CSIS 5857: Encoding and Encryption

Assignment 4: Public Key Encryption

Due Tuesday, March 30

These problems will give you experience different types of **public key encryption**, including RSA, Elgamal, and Diffie-Hellman, as well as potential vulnerabilities of these algorithms.

Please turn these in to the course **Blackboard site** using a **word processor** (such as Word), instead of hand-written form.

For these first three problems involving computation, you are required to **show your work** for full credit (however, do feel free to use a calculator for the exponentiation, of course!)

1. In a public key system using **RSA**, suppose that you intercept the ciphertext ***C*** = **10** sent to a user whose public key is ***E*** = **5**, ***n*** = **35**.

   a) What is the **private key *D*** of this user?

   Hint: Think about how ***D*** was created. In particular, consider:
   - What the primes ***p*** and ***q*** must have been.
   - What the totient **Φ** must have been.

   Here, $E = 5$.
   $n = 35 = 5*7$, so p = 5 and q = 7.
   So, $\Phi(n) = (5-1)*(7-1) = 4*6 = 24$.
   Now, $D = E^{-1}$ mod 24 = 5 because 5*5 = 25 = 1 mod 24. Thus, $D = 5$.

   b) What **plaintext message *M*** was sent?

   Now, $M = C^D$ mod $n = 10^5$ mod 35 = 5. Thus, $M = 5$.

2. Suppose that you are going to use **Elgamal** encryption to send me secure information, and that we have agreed to use **19** as the prime and **3** as the primitive root generator. Also suppose that my public $\mathbf{Y_A = 2}$.

   Also suppose that you will choose the **last digit of your Banner ID + 2** as your secret integer ***k*** (for instance, if your last digit is **9**, your ***k*** is **11**).

   Last digit of Banner ID = 1. So, key (k) = 3.
   We have $q = 19$, $\alpha = 3$, and $Y_A = 2$.

   a) What is your secret **one time key *K***?
   $K = Y_A^k$ mod $q = 2^3$ mod 19 = 8. So, $K = 8$.

   b) Suppose that you were to use this value of ***K*** to encrypt the **plaintext** message **10**. What is the corresponding **ciphertext**?
   Here, $M = 10$.
   So, $C_1 = \alpha^k$ mod $q = 3^3$ mod 19 = 8.
   And $C_2 = KM$ mod $q = 8*10$ mod 19 = 4.

3. Suppose that we are using **Diffie-Hellman** to create a secret shared key, using **71** as the prime ***p***, and **7** as the primitive root generator ***g***.

   Also suppose that you will choose the **last digit of your Banner ID + 3** as your secret integer ***x*** (for instance, if your last digit is **9**, your ***x*** is **12**).

   Last digit of Banner ID = 1. So, $x = 4$.
   We have $p = 71$, $g = 7$.

   a) Based on this, what number $\boldsymbol{R_1}$ would you send to me?
   $R_1 = g^x \bmod p = 7^4 \bmod 71 = 58$. So, $R_1 = 58$.

   b) Supposed that you received the number **54** from me as my number $\boldsymbol{R_2}$. What would you then compute for our shared key ***k***?
   $k = R_2^x \bmod p = 54^4 \bmod 71 = 25$. So, shared key, $k = 25$.

Unfortunately, Barney Fife is still in charge of your information security, and has a couple more bad ideas for "improving" encryption.

4. Barney wants to use RSA public key encryption to securely send **credit card numbers** from multiple locations to a central server. For this problem, assume all credit card numbers are **16 digits long**.

   Specifically, he would use RSA to encrypt a credit card number using the **public key** of the server, and then send that encrypted number to the server.

   You may assume that the server public key is well known, and that the encrypted message is being sent over an unsecured network (and may therefore be viewed by Darth).

   a) Why is this a bad idea? Specifically, if Darth intercepts the encrypted credit card number, how could he quickly determine the plaintext credit card number that it corresponds to?
   This is a bad idea because Darth could perform the Short Message Attack. For this attack, he would generate a table of all possible ciphertexts beforehand (10^{16} naively, or much less if only valid credit card numbers are taken). And when he intercepts the encrypted number, we would just compare it to his list of ciphertexts to find the match, and its corresponding plaintext (unencrypted credit card number).

   b) What is a simple way that you could have Barney modify this process so that he could still use RSA to send 16-digit credit card numbers, but to keep them secure from the kind of attack in part a)?
   A simple modification to make this process secure is to use Optimal Asymmetric Encryption Padding (OAEP) where additional (random) bits are padded to conceal the plain text. As a result, it becomes computationally infeasible for Darth to check all possible ciphertexts.

5. Suppose that Barney does not like modular arithmetic (he does not like things that are "mod"). He wants to use Diffie-Hellman to create secure keys, but wants to do so by just taking the secret numbers to the power of a known generator number.

   For example, suppose that you intercept the following exchange between Barney and Andy:

   Barney: We will use **3** as our generator α. My $\boldsymbol{R_1}$ is **27**.

   Andy: Ok. My $\boldsymbol{R_2}$ is **243**

a) What did Barney and Andy choose as their secret numbers?
We have, $g = 3$, R_1 is 27, and R_2 is 243.
Here, $R_1 = g^x$ and $R_2 = g^y$ (the "mod"s are omitted). So,
(Barney) $x = \log_g(R_1) = \log_3(27) = 3$, and
(Andy) $y = \log_g(R_2) = \log_3(243) = 5$.

b) What "secure" key ***k*** will they generate?
(Barney) $k = R_2^x = 243^3 = 14348907$.
(Andy) $k = R_1^y = 27^5 = 14348907$.

Additional problem for Graduate Students:

6. This question will involve **adding two points** on the elliptic curve $\mathbf{E_{13}(1, 1)}$ – in other words, the elliptic curve $\boldsymbol{y^2 = x^3 + x + 1}$ (that is, the one I used in my notes).

   The first point is **(11, 2)**.

   The second point depends on the last digit of your Banner ID:

Last digit	Point to add
0	(0, 12)
1	(1, 4)
2	(1, 9)
3	(4, 11)
4	(5, 1)
5	(5, 12)
6	(7, 0)
7	(8, 1)
8	(8, 12)
9	(10, 7)

For example, if the last digit of your Banner ID was **3**, you would compute the sum **(11, 2) + (4, 11)**.

You must also **show your work** to receive full credit on this problem.

Last digit of Banner ID = 1. So, we need to compute the sum (11, 2) + (1, 4).

Step 1: Since the x-coordinates are different, we will use equation from Case 1 to compute Δ.

$$\Delta = (y_Q - y_P)/(x_Q - x_P)$$
$$\text{or, } \Delta = (4-2)*(1*11)^{-1} \bmod 13$$
$$\text{or, } \Delta = 2*(-10)^{-1} \bmod 13$$
$$\text{or, } \Delta = 2*(3)^{-1} \bmod 13 \text{ (since } -10 = 3 \bmod 13)$$
$$\text{or, } \Delta = 2*9 \bmod 13 \text{ (since } 9*3 \bmod 13 = 27 \bmod 13 = 1)$$
$$\text{or, } \Delta = 18 \bmod 13 = 5.$$

Step 2: Compute $x_R = \Delta^2 – x_P – x_Q$.

$$x_R = 25 – 11 -4 \bmod 13 = 10.$$

Step 3: Compute $y_R = \Delta(x_P – x_R) – y_P$.

$$y_R = 5*(11-10) – 2 \bmod 13 = 3.$$

Thus, (11, 2) + (1, 4) = (10,3).