Math 173A - RSA

1. Recall that decrypting in RSA involves inverting a number e modulo $\phi(N)$, where N is a product of two large (distinct) primes p and q. The difficulty is that if Eve doesn't know p or q, it's (presumably) hard for her to compute $\phi(N)$, and therefore hard for her to invert e.

   Explain how Eve can find p and q if she knows $N = pq$ (which we always assume she does) and the sum $p + q$. *Hint: expand* $(x - a)(x - b)$.

2. The ciphertext 75 was obtained using RSA with $N = 437$ and $e = 3$. You know that the plaintext is either 8 or 9. Determine which it is without factoring N.

3. In order to increase security, Bob chooses n and two encryption exponents e_1, e_2. He asks Alice to encrypt her message m to him by first computing $c_1 \equiv m^{e_1} \pmod{N}$, then encrypting c_1 to get $c_2 \equiv c_1^{e_2} \pmod{N}$. Alice then sends c_2 to Bob. Does this double encryption increase security over single encryption? Why or why not?