CIS 3362 Quiz #5: Public Key Encryption

Date: 11/15/2024

Name : _____

1) (9 pts) Consider doing a Diffie-Hellman Key Exchange with the public keys p = 37 and g = 5. Let Alice choose a private key of a = 23 and Bob choose a private key of b = 17. Calculate

(a) The value that Alice sends to Bob.
(b) The value that Bob sends to Alice.
(c) The shared key that both Alice and Bob will calculate at the end.

Please show which modular exponentiations you are calculating, and then use your calculator to compute them, just showing the result. You may break down your expressions in any way you see fit (ie. you don't have to follow exactly the fast modular exponentiation algorithm shown in class, but can use any exponential break down that makes sense to you.) Also, you may use Fermat's Theorem to get the final answer, if you deem it useful. **Note: but you do have to show clear work that indicates that you know the steps to make the calculation without a built in modular exponentiation function.**

Alice sends Bob: _____ Bob sends Alice: _____ Shared Key: _____

2) (10 pts) In an RSA system, p = 13, q = 37 and e = 125. What is d? (Note: Full credit will only be given to responses that appropriately use the Extended Euclidean Algorithm.)

d = _____

3) (10 pts) Let the public elements of an El Gamal Cryptosystem be $q = 47$, $\alpha = 13$. Let Alice's private key $X_A = 28$. Do the following:

1. Calculate Alice's Public Key (Y_A). (Show the appropriate modular exponential breakdown.)
2. Calculate the ciphertext (C_1, C_2) when Bob sends a message to Alice where $M = 21$ and his randomly chosen value $k = 26$. In the process, show the value of K.

Y_A = _____ , C1 = _____ , K = _____ , C2 = _____

4) (10 pts) Let C be the elliptic curve $E_{31}(6, 7)$. Two points on C are P = (16, 18) and Q = (4, 23). What is the result of adding P and Q? (The answer is a point on the curve.)

P + Q = (_____ , _____)

5) (10 pts) On the elliptic curve $E_{31}(6, 7)$, the following are results of several products of integers and points:

```
1.  20 x (29, 7)  = ORIGIN
2.   4 x (29, 7)  = (19, 6)
3.  11 x (29, 7)  = (20, 6)
4.  16 x (29, 7)  = (19, 25)
5.  17 x (29, 7)  = (16, 13)
```

Using this information, determine the value of 13 x (29, 7). **Note: you will have to do some computation, but it's not an unreasonable amount.**

13 x (29, 7) = (_____ , _____)

6) (1 pt) Kingston is the mascot of the MLS playoff Orlando Lions.
What type of animal is Kingston? _____

Scratch Page – Please clearly mark any work on this page you would like graded.