CIS 3362 Quiz #5: Public Key Encryption Solutions

Date: 11/17/2023

1) (9 pts) Consider doing a Diffie-Hellman Key Exchange with the public keys p = 43 and g = 12. Let Alice choose a private key of a = 19 and Bob choose a private key of b = 29. 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 to Bob 12^{19} mod 43. Use a Calculator to compute.
$12^2 = 144 \equiv 15 \pmod{43}$
$12^4 = (12^2)^2 \equiv 15^2 \equiv 225 \equiv 10 \pmod{43}$
$12^8 \equiv 10^2 \equiv 100 \equiv 14 \pmod{43}$
$12^{16} \equiv 14^2 \equiv 196 \equiv 24 \pmod{43}$
$12^{19} = 12^{16}12^2 12^1 \equiv (24)(15)(12) \equiv (360)(12) \equiv (16)(12) \equiv 192 \equiv \underline{\mathbf{20 \pmod{43}}}$

Bob sends Alice:
$12^{29} \equiv 12^{16}12^8 12^4 12 \equiv (24)(14)(10)(12) \equiv (240)(168) \equiv (25)(-4) \equiv -100 \equiv \underline{\mathbf{29 \pmod{43}}}$

Their shared key is $12^{19(29)} = 12^{551} \equiv (12^{42})^{13}12^5 \equiv 1^{13}12^5 \equiv 12^4 12^1 \equiv (10)(12) \equiv \underline{\mathbf{34 \bmod 43}}$

Alice sends Bob: **20**   Bob sends Alice: **29**   Shared Key: **34**

Grading: 3 pts each, full credit if reasonable breakdown and work (assuming calculator)
1 pt for writing down correct base and exponent for a calculation
2 pts for the intermediate work
0 out of 3 if only answer is written and it's correct.

2) (10 pts) In an RSA system, p = 23, q = 29 and e = 135. What is d? (Note: Full credit will only be given to responses that appropriately use the Extended Euclidean Algorithm.)

n = 23 x 29, so $\phi(n) = (23 - 1)(29 - 1) = 22 \times 28 = 616$

It follows that d = 135^{-1} mod 616. Use the Extended Euclidean Algorithm to find d:

616 = 4 x 135 + 76
135 = 1 x 76 + 59
76 = 1 x 59 + 17
59 = 3 x 17 + 8
17 = 2 x 8 + 1

17 – 2 x 8 = 1
17 – 2(59 – 3 x 17) = 1
17 – 2 x 59 + 6 x 17 = 1
7 x 17 – 2 x 59 = 1
7(76 – 59) – 2 x 59 = 1
7 x 76 – 7 x 59 – 2 x 59 = 1
7 x 76 – 9 x 59 = 1
7 x 76 – 9(135 – 76) = 1
7 x 76 – 9 x135 + 9 x 76 = 1
16 x 76 – 9 x 135 = 1
16(616 – 4 x 135) – 9 x 135 = 1
16 x 616 – 64 x 135 – 9 x 135 = 1
16 x 616 – 73 x 135 = 1

Take this equation mod 616 to yield

-73 x 135 ≡ 1 (mod 616)

It follows that d = 135^{-1} ≡ -73 ≡ **543 (mod 616).**

Grading: 2 pts to get 616 as phi
1 pt to ID that we need 135^{-1} mod 616
2 pts Euclidean
4 pts Extended Euclidean
1 pt to make -73 to 543.

3) (10 pts) Let the public elements of an El Gamal Cryptosystem be $q = 53$, $\alpha = 5$. Let Alice's private key $X_A = 22$. 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 $M = 33$ and his randomly chosen value $k = 8$.

Alice's Public Key will be $5^{22} \bmod 53$. Using a calculator, we find $5^4 = 625 \equiv (-11) \pmod{53}$
$5^{20} = (5^4)^5 \equiv (-11)^5 = -161051 \equiv 16 \pmod{53}$, via calculator
Thus, $5^{22} = 5^{20}5^2 \equiv (16)(25) \equiv 400 \equiv$ **29 mod 53**

Bob's value of $C_1 = 5^8 = (5^4)^2 \equiv (-11)^2 \equiv 121 \equiv$ **15 (mod 53)**

Bob's value of $K = 29^8 = (29^4)^2 = ((29^2)^2)^2 \equiv (841^2)^2 \equiv ((-7)^2)^2 \equiv 49^2 \equiv (-4)^2 \equiv 16 \pmod{53}$

Bob's value of $C_2 = KM = 16(33) = 528 \equiv$ **51 (mod 53)**

Y_A = **29** C1 = **15**, K = **16** C2 = **51**

Grading: 1 pt for writing 5^{22}, 2 pts for the calculation and answer
1 pt for writing 29^8, 2 pts for the calculation and answer
1 pt for writing 5^8, 1 pt for the calculation and answer
1 pt for writing 16 x 33, 1 pt for the calculation and answer

Can give full credit for a part if their answer is correct based on a previous incorrect answer.

4) (10 pts) Let C be the elliptic curve $E_{29}(11, 3)$. Two points on C are P = (8, 20) and Q = (19, 13). What is the result of adding P and Q? (The answer is a point on the curve.)

$$\lambda = \frac{13-20}{19-8} = (-7)(11^{-1} mod 29)$$

Use Extended Euclidean to find 11^{-1} mod 29:

29 = 2 x 11 + 7
11 = 1 x 7 + 4
7 = 1 x 4 + 3
4 = 1 x 3 + 1
4 – 1 x 3 = 1
4 – (7 – 4) = 1
2 x 4 – 1 x 7 = 1
2(11 – 7) – 1 x 7 = 1
2 x 11 – 3 x 7 = 1
2 x 11 – 3(29 – 2 x 11) = 1
8 x 11 – 3 x 29 = 1
Take this equation mod 29 to get
8 x 11 ≡ 1 (mod 29) so 11^{-1} ≡ 8 (mod 29)

It follows that $\lambda = (-7)(8) = -56 \equiv 2 \ (mod\ 29)$

x = 2^2 – 8 – 19 = 4 – 27 = -23 ≡ 6 (mod 29)
y = 2(8 – 6) – 20 = 4 – 20 = -16 ≡ 13 (mod 29)

P + Q = (**6, 13**)

Grading: 1 pt lambda set up
4 pts 11^{-1} mod 29 via EEA
1 pt get lambda
2 pts get x
2 pts get y

5) (10 pts) On the elliptic curve $E_{29}(11, 3)$, the following are results of several addition problems between points:

```
1.  ORIGIN   + (8, 20)  = (8, 20)
2.  (8, 20)  + (8, 20)  = (13, 9)
3.  (13, 9)  + (13, 9)  = (12, 23)
4.  (12, 23) + (12, 23) = (28, 7)
5.  (28, 7)  + (28, 7)  = (3, 18)
```

Using this information, determine the value of 20 x (8, 20). **Note: you will have to do some computation, but it's not an unreasonable amount.**

20 x (8, 20) = (16 + 4) x (8, 20)
= 16 x (8, 20) + 4 x (8, 20)
= (3, 18) + (12, 23), from statements above.
The values listed are 1 x (8, 20), 2 x (8, 20), 4 x (8, 20), 8 x (8, 20) and 16 x (8, 20).

Now, let's add these two points.

$$\lambda = \frac{23 - 18}{12 - 3} = (5)(9^{-1} mod 29)$$

Use Extended Euclidean to find 9^{-1} mod 29:

29 = 3 x 9 + 2
9 = 4 x 2 + 1

9 – 4 x 2 = 1
9 – 4(29 – 3 x 9) = 1
9 – 4 x 29 + 12 x 9 = 1
13 x 9 – 4 x 29 = 1
Take this equation mod 29 to get
13 x 9 ≡ 1 (mod 29) so 9^{-1} ≡ 13 (mod 29)

It follows that $\lambda = (5)(13) = 65 \equiv 7 \ (mod\ 29)$

x = 7^2 – 3 – 12 = 49 – 15 = 34 ≡ 5 (mod 29)
y = 7(3 – 5) – 18 = -14 – 18 = -32 ≡ 26 (mod 29)

20 x (8, 20) = (**5, 26**)

Grading: 4 pts to identify which 2 pts to add, 4 pts for lambda (1 pt set up, 2 pts mod inv, 1 pt complete), 1 pt x, 1 pt y

6) (1 pt) What is the first name of the founder of Papa John's Pizza? **John (Give to all)**