UNIVERSITY OF CALIFORNIA, MERCED

BERKELEY · DAVIS · IRVINE · LOS ANGELES · MERCED · RIVERSIDE · SAN DIEGO · SAN FRANCISCO

SANTA BARBARA · SANTA CRUZ

CSE15: Discrete Mathematics
Take Home Final

Spring 2020

Instructions

Answer the following questions and type your solutions. LaTeX is preferable but you can use some other document creation software. Save your document as s PDF and upload it to CatCourses?

Questions

1. Generate a public and private RSA key pair. You need to show the workings of the entire process and make sure you clearly mark the values for p, q, n, $\varphi(n)$, e, and d. You need to show/explain how you obtained each value, and what (if any) constraints apply to it. Your key does not need to be large but it must follow all the appropriate rules of the RSA algorithm. [50 points]

2. What makes RSA secure? Explain what one would need to do to decode an intercepted message, without knowledge of the private key, and what can we do to ensure that this is difficult. Be as specific as you can. [50 points]