CIS 3362 Quiz #5 Review 11/12/25

AIDS: Calculator, 2 sheets of notes, your responsible fore the relevant formulas

TOPICS: ① Diffie-Hellman Key Exchange
② RSA
③ El Gamal
④ Elliptic Curves (how to add, mult)
⑤ ECCrypto via El Gamal
* ⑥ How to encode a bitstring as an EC point
⑦ Quantum Crypto
(so no TBDH)

Will do 2024 Quiz #5

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.**

$A \to B \quad 5^{23} \mod 37$

$5^5 = 3125 \equiv 17$

$5^6 = 17 \times 5 = 85 \equiv 11$

$B \to A \quad 5^{17} \mod 37$

$5^{17} \equiv 5^6 \times 5^6 \times 5^5 = 11 \times 11 \times 17 = 2057$

$\equiv 22 \mod 37$

$5^{23} \equiv 5^{17} \times 5^6$

$\equiv 22 \times 11$

$= 242$

$\equiv 20 \mod 37$

then do $A \to B \quad 20^{17} \mod 37$

$20^{17} \equiv 20^{16} \times 20$

$\equiv 16 \times 20$

$\equiv 320$

$\equiv 24$

$20^2 \equiv (-7) \mod 37$

$20^4 \equiv (-7)(-7) \equiv 49 \equiv 12 \mod 37$

$20^8 \equiv 12 \times 12 = 144 \equiv -4 \mod 37$

$20^{16} \equiv (-4)^2 \equiv 16 \mod 37$

Alice sends Bob: 20 Bob sends Alice: 22 Shared Key: 24

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.)

$n = 13 \times 37$

$\phi(n) = (13-1)(37-1)$

$= 12 \times 36$

$= 432$

$d = e^{-1} \bmod \phi(n) = 125^{-1} \bmod 432$

$432 = 3 \times 125 + 57$

$125 = 2 \times 57 + 11$

$57 = 5 \times 11 + 2$

$11 = 5 \times 2 + 1$

$11 - 5 \times 2 = 1$

$11 - 5(57 - 5 \times 11) = 1$

$11 - 5 \times 57 + 25 \times 11 = 1$

$26 \times 11 - 5 \times 57 = 1$

$26(125 - 2 \times 57) - 5 \times 57 = 1$

$26 \times 125 - 52 \times 57 - 5 \times 57 = 1$

$26 \times 125 - 57 \times 57 = 1$

$26 \times 125 - 57(432 - 3 \times 125) = 1$

$26 \times 125 - 57 \times 432 + 171 \times 125 = 1$

$197 \times 125 - 57 \times 432 = 1 \bmod 432$

$197 \times 125 \equiv 1 \bmod 432$

is neg add mod #

$d = 125^{-1} = 197$

d = 197

3) (10 pts) Let the public elements of an El Gamal Cryptosystem be q = 47, α = 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.

1. $Y_A = \alpha^{X_A} = 13^{28} \mod 47$

$13^1 \equiv 13$

$13^2 \equiv 169 \equiv 28 \mod 47$

$13^4 \equiv 28^2 \equiv 32 \mod 47$

$13^8 \equiv 32^2 \equiv -10 \mod 47$

$13^{16} \equiv (-10)^2 \equiv 100 \equiv 6 \mod 47$

$13^{28} = 13^{16} \times 13^8 \times 13^4$

$\equiv 6 \times (-10)(-15)$

$\equiv 900$

$\equiv 7$

$C_1 = \alpha^k = 13^{26} \equiv 13^{16} \times 13^8 \times 13^2$

$\equiv 6 \times (-10)(28)$

$\equiv -60 \times 28$

$\equiv (-13) \times 28$

$\equiv -364$

$\equiv 12 \mod 47$

$7^2 \equiv 49$

$\equiv 2 \mod 47$

$(7^{12}) = (7^2)^6$

$\equiv 2^6 \equiv 64$

$\equiv 17 \mod 47$

part of Diffie-Hellman key exchange

$K = \cancel{C_2} \; Y_A^k = 7^{26} =$

$7^{26} \equiv 7^{24} \times 7^2$

$\equiv 7 \times 2$

$\equiv 14$

$7^{24} = (7^{12})^2$

$= 17^2$

$= 289$

$\equiv 7$

$C_2 = K \cdot M \mod q$

$14 \times 21 = 294$

$\equiv 12$

$Y_A =$ 7 , C1 = 12 , K = 14 , C2 = 12

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.)

prime = 31, $a=6$, $b=7$

$P+Q$: $\lambda = \frac{23-18}{4-16} = \frac{5}{-12} = 5(19^{-1} \bmod 31)$

$31 = 1\times19 + 12$
$19 = 1\times12 + 7$
$12 = 1\times7 + 5$
$7 = 1\times5 + 2$
$5 = 2\times2 + 1$

$5 - 2\times2 = 1$
$5 - 2(7-5) = 1$
$3\times5 - 2\times7 = 1$
$3(12-7) - 2\times7 = 1$

$3\times12 - 5\times7 = 1$
$3\times12 - 5(19-12) = 1$
$3\times12 - 5\times19 + 5\times12 = 1$
$8\times12 - 5\times19$
$8(31-19) - 5\times19 = 1$
$8\times31 - 13\times19 = 1$
$19^{-1} \equiv -13 \equiv 18 \bmod 31$

$\lambda = 5\times18$
$= 90 \equiv 28 \bmod 31$
$-62 \equiv -3$

$x_R = (\lambda^2 - x_P - x_Q) \bmod p$
$= (-3)^2 - 16 - 4$
$= 9 - 20 = -11 \equiv 20$

$y_R = (\lambda(x_P - x_R) - y_P) \bmod p$
$= (-3)(16-20) - 18$
$= (-3)(-4) - 16$
$= 12 - 18$
$= -6 \equiv 25 \bmod 31$

P + Q = (20 , 25)

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)

P + (-P) = ORIGIN

17 x (29,7) = (16,13)

n x (29,7) = (16,16)

what is n? 3

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.**

33P = 13P

more generally if a pt's cycle size is n,

then $xP = yP$ iff $x \equiv y \pmod n$

Intended was (19,25) + (16, 13)

$$\lambda = \frac{13 - 25}{16 - 19} = \frac{-12}{-3} = 4$$

$$x_R = (\lambda^2 - x_P - x_Q) \bmod p$$
$$= 4^2 - 19 - 16 \bmod 31$$
$$= -19 \equiv 12 \bmod 31$$

$$y_R = (\lambda(x_P - x_R) - y_P) \bmod p$$
$$= 4(19 - 12) - 25$$
$$= 28 - 25$$
$$= 3 \bmod 31$$

Also works

17P - 4P

4P - 11P

13 x (29, 7) = (12 , 3)

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