WORKSHOP 15: §7.5, 7.8, 7.9 MARCH 7, 2017

Name: _____

(1) You'll need a group of three people for this one. You should each play the role of Bob, Alice, and Eve once.
   (a) Bob: Choose two small 3-digit primes. Construct an RSA public key (N, e) and announce it to your two neighbors. Construct the decoding key d and keep it secret.
   (b) Alice: Create a two-character text message you would like to share with Bob (but hide from Eve). Turn your message into an integer, using either the scheme from the textbook or ASCII codes, then encode it using the public key Bob announced. Announce the encoded message to your neighbors. (You'll need to also announce whether you used the textbook scheme or ASCII. Using ASCII will allow you to use characters other than just letters.)
   (c) Eve: You eavesdropped on Alice's announced message. To decode it you would need to know how to factor N. Since N was small-ish, you can do this with brute force. Do it, probably using a calculator such as WolframAlpha. Now you know everthing that Bob knows!
   (d) Bob&Eve: Decrypt Alice's message. (Check with Alice that you've got it right.)

   Again, the difficulty for Eve is factoring N. In real applications, both primes chosen have hundreds of digits, so their product has perhaps thousands of digits. There are no (publicly) known algorithms that can factor such an integer (on today's computers) in less than about 10 years of processing time.

(2) Theorem 7.5.2 in your text is called Bézout's Identity[1], and the coefficients s, t are called Bézout coefficients.
   (a) Using prime factorization, find $\gcd(125, 35)$.
   (b) Find Bézout coefficients for 125 and 35 by inspection *(a phrase which here means "stare at it, play around with it, guess an answer").*
   (c) Use the Extended Euclidean Algorithm to answer both 2a and 2b.
   (d) Did you get the same Bézout coefficients in 2b and 2c? Do you think Bézout coefficients are unique?
   (e) Find integers m, n such that $0 = 125m + 35n$.
   (f) Can you use your answer to 2e to prove that Bézout coefficients are NOT unique (for 125 and 35, but can you also generalize)?

(3) Find multiplicative inverses for the following elements in the given ring, or else state that the inverse doesn't exist.
   (a) 2 in $\mathbb{Z}_3$ *(Hint: there are not many choices, just try them all.)*
   (b) 8 in $\mathbb{Z}_9$ *(Hint: replace 8 by something easier that is equal to 8 in $\mathbb{Z}_9$. Then find the inverse by inspection.)*
   (c) 6 in $\mathbb{Z}_9$
   (d) 11 in $\mathbb{Z}_{13}$
   (e) 1523 in $\mathbb{Z}_{1601}$ *(Hint: do NOT try to guess this one.)*

[1] Bézout proved a version for polynomials in 1779; for integers, it was proven by Bachet in 1624.