Math 314 - Fall 2018   **Name:**

Mission 10   Due December 3rd, 2018

A signature always reveals a man's character - and sometimes even his name.
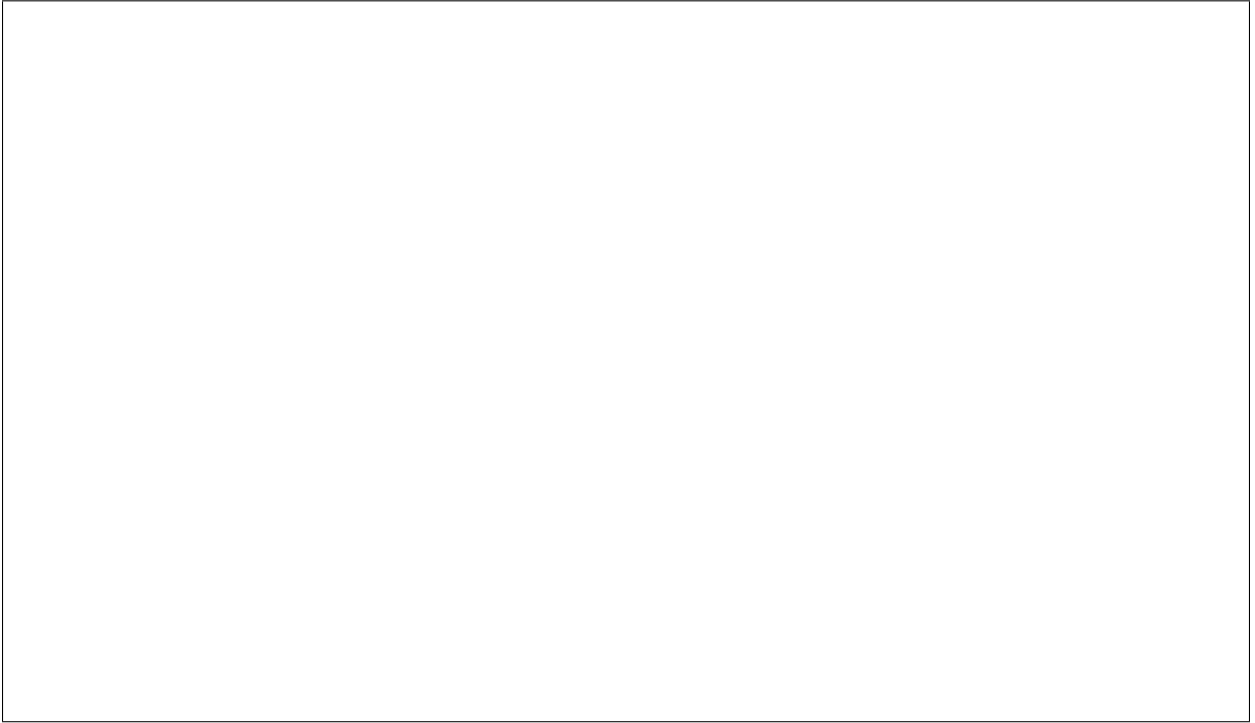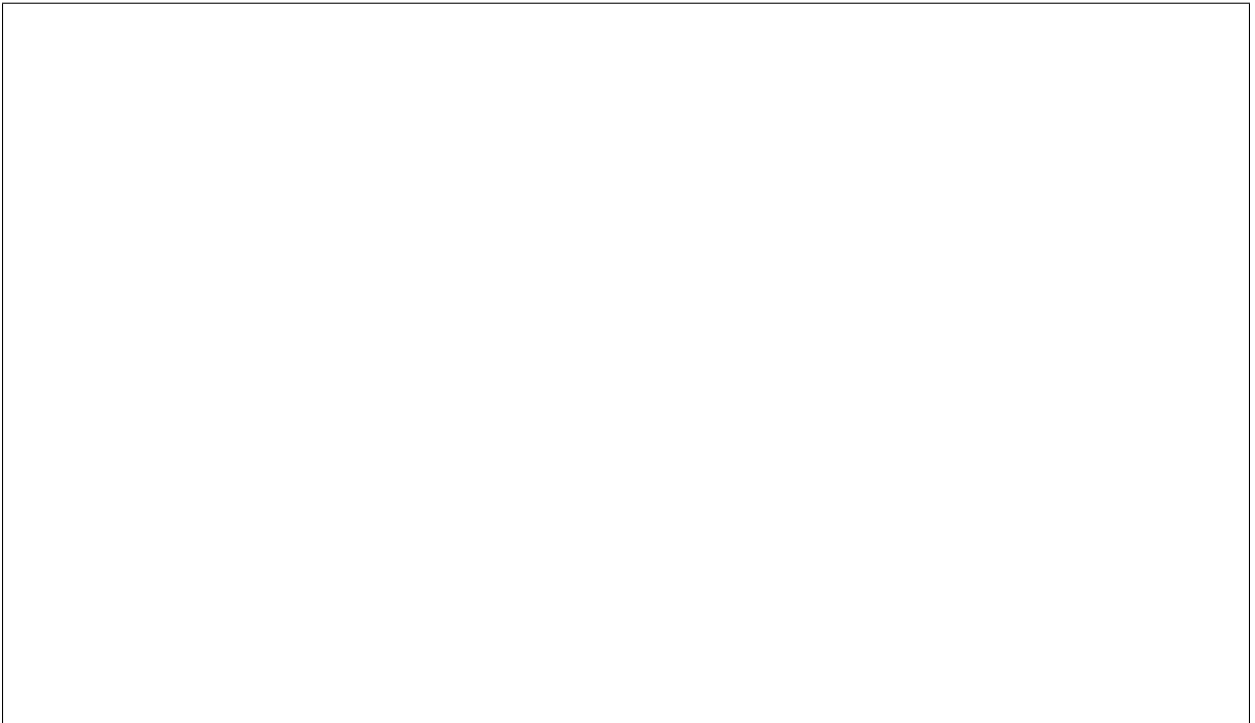
— Evan Esar

1. Graded Problems

1. Exercise 7.6.11

2. Exercise 9.6.3

3. Exercise 8.8.2

4. Alice sets up an RSA key with the primes $p = 31$ and $q = 43$ and exponent $e = 13$. Determine what her signature on the message $m = 100$ would be. (Use a calculator/cocalc to do the exponentiation, but explain your steps!) Verify that the signature is valid.

5. Alice sets up an DSA key with the primes $p = 67$, $q = 11$, and the primitive root $g = 2$. Suppose she picks the secret number $a = 5$. Determine the rest of her public key, and sign the message $m = 17$ (supposing she picks $k = 3$. Verify that the signature is valid.