**CIS 3362 Quiz #5: Public Key Encryption**

**Date: 11/14/2025**

**Name : ______________________________________**

1) (9 pts) Consider doing a Diffie-Hellman Key Exchange with the public keys p = 31 and g = 3. Let Alice choose a private key of a = 12 and Bob choose a private key of b = 21. 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, n = 493 and e = 297. 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 = 37, α = 5. Let Alice's private key $X_A$ = 22. 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 = 9 and his randomly chosen value k = 30. In the process, show the value of K.

$Y_A$ = __________ , K = __________ , C1 = __________ , C2 = __________

4) (10 pts) Let C be the elliptic curve $E_{31}(3, 5)$. One point on C is P = (18, 1). What is the result of P + P? (Please provide your answer as a point.)

P + P = ( ________ , _________ )

5) (10 pts) Consider the task of encoding a 4-bit value (a hex character) on the Elliptic Curve $E_{79}(1, 1)$. We learned a technique in class to store an arbitrary bit string in class as a point on an Ellipitic Curve. **Using the same technique in class determine the Point encoding of the plaintext message m = 11 on the curve $E_{79}(1, 1)$.** Since this is computationally intensive, some facts will be given below that you may use to solve the problem. Use the facts as necessary. (Note: some of the facts are intentionally irrelevant, so part of what I am testing is to see if you can figure out what you actually need to use. Also, there is one calculation that I think is easy enough to do on your calculator for which I haven't provided the result.)

$11^{39} \equiv 1 \pmod{79}$
$22^{39} \equiv 1 \pmod{79}$
$27^{39} \equiv 78 \pmod{79}$
$32^{39} \equiv 1 \pmod{79}$
$43^{39} \equiv 78 \pmod{79}$
$59^{39} \equiv 78 \pmod{79}$

$11^{20} \equiv 13 \pmod{79}$
$11^{27} \equiv 52 \pmod{79}$
$27^{20} \equiv 62 \pmod{79}$
$27^{40} \equiv 52 \pmod{79}$
$40^{20} \equiv 44 \pmod{79}$
$40^{27} \equiv 67 \pmod{79}$

Plaintext Point = ( ________ , _________ )

6) (1 pt) By what acronym is the Public Key Encryption system created by Ron Rivest, Adi Shamir and Leonard Adelman known as?

______________________

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