CIS 3362 Final Exam - Part D (Public Key Crypto, Odds, Ends) - 25 pts Solution

1) (8 pts) Alice is using the El Gamal Cryptosystem. Her global public elements are:

q = 43 (prime number)
α = 12 (generator)

Alice's private key $X_A = 11$ and her posted public key is $Y_A = 26$.

Bob has sent Alice the following ciphertext: $C_1 = 40$, $C_2 = 20$.

Go through the process Alice would go through to recover the plaintext, showing your work and highlight the plaintext message Bob sent to Alice. **Please show your step by step work by hand for both modular exponentiation AND the Extended Euclidean Algorithm. (You can check individual steps with the calculator, but part of the points for the question are devoted to seeing if you know how to do these by hand.)**

Solution

When receiving a message, the first thing Alice should do is calculate K, as follows:

$K = (C_1)^{XA} \bmod q = 40^{11} \bmod 43$

To calculate this by hand we can rewrite it as:

$K \equiv (-3)^{11} \equiv -3^{11} \equiv -(3^4)^2(3^3) \equiv -(81)^2(27) \equiv -(5)^2(3^3) \equiv -25 \times 27 \equiv -675 \equiv 13 \pmod{43}$

The next step for Alice is to calculate $K^{-1} \bmod q$, so in this case $13^{-1} \bmod 43$:

$43 = 3 \times 13 + 4$
$13 = 3 \times 4 + 1$

$13 - 3 \times 4 = 1$
$13 - 3(43 - 3 \times 13) = 1$
$13 - 3 \times 43 + 9 \times 13 = 1$
$10 \times 13 - 3 \times 43 = 1$, take this mod 43 to get $10 \times 13 \equiv 1 \pmod{43}$, so $K^{-1} \equiv 10 \pmod{43}$

Now, we calculate the plaintext message as follows:

$M = (C_2 K^{-1}) \bmod q = 20 \times 10 = 200 \equiv$ **28 (mod 43).**

Grading: Writing down which modular exponent to calculate 1 pt.
Showing the hand/calculator calculation: 2 pts
Finding 13 inverse mod 43: 3 pts
Plugging in and simplifying to obtain M: 2 pts

2) (8 pts) The Elliptic Curve $E_{37}(4, 7)$ has points P = (20, 24) and Q = (32, 26). Determine the sum P + Q on this curve.

Solution

First find lambda: $\lambda = \frac{26-24}{32-20} = \frac{2}{12} = \frac{1}{6} (mod\ 37)$. This we must find 6^{-1} mod 37. Use the Extended Euclidean Algorithm:

37 = 6 x 6 + 1
37 - 6 x 6 = 1

Take this equation mod 37 to get

-6 x 6 ≡ 1 (mod 37), so $6^{-1} \equiv -6 \equiv 31 \pmod{37}$

Now, we solve for the x coordinate of the sum (x_R):

$x_R = \lambda^2 - x_P - x_Q = (-6)^2 - 20 - 32 = 36 - 20 - 32 = -16 \equiv 21 \pmod{37}$

Finally, we solve for the y coordinate of the sum (y_R):

$y_R = -y_P + \lambda(x_P - x_R) = -24 + (-6)(20 - 21) = -24 + 6 = -18 = 19 \pmod{37}$

It follows that the desired point is **(21, 19).**

Grading: 2 pts for lambda set up, 2 pts to solve for lambda, 2 pts to solve for x, 2 pts to solve for y

3) (4 pts) Alice and Bob have both set up their own RSA systems and want to use them for both encrypting messages and digital signatures. Both decided it would be easier to perform the double encryption if they both used the same public key n. What is the problem if they do this?

Solution

If Alice used the same n as Bob, then she would have to know its prime factorization to generate her own e and corresponding d. But, if she knew the prime factorization of n and she knew Bob's value of e (which is public), then she could use the Extended Euclidean Algorithm to calculate Bob's secret value d. Then, she could forge a message from Bob using his value of d and then Bob's digital signature would no longer be proof that he sent a message.

Grading: Full credit for any response that clearly explains that either Bob or Alice could forge the other's signature and why. Give partial credit if you think the student is on the right path but isn't clear with their explanation as you see fit.

4) (5 pts) The Universal Studios ride, E. T. Adventure is based on what feel good 1980s movie?

E.T., Give to All!