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

Quiz 9a (unofficial)

Problem 1
In what sense is breaking Rabin's cryptosystem as hard as factoring? Explain in detail using $n = 589$ as an example. Show the computation.

Hint: $R(307) = 9$*, where* R *denotes Rabin encryption using modulus 589.*