UMBC | CMSC–443
Fall 1994 | Cryptography and Data Security

Quiz 6

Problem 1
Answer one (not both) of the following questions:

a) Ask a question about any course material covered to date that you do not completely understand. Try to state your question in focused and well-defined fashion. The instructor will try to answer your question in writing.

b) If you completely understand everything in the course so far, then consider Rabin's variation of the RSA cryptosystem in which the encryption exponent is always 2. Thus, for every message $x \in \mathbb{Z}_n$, the encryption of x is $R(x) = x^2 \bmod n$, where $n = pq$ is the product of two large distinct primes p and q. Prove that breaking Rabin's scheme is as hard as factoring the modulus.