Fall 2021 CIS 3362 Homework #6: Public Key Encryption
Check WebCourses for the due date

1) In the Diffie-Hellman Key Exchange, let the public keys be p = 53, g = 12, and the secret keys be a = 24 and b = 43, where a is Alice's secret key and b is Bob's secret key. What value does Alice send Bob? What value does Bob send Alice? What is the secret key they share? Use a program or calculator to quickly simplify the modular exponentiations that arise, but show what each calculation is.

2) In an RSA scheme, p = 41, q = 17 and e = 543. What is d?

3) In Elliptic Curve Arithmetic what is the sum of the points (7, 9) and (15, 29) on the curve $E_{41}(3, 4)$?

4) In Elliptic Curve Arithmetic calculate 4 x (5, 12) on the curve $E_{41}(3, 4)$? (Note: This will require you to multiply by two twice.)

5) Consider an El Gamal cryptosystem with the prime q = 37 and the primitive root a = 18. Alice picks $X_A = 13$ for her secret key. What is the public key Y_A that Alice posts? Now, consider sending the message M = 31 to Alice. Give two different ordered pairs that you could send to Alice using her public keys to encrypt M. For each, write down which value of k you picked, the corresponding value of K, as well as the cipher text, the ordered pair (C_1, C_2). Use a program or calculator to quickly simplify the modular exponentiations that arise, but show what each calculation is.

6) Time to break a code! This was produced using RSA2BigInt.java. Here are the public keys for the system used.

```
Public key n = 276503917826766849902006184l
Public key e = 92253545271575760672283812l
```

Here is the ciphertext to decipher:

```
195038167899690250214751691
214171160422201655779853660 2
106654869321135983523765373 8
231720262266066246658832523 2
206983403668062601872605818 0
270792048632129421613463075 3
112373083172823378545343444
152241549204075536244924875 9
231871222174753878251146491 5
226794694796500193353843562 9
```

Each number represents a block of 19 uppercase letters.

Good luck!

Arup