CIS 3362 Quiz #5: Public Key Encryption Solutions

Date: 11/12/2021

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 = 15 and Bob choose a private key of b = 24. 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.

(a) Alice sends to Bob: 5^{15} mod 37. Here is a table of the first few exponents of 5, mod 37:

Exponent	1	2	3	4	5
5^{exp} mod 37	5	25	14	33	17

Thus, : $5^{15} \equiv (5^5)^3 \equiv 17^3 \equiv$ **29 (mod 37)**

(b) Bob sends to Alice: $5^{24} \equiv (5^4)^6 \equiv (-4)^6 \equiv 4096 \equiv$ **26 (mod 37)**

(c) Their shared key is $5^{15*24} \equiv 5^{360} \equiv (5^{36})^{10} \equiv 1^{10} \equiv$ **1 (mod 37)**, using Fermat's Theorem for the major simplification.

Alice sends Bob: **29** Bob sends Alice: **26** Shared Key: **1**

Grading: 3 pts for each, give partial as you see fit.

2) (10 pts) In an RSA system, p = 17, q = 31 and e = 91. What is d? (Note: Full credit will only be given to responses that appropriately use the Extended Euclidean Algorithm.)

$\Phi(n) = (17-1) \times (31-1) = 16 \times 30 = 480$

$d = 91^{-1} \bmod 480$

Use the Extended Euclidean Algorithm:

$480 = 5 \times 91 + 25$
$91 = 3 \times 25 + 16$
$25 = 1 \times 16 + 9$
$16 = 1 \times 9 + 7$
$9 = 1 \times 7 + 2$
$7 = 3 \times 2 + 1$

$7 - 3 \times 2 = 1$
$7 - 3(9 - 7) = 1$
$4 \times 7 - 3 \times 9 = 1$
$4(16 - 9) - 3 \times 9 = 1$
$4 \times 16 - 7 \times 9 = 1$
$4 \times 16 - 7(25 - 16) = 1$
$11 \times 16 - 7 \times 25 = 1$
$11(91 - 3 \times 25) - 7 \times 25) = 1$
$11 \times 91 - 33 \times 25 - 7 \times 25 = 1$
$11 \times 91 - 40 \times 25 = 1$
$11 \times 91 - 40(480 - 5 \times 91) = 1$
$11 \times 91 - 40 \times 480 + 200 \times 91 = 1$
$211 \times 91 - 40 \times 480 = 1$

Taking this equation mod 480 we find:

$211 \times 91 \equiv 1 \pmod{480}$

It follows that **$d = 211$.**

Grading: 2 pts for phi, 3 pts for Euclidean, 4 pts for Extended, 1 pt to extract answer

3) (12 pts) Let the public elements of an El Gamal Cryptosystem be q = 41, α = 12. Let Alice's private key X_A = 17. Do the following:

1. Calculate Alice's Public Key.
2. Calculate the ciphertext (C_1, C_2) when Bob sends a message to Alice where M = 6 and his randomly chosen value k = 19.

1. $Y_A = 12^{17} \bmod 41$. Here is a table of the first few exponents of 12, mod 41:

Exponent	1	2	3	4	5
$12^{exp} \bmod 41$	12	21	6	31	3

$12^{17} \equiv (12^5)^3 12^2 \equiv 3^3(21) \equiv 27 \times 21 \equiv$ **34 mod 41.**

2. $K \equiv 34^{19} \pmod{41} \equiv (-7)^{19} \equiv ((-7)^2)^9(-7) \equiv 8^9(-7) \equiv (8^3)^3(-7) \equiv 20^3(-7) \equiv -56000 \equiv$ **6 (mod 41)**

$C_1 \equiv 12^{19} \equiv 12^{17}12^2 \equiv 34 \times 21 \equiv 714 \equiv$ **17 (mod 41)**

$C_2 \equiv KM \equiv 6(6) \equiv$ **36 (mod 41)**

C1 = **17**, C2 = **36**

Grading: 3 pts for Alice's Public Key, 3 pts for calculation of K, 3 pts for C_1 and 3 pts for C_2

4) (10 pts) Let C be the elliptic curve $E_{37}(17, 5)$. Two points on C are P = (21, 15) and Q = (26, 2). What is the result of adding P and Q? (The answer is a point on the curve.)

First we find lambda: $\lambda = \frac{2-15}{26-21} mod\ 37 = (-13)(5^{-1}) mod\ 37$

Use the Extended Euclidean Algorithm to find 5^{-1} mod 37:

37 = 7 x 5 + 2
5 = 2 x 2 + 1
5 - 2 x 2 = 1
5 - 2(37 - 7 x 5) = 1
15 x 5 - 2 x 37 = 1
$5^{-1} \equiv 15$ (mod 3), so $\lambda = (-13)(15) \equiv -195 \equiv 27\ mod 37$

$x_R = \lambda^2 - x_P - x_Q = 27^2 - 21 - 26 = 682 \equiv 16$

$y_R = \lambda(x_P - x_R) - y_P = 27(21 - 16) - 15 = 27 \text{ x } 5 - 15 = 120 \equiv 9$

P + Q = (16, 9)

Grading: 2 pts for expression for lambda, 2 pts for 5^{-1}, 2 pts for getting lambda, 2 pts for x, 2 pts for y

5) (6 pts) On the elliptic curve $E_{37}(17, 5)$, the following are results of several addition problems between points:

```
1.  ORIGIN   + (26, 2) = (26, 2)
2.  (26, 2)  + (26, 2) = (19, 34)
3.  (19, 34) + (26, 2) = (28, 23)
4.  (28, 23) + (26, 2) = (10, 18)
5.  (10, 18) + (26, 2) = (2, 11)
6.  (2, 11)  + (26, 2) = (34, 1)
7.  (34, 1)  + (26, 2) = (25, 21)
8.  (25, 21) + (26, 2) = (14, 29)
9.  (14, 29) + (26, 2) = (9, 6)
10. (9, 6)   + (26, 2) = (5, 17)
11. (5, 17)  + (26, 2) = (5, 20)
12. (5, 20)  + (26, 2) = (9, 31)
13. (9, 31)  + (26, 2) = (14, 8)
14. (14, 8)  + (26, 2) = (25, 16)
15. (25, 16) + (26, 2) = (34, 36)
16. (34, 36) + (26, 2) = (2, 26)
17. (2, 26)  + (26, 2) = (10, 19)
18. (10, 19) + (26, 2) = (28, 14)
19. (28, 14) + (26, 2) = (19, 3)
20. (19, 3)  + (26, 2) = (26, 35)
21. (26, 35) + (26, 2) = ORIGIN
```

Using just the information in these facts, **without doing any difficult computation (like question #4)**, determine the following sum (34, 36) + (28, 14). There is a little bit of work to show to justify your answer, please explain that work in words and provide your answer.

The chart shows each multiple of (26, 2) until it loops, so we find that:

(34, 36) = 15 x (26, 2)
(28, 14) = 18 x (26, 2)

(34, 36) + (28, 14) = 15 x (26, 2) + 18 x (26, 2)
= 33 x (26, 2)
= 21 x (26, 2) + 12 x (26, 2), breakdown like this to use looping structure.
= ORIGIN + (9, 31), look up 12 x (26, 2) from the chart above.
(34, 36) + (28, 14) = (9, 31)

Grading: 1 pt for finding 15 for (34, 36), 1 pt for finding 18 for (28, 14), 2 pts for recognizing looping behavior, 2 pts for the final answer

6) (3 pts) Who is commemorated on the Martin Luther King Jr. Memorial in Washington, D.C.?

Martin Luther King Jr. (Grading: Give to all)