CIS 3362 Final Exam - Part D (Public Key Crypto, Odds, Ends) - 25 pts

Date: 12/9/2020
Start Time: 12:00 pm EST
End Time: 12:40 pm EST

You may use your class notes, reference sheets and calculator. Please still show each step but just put answers of calculations you made in your calculator.

Note: Please put your name in the document you turn in.

1) (8 pts) Alice is using the El Gamal Cryptosystem. Her global public elements are:

q = 43 (prime number)
α = 12 (generator)

Alice's private key $X_A = 11$ and her posted public key is $Y_A = 26$.

Bob has sent Alice the following ciphertext: $C_1 = 40$, $C_2 = 20$.

Go through the process Alice would go through to recover the plaintext, showing your work and highlight the plaintext message Bob sent to Alice. **Please show your step by step work by hand for both modular exponentiation AND the Extended Euclidean Algorithm. (You can check individual steps with the calculator, but part of the points for the question are devoted to seeing if you know how to do these by hand.)**

2) (8 pts) The Elliptic Curve $E_{37}(4, 7)$ has points P = (20, 24) and Q = (32, 26). Determine the sum P + Q on this curve.

3) (4 pts) Alice and Bob have both set up their own RSA systems and want to use them for both encrypting messages and digital signatures. Both decided it would be easier to perform the double encryption if they both used the same public key n. What is the problem if they do this?

4) (5 pts) The Universal Studios ride, E. T. Adventure is based on what feel good 1980s movie?