/p.

(B) Every algorithm that always succeeds in time t can be turned into an algorithm that succeeds with probability p in time t*p for every p>0.

3. A small security loss in a cryptographic reduction is desirable because it...

(A) ...leads to better security guarantees than a reduction with a larger loss would

(B) ...gives more confidence in the underlying assumption (e.g., the RSA problem)

(C) ...leads to better parameter choices and more efficient cryptographic schemes

(D) ...implies security against quantum computers

4. Choosing RSA keys with primes P,Q of length about 128 bits can be considered secure.

(T) True

(F) False