MATH 5347: APPLIED ALGEBRA WITH CRYPTOLOGY

Graded Homework 5 (50 points)

Kimberly Mandery

DUE 1600 181102

Instructions: This is a graded homework assignment worth 50 points. Solutions must be organized, neat in appearance, and must clearly indicate the answer to each problem. Be sure to show your work where appropriate.

1. (10 points) Use the Euclidean algorithm to find the greatest common divisor of $294,906$ and $178,549$. Also, find integer multiples of these numbers who sum is the gcd.

    1. 294906 = 178549(1) + 116357
    2. 178549 = 116357(1) + 62192
    3. 116357 = 62192 (1) + 54165
    4. 62192 = 54165 (1) + 8027
    5. 54165 = 8027 (6) + 6003
    6. 8027 = 6003 (1) + 2024
    7. 6003 = 2024 (2) + 1955
    8. 2024 = 1955 (1) + 69
    9. 1955 = 69 (28) + **23**
    10. 69 = 23 (3) + 0

    Thus our gcd is **23**.

    We can use the Extended Euclidean Algorithm found here to find the integer coefficients.

    1 = **2558**(294,906) **-4225**(178,549)

2. (20 points) Let $p = 19$, $q = 29$, and $e = 215$. Encipher the message $M = 15$ using the RSA scheme. Next, decipher your ciphertext to make sure you get 15 back.

    Step 1: Check Assumptions
    We need to check that e is appropriate. We can do this by calculating the $gcd(e,(p-1)(q-1))$ and hope that it is equal to 1. For $e = 215$, we get the $gcd(215, 18 * 28) = gcd(215, 504) = 1$. Since 215 and 504 are relatively prime, we can continue to step 2.

    Step 2: Encryption
    To compute our ciphertext c, we use the form $c \equiv m^e$ mod$N$. Plugging in our variables, we get $c \equiv 15^{215}$ mod551. To compute 15^{515}, we will use the online modular calculator found here. Our ciphertext becomes $c \equiv 280$ mod551. Thus $c = 280$.

    Step 3: Decryption
    We need to find a d such that $ed \equiv 1$ mod$(p-1)(q-1) \equiv 1$ mod504. To solve, we can use the Euclidean Algorithm.

    1. 504 = 215(2) + 74
    2. 215 = 74(2) + 67
    3. 74 = 67(1) + 7
    4. 67 = 7(9)+ 4
    5. 7 = 4(1) + 3
    6. 4 = 3(1) + 1
    7. 3=1(3) + 0

    Notice in step 6 we get a remainder of 1. This value corresponds to the gcd of 215 and 504 which is also 1. Neat. We can use the Extended Euclidean Algorithm mentioned in Exercise 1 to find the coefficients below.

    1 = (504)(-61) + (215)(143)

Step 4: Verification
To verify that this will give us $e = 215$ back, we use the fact that $e \equiv c^d \bmod N$. Thus we have $c \equiv 280^{143} \bmod 551$. Using the modular calculator from above, we verify that this $c \equiv 215 \bmod 551$.

3. (5 points) Typically the primes multiplied together to form the modulus for RSA are of about the same size. Explain why this might be.

   If the primes are of different sizes, then the smaller of the two primes could be easier to find and thus make the system more prone to attacks.

4. (15 points) Formulate a man-in-the-middle attack, similar to the attack described in Example 3.13 on page 126 for the RSA public key cryptosystem.

   Step 1: Alice publishes N and e.

   Step 2: Eve intercepts Alice's publication and changes N and e to N* and e* respectively.

   Step 3: Bob has a message m. He encrypts message m using $m^{e*} \bmod N \equiv c$. He sends the ciphertext c* to Alice.

   Step 4: Instead of c* going directly to Alice, Eve intercepts and decrypts c* using the keys N* and e* sent to Bob. This message is then encrypted using Alice's original keys, N and e, and sent as ciphertext c to Alice.

   Step 5: Alice decrypts c using N and e to get Bob's message m. Alice and Bob are none-the-wiser that Eve was listening in on their exchange.