Name: _____

Directions: Show all work. No credit for answers without work.

1. **[5 parts, 1 point each]** Alice and Bob use RSA to communicate.

   (a) To make his RSA key pair, Bob selects $p = 71$ and $q = 101$. What are N and N'?

   (b) Next, Bob needs to select an encryption exponent; to make encryption fast but nontrivial, he wants his encryption exponent e to be in the range $5 \leq e \leq 10$. Which exponent should Bob choose?

   (c) Find the decryption exponent d.

   (d) What should Bob publish as his public key?

   (e) Alice wants to send Bob $m = 1544$. What ciphertext should she send to Bob?

2. **[3 points]** Given that $N = 1994969$ and $N' = 1992144$, factor N.

3. **[2 points]** Alice publishes (N, e) as her public RSA key. Unfortunately, Alice did not pay attention in cryptography class and is willing to prove her identity by decrypting ciphertexts of random messages encrypted with her public key. Previously Eve intercepted a ciphertext c that Bob sent to Alice. What should Eve send to Alice under the guise of verifying Alice's identity that will allow her to decrypt c? Note: if Eve simply sends c to Alice, then Alice will recognize the decrypted plaintext and refuse Eve's request.