CIS 3362 Quiz #5: Public Key Encryption Solutions

Date: 11/14/2025

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 to Bob $3^{12} = (3^6)(3^6) = 729 \times 729 \equiv 16 \times 16 = 256 \equiv 8 \pmod{31}$

Bob sends to Alice $3^{21} = (3^{12})(3^9) \equiv 8 \times 19683 \equiv 8 \times 29 \equiv 232 \equiv 15 \pmod{31}$

Alice receives 15 from Bob and calculates $15^{12} = (15^3)^4 \equiv 3375^4 \equiv (-4)^4 \equiv 256 \equiv 8 \pmod{31}$ as their shared key.

Alice sends Bob: **8**   Bob sends Alice: **15**   Shared Key: **8**

Grading:

1 pt for listing 3^{12} mod 31, 2 pts for work calculating it (any reasonable breakdown is fine)

1 pt for listing 3^{21} mod 31, 2 pts for work calculating it (any reasonable breakdown is fine)

1 pt for listing either 15^{12}, 8^{21}, 3^{12*21} mod 31 for final key, 2 pts for calculation

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.)

First we must factor 493 via trial division. On the calculator, we find that 493/17 = 29. It follows that φ(493) = φ(17) x φ(29) = (17 – 1)(29 – 1) = 16 x 28 = 448.

It follows that d = 297^{-1} mod 448.

Let's run the Extended Euclidean Algorithm:

448 = 1 x 297 + 151
297 = 1 x 151 + 146
151 = 1 x 146 + 5
146 = 29 x 5 + 1

146 – 29 x 5 = 1
146 – 29(151 – 146) = 1
146 – 29 x 151 + 29 x 146 = 1
30 x 146 – 29 x 151 = 1
30(297 – 151) – 29 x 151 = 1
30 x 297 – 30 x 151 – 29 x 151 = 1
30 x 297 – 59 x 151 = 1
30 x 297 – 59(448 – 297) = 1
30 x 297 – 59 x 448 + 59 x 297 = 1
89 x 297 – 59 x 448 = 1

Take this equation mod 448 to get

89 x 297 ≡ 1 (mod 448)

It follows that d = 89.

Grading: 2 pts factoring 493
1 pt phi(493)
1 pt stating that we need 297^{-1} mod 448
2 pts Euclidean
3 pts Extended Euclidean
1 pt extracting correct answer
AUTOMATIC 0/10 if they do a gcd(493,297) or gcd(492,297)

3) (10 pts) Let the public elements of an El Gamal Cryptosystem be $q = 37$, $\alpha = 5$. 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.

$Y_A = 5^{22} = (5^5)^4 5^2 = 3125^4 \text{ x } 25 \equiv 17^4 \text{ x } 25 \equiv 83521 \text{ x } 25 \equiv 12 \text{ x } 25 \equiv 300 \equiv$ **4 mod 37**

Bob calculates $K = 4^{30} = (4^{15})^2 = (2^{30})^2 \equiv 11^2 = 121 \equiv$ **10 mod 37**

Bob sends $C1 = 5^{30} = 5^{22} \text{ x } 5^8 \equiv 4 \text{ x } 390625 \equiv 4 \text{ x } 16 \equiv 64 \equiv$ **27 mod 37**

Bob sends $C2 = KM = 10 \text{ x } 9 = 90 \equiv$ **16 mod 37**

$Y_A = \underline{\mathbf{4}}$, $K = \underline{\mathbf{10}}$, $C1 = \underline{\mathbf{27}}$, $C2 = \underline{\mathbf{16}}$

Grading: 1 pt expression Y_A, 2 pts simplify to 4

1 pt expression K, 1 pt simplify to 10

1 pt expression C1, 2 pts simplify to 27

1 pt expression C2, 1 pt simplify to 16

Give carry through credit if possible (so use their wrong value of K for C2 calc)

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.)

$$\lambda = \frac{3 \times 18^2 + 3}{2} = 975 \times 2^{-1} \equiv 14 \times 16 \equiv 224 \equiv 7\ (mod\ 31)$$

Note that $2^{-1} \equiv 16$ mod 31 since 2 x 16 = 32 ≡ 1 mod 31.

Note, we can alternatively do $\frac{975}{2} \equiv \frac{14}{2} \equiv 7\ (mod\ 31)$.

$$x_{2P} = (7^2 - 18 - 18) \equiv 49 - 36 \equiv 13\ mod\ 31$$

$$y_{2P} = (7(18 - 13) - 1) = 35 - 1 \equiv 34 \equiv 3\ mod\ 31$$

P + P = **(13, 3)**

Grading: 4 pts for lambda – 1 pt formula, 1 pt correct mod inverse, 2 pts answer
3 pts for x
3 pts for y, take off 1 pt if they put 34 (forgot to reduce mod 31)

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.)

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

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

Step 1
In class, we stored the message in the least significant bits of the x coordinate. Thus, our message x coordinate will be of the form q x $2^4 + 11$, where we try each possible value of q, starting with q = 0, until we find a value of x which has a solution for y.

We first try 0 x $2^4 + 11 = 11$.
Step 1 is to compute $c = 11^3 + 1 \times 11 + 1 = 1331 + 12 \equiv 0 \pmod{79}$.
Technically, in the posted code, although this value is a quadratic residue, our implementation did the following:

```
rem = pow(c, (self.p-1)//2, self.p)
if rem != 1:
    return None
```

So, for our implementation, we only consider values of x, which produce a value of c, which, when raised to the power (p-1)/2 mod p produce the value of 1. Thus, since 0 to any positive power will be 0, 11 fails.

Next, we try 1 x $2^4 + 11 = 27$.
Step 1 is to compute $c = 27^3 + 1 \times 27 + 1 = 19711 \equiv 40 \pmod{79}$.
Step 2 is to compute $c^{(p-1)/2}$, so 40^{39} mod 79, to see if this value is 1. Since this isn't in the chart, we can get pretty close by computing $40^{40} = (40^{20})^2 \equiv 44^2 \equiv 1936 \equiv 40 \pmod{79}$. It follows since $40^{40} = 40^{39} \times 40 \equiv 40 \pmod{79}$, that we can multiply this equation through by 40^{-1} to prove that $40^{39} \equiv 1 \pmod{79}$. This means that we have a matching value of y!!!
Step 3 is to compute the matching value of y. The matching y value must be $40^{(79+1)/4} = 40^{20}$ mod 79. Look this up on the chart to find that the matching y value is 44.

Plaintext Point = **(27, 44)**

Grading: 3 pts to obtain the correct x value of 27.
3 pts to plug in 27 into the curve equation to get 40.
3 pts to take 40 and exponentiate it to the right value to get 44.
1 pt to correctly fill in the point.
Note: I decided to accept (11, 0) even though it's not the point produced by my code.

6) (1 pt) By what acronym is the Public Key Encryption system created by Ron Rivest, Adi Shamir and Leonard Adelman known as? **RSA (Grading: give to all)**