socrative

Name _____
Date _____

RSA-based signatures 2

Score _____

1. The random oracle model is a heuristic in which...

✗ (A) ...the signature oracle is replaced by an oracle that returns random bitstrings

✗ (B) ...the signature oracle is replaced by an oracle that returns signatures for random bitstrings

✗ (C) ...the secret key is not chosen by the Gen algorithm, but chosen as a random bitstring

✓ (D) ...the hash function is replaced by an oracle that returns random bitstrings on all inputs

2. There are cryptographic constructions that can be proven secure (with a reduction to a computational assumption such as the RSA assumption) in the random oracle model and in the standard model.

✓ (T) True

✗ (F) False

3. If the RSA assumption holds, then the RSA-FDH signature scheme is...

EUF-CMA secure in the Random Oracle Model

4. The security proof of RSA-FDH uses that...

✓ (A) ...the success probability of an adversary A that never hashes the forgery message m^* is negligible

✗ (B) ...given a random sigma in Z_N, it is always possible to find a message m, such that sigma is a valid RSA-FDH signature for m

✓ (C) ...given a random sigma in Z_N, it is always possible to find a hash value y, such that sigma is a valid RSA-FDH signature for any message m with hash value H(m)=y

✓ (D) ...the reduction B can adaptively choose the hash values requested by A

✗ (E) ...the challenger C has to supply the random oracle for both B and A

5. In the random oracle model, the RSA-FDH signature scheme is XOR-homomorphic (in the sense that given two messages m_1,m_2 with signatures sigma_1,sigma_2, it is efficiently possible to compute a signature for m_1 XOR m_2).

✗ (T) True

✓ (F) False