
Exercise 10-2  The RSA hardness assumption states that \( P(\text{RSA-inv}_A(n) = 1) \leq \text{negl}(n) \) for any probabilistic polynomial time adversary \( A \).

Show that the RSA hardness assumption implies that factoring is hard in the following sense: No probabilistic polynomial time adversary \( B \) can succeed in the following factoring experiment with non-negligible probability.

1. Randomly generate two primes \( p \) and \( q \) and let \( N := p \cdot q \).
2. Adversary \( B \) is given \( N \) and returns two numbers \( p' \) and \( q' \).
3. The adversary succeeds in the experiment if \( p' \cdot q' = N \).

Exercise 10-3  For any given pseudorandom function \( F \), one can attempt to define a hash function \( (\text{Gen}, H) \) by letting \( \text{Gen}(n) \) be a random string \( s \) of length \( n \) and defining \( H_s(x) := F_s(x) \). Would this definition always produce a collision-resistant hash function?