Assignment6 Part A

By Shuwen Zhou

(2) Send a message to Bob. The message that you want to send is the left brace character '{'. You know that Bob's (e, n) pair is (5, 437). What integer will you send? ____16___

(3) Bob receives a message. It is the integer 16. Bob's (d, n) pair is (317, 437). What message did Bob receive? ___{___

(4) An eavesdropper is watching all communications that are destined for Ken. The eavesdropper sees the pair (9,247). He knows that the first number is an encoded ASCII value and the second number is Ken's value for n. He also knows the algorithm that Ken uses to determine n, phi, e and d from p and q. The eavesdropper sees that Ken has chosen a rather small value for n and so decides to break this code. What ASCII character is being sent to Ken? ___Q___

Decoded int = 9;

N = 247

(5) Consider an RSA key set with p = 11, q = 29, n = 319, and e = 3. What value of d should be used in the secret key? ____187___

What is the encryption of the message m = 100? ___z____

(6) Bob receives several digitally signed messages from someone he thinks may be Alice. He knows that Alice's public key is (e = 3, n = 391). The messages each arrive in two parts. The first part is "in the clear" and is not protected from disclosure. The second part is the first part encrypted using the signer's secret key d. Here are the message pairs Bob receives. Which ones are actually from Alice and which one's have been corrupted or are forged? (Hint: Alice uses her secret key to encrypt the signed part. Bob needs to use Alice's public key to compare the clear text with the encoded text.)

<'A', 112> actual = 143

<'L', 359> actual = 274

<'X', 296> actual = 350

<'B', 113> actual = 111

None of those is from Alice.