

GHR signatures

1. The strong RSA assumption is at least as strong as the prime-e-RSA assumption. (Prime-e-RSA assumption: like RSA assumption, but with e chosen as prime between 2^n and $\phi(N)$.)

- T True
- F False

2. According to the current state of knowledge, it is [fill in word here] to factor N to break the EUF-naCMA security of the GHR signature scheme. (Multiple answers can be correct.)

- A sufficient
- B necessary

3. The GHR signature scheme... (Multiple answers can be correct.)

- A ...is more efficient than RSA-FDH signatures
- B ...requires a hash function that maps to group generators
- C ...requires a hash function that maps to prime numbers
- D ...is deterministic (such that the same message is always mapped to the same signature)
- E ...has unique signatures (such that for every message, there exists at most one signature that verification accepts)

4. The GHR signature scheme is EUF-naCMA secure, when the strong RSA assumption holds and the hash function h is... (Assuming that the hash functions outputs only sufficiently large primes.) (Multiple answers can be correct.)

- A ...collision-resistant.
- B ...replaced by a random oracle (ROM).
- C ...2-universal.