**CS 4732/57322 Homework #5**

***Due electronically by midnight July 20th, 2020***.

For submission, if done on paper please scan and submit as a pdf. If done in word, please submit the .docx or .doc format.

**IMPORTANT**: Clearly indicate outside resources utilized and sign below. Failure to cite use of outside resources will be reported for appropriate disciplinary actions. Note that discussions with other students are encouraged; copying – with or without modifications – is unacceptable and will also be reported.

I discussed one or more problems with the following people:

I hereby certify that any outside resources utilized, other than the textbook and class materials, are clearly cited. All other material I provide for this homework submission is my own original work.

*Printed name*

1. (15 points) Briefly describe what the trap-door one-way functions are for RSA, Diffie-Hellman and ECC. In particular, what can we do easily and what is hard for each of them.

**Trap door function is a one way function that has an additional requirement. With a one way function, the type of function evalution is on the forward direction or in one direction that is the forward direction. The reverse directions becomes more complex and difficult. We add some additional requirement in the reverse direction the computation becomes simple and straightforward and it reveals an additional or trap door information.**

**You can also use the example of factorization and multiplication of two prime numbers. While the factorization of both numbers is easy the product is much more complicated and difficult. This is what RSA encryption uses.**

1. (10 points) You are sent a ciphertext message 9 sent to you using your public key using RSA. Your private key is e=5 and n=35. What is the plaintext number? Show all your work.
2. calculate Private Key

**ed = 1 mod (p-1) (q-1)**

**n= p x q = 35** = 5 x 7

(p-1)(q-1) = 4 x 6 = 24

5 x d = 1 mod 24

Here we get d =5 as 25 mod 24= 1

**Private key pair is { d , n } ={ 5, 35 }**

1. Now decrypt the Message i.e C = 9

P= C^d mod n

P = 9 ^ 5 mod 35

**P = 4**

3. (10 points) You see that someone’s RSA public key is (23,56153). You figure out how to factor 56153 into 233 and 241. Knowing this, tell me what that person’s public key is (if it actually exists). If there exists no valid private RSA key for this, then justify why that is the case.

Given public key

e=23

n=56153

Valid public key GCD(phy(n),e)=1

n=56153=233\*241

Phi(n)=232\*240=55680

gcd(23,56153)=1 so public key e is valid

Private key (d)

d\*e mod phi(n)=1

23\*d mod 55680=1

**d=19367**

4. (12 points) Alice and Bob are communicating private keys with each other using Diffie-Helman. They have decided on a prime of 11 and a primitive root of 2.

a) Show that these are at least somewhat valid by demonstrating that 2 is a primitive root of 11.

|  |
| --- |
| 21= 2 mod 11 =2 |
| 22= 4 mod11=4 |
| 23= 8 mod 11 = 8 |
| 24= 16 mod 11 = 5 |
| 25= 32 mod 11 =10 |
| 26= 64 mod 11 = 9 |
| 27= 128 mod 11 = 7 |
| 28= 256 mod 11 = 3 |
| 29= 512 mod 11 = 6 |
| 210= 1024 mod 11 = 1 |

**Since all the values are unique, we can conclude that 2 is a primitive root of 11**

b)Suppose Alice has a public key of 9, what is Alice’s private key?

**Private key of Alice (xa) = ?**

**Given public key (Ya)=9**

**9=2xamod11**

**Therefore xa=6**

**As 26 -> 64mod11=9**

**Alice’s private key is 9**

1. If Bob has a public key of 3, what is the overall secret key shared with Alice?

**Overall secret key can be calculated by k=(ya)xamodq**

**=(3)6mod 11**

**=3**

**Therefore Ya=3 which is bobs public key**

**Overall secret key shared is 3**

5. (6 points) You see on a website a file and an associated hash. You download the file and use the same hashing algorithm and you find that the hashes are equal. Should you feel secure? Why or why not?

**Yes,** I should feel secure. Every hashing algorithm produces a hash value (a fixed length unique string). This hash value is calculated based on some complex mathematical calculation (hash function) on the data (in binary format). The hash value of the same data using different hashing algorithms are different. The hash value displayed on the website should represent the actual information which indicates the file integrity. When the hash values (calculated and displayed) are same then it means, No modification of data has been happened while downloading the file and The file is not corrupted.