CIS 3362 Quiz #5: Public Key Encryption Solutions

Date: 11/15/2024

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) Alice sends to Bob $5^{23} = 5^{20} \times 5^3 = (5^4)^5 \times 5^3 = 625^5 \times 125 \equiv 33^5 \times 14$
$\equiv (-4)^5 \times 14 \equiv -1024 \times 14 \equiv -14336 \equiv -17 \equiv$ **20 (mod 37)** [via calc]

(b) Bob sends to Alice $5^{17} = (5^4)^4 \times 5 = 625^4 \times 5 \equiv (-4)^4 \times 5 \equiv 256 \times 5 \equiv 1280 \equiv$ **22 (mod 37)** [via calc]

(c) Note that $\varphi(37) = 36$, so $5^{36} \equiv 1 \pmod{37}$ via Fermat's Theorem

Shared key is $5^{23 \times 17} = 5^{391} = (5^{36})^{10} \times 5^{31} \equiv 1 \times 5^{31} \equiv 5^{23} \times 5^8 \equiv 20 \times (5^4)^2$
$\equiv 20 \times (625)^2 \equiv 20 \times (-4)^2 \equiv 20 \times 16 \equiv 320 \equiv$ **24 (mod 37)**

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

Grading: 3 pts for each blank and work
2 pts for answer, 1 pt for work
if answer is wrong due to arithmetic error, can award 2/3
can give full credit to part c if it's correctly built off of an incorrect old part.
any reasonable exponential breakdown is fine.

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.)

$\varphi(pq) = \varphi(13 \times 37) = \varphi(13) \times \varphi(37) = 12 \times 36 = 432$

It follows that $d \equiv e^{-1} \bmod \varphi(n) \equiv 125^{-1} \bmod 432$

Let's run the Extended Euclidean Algorithm:

$432 = 3 \times 125 + 57$
$125 = 2 \times 57 + 11$
$57 = 5 \times 11 + 2$
$11 = 5 \times 2 + 1$

$11 - 5 \times 2 = 1$
$11 - 5(57 - 5 \times 11) = 1$
$11 - 5 \times 57 + 25 \times 11 = 1$
$26 \times 11 - 5 \times 57 = 1$
$26(125 - 2 \times 57) - 5 \times 57 = 1$
$26 \times 125 - 52 \times 57 - 5 \times 57 = 1$
$26 \times 125 - 57 \times 57 = 1$
$26 \times 125 - 57(432 - 3 \times 125) = 1$
$26 \times 125 - 57 \times 432 + 171 \times 125 = 1$
$197 \times 125 - 57 \times 432 = 1$

Taking this equation mod 432 we find

$197 \times 125 \equiv 1 \pmod{432}$

It follows that **d = 197.**

d = 197

Grading: 2 pts for phi (if phi is wrong or EEA not with 432, MAX SCORE 1/10)
2 pts for Euclidean
5 pts for EEA
1 pt to extract answer and properly state it.

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. (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.

1. $Y_A = \alpha^{X_A} = 13^{28} = (13^4)^7 \equiv 28561^7 \equiv 32^7 \equiv 32^4 \times 32^3 \equiv 1048576 \times 32768$
$\equiv 6 \times 9 \equiv 54 \equiv \mathbf{7}\ (\boldsymbol{mod}\ \mathbf{47})$

2. $C_1 = \alpha^k = 13^{26} = (13^4)^4 \times (13^4)^2 \times 13^2 \equiv 1048576 \times 32^2 \times 28$
$\equiv 6 \times 1024 \times 28 \equiv 6 \times (-10) \times 28$
$\equiv -1680 \equiv -35 \equiv \mathbf{12}\ (\boldsymbol{mod}\ \mathbf{47})$

3. $K = {Y_A}^k = 7^{26} = (7^2)^{13} \equiv 49^{13} \equiv 2^{13} \equiv 8192 \equiv \mathbf{14}\ (\boldsymbol{mod}\ \mathbf{47})$

Finally, $C_2 = KM = 14 \times 21 = 294 \equiv \mathbf{12}\ (\boldsymbol{mod}\ \mathbf{47})$

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

Grading: 3 pts for Y_A
3 pts for C_1
2 pts for K
2 pts for C_2

Give full credit if each exponent is properly written down from the definition. Give 1 pt for each answer, Give carry over credit when possible (so if Y_A is wrong, but it's used correctly to figure out K, go ahead and give credit for a wrong K that is correct for the wrong Y_A)

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.)

$$\lambda = \frac{23 - 18}{4 - 16} = \frac{5}{-12} = 5 \times 19^{-1} (mod\ 31)$$

Use EEA to find 19^{-1} mod 31

31 = 19 + 12
19 = 12 + 7
12 = 7 + 5
7 = 5 + 2
5 = 2x2 + 1

5 – 2 x 2 = 1
5 – 2(7 – 5) = 1
3 x 5 – 2 x 7 = 1
3(12 – 7) – 2 x 7 = 1
3 x 12 – 5 x 7 = 1
3 x 12 – 5(19 – 12) = 1
3 x 12 – 5 x 19 – 5 x 12 = 1
8 x 12 – 5 x 19 = 1
8(31 – 19) – 5 x 19 = 1
8 x 31 – 13 x 19 = 1
Thus $19^{-1} = -13 \equiv 18\ (mod\ 31)$

It follows that $\lambda = 5 \times 18 = 90 \equiv 28 \equiv -3\ (mod\ 31)$.

$$x_R = \lambda^2 - x_P - x_Q = (-3)^2 - 16 - 4 = 9 - 20 = -11 \equiv \mathbf{20}\ (\boldsymbol{mod\ 31})$$

$$y_R = (\lambda(x_P - x_R) - y_P) = (-3(16 - 20) - 18) = 12 - 18 = -6 \equiv \mathbf{25}\ (\boldsymbol{mod\ 31})$$

P + Q = (20 , 25)

Grading: 1 pt lambda formula
5 pts EEA to get 19 inverse mod 31
1 pt to plug in to get final lambda
2 pts plug in to get x_R
1 pt to plug into get y_R

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.**

The first line of information tells us that the order of the point (29, 7) on $E_{31}(6, 7)$ is 20. Thus, we seek to integers A and B such that A + B ≡ 13 (mod 20) where we can easily calculate

A x (29, 7) + B x (29, 7).

(In theory, we could add several terms, but one addition on Elliptic Curves by hand is quite a lot, so our hope is to get it done with one.)

Thus, we seek A + B = 13 or A + B = 33. Scanning the given information, we see that we know

16 x (29, 7) and 17 x (29, 7) and that 16 + 17 = 33. It follows that

13 x (29, 7) = 16 x (29, 7) + 17 x (29, 7) = (19, 25) + (16, 13). Let P = (19, 25), Q = (16, 13)

$$\lambda = \frac{13 - 25}{16 - 19} = \frac{-12}{-3} = \mathbf{4}\ (\boldsymbol{mod}\ \mathbf{31})$$

$$x_R = \lambda^2 - x_P - x_Q = 4^2 - 19 - 16 = 16 - 35 = -19 \equiv \mathbf{12}\ (\boldsymbol{mod}\ \mathbf{31})$$

$$y_R = (\lambda(x_P - x_R) - y_P) = (4(19 - 12) - 25) = 28 - 25 \equiv \mathbf{3}\ (\boldsymbol{mod}\ \mathbf{31})$$

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

Grading: 5 pts for reasoning for adding the last two points listed (give partial as needed)
1 pt for lambda
2 pts for x
2 pts for y
If wrong points added, max grade 4 of 10, decide as needed.

6) (1 pt) Kingston is the mascot of the MLS playoff Orlando Lions.
What type of animal is Kingston? **Lion (give to all)**