**CS 4732/57322 Homework #5**

***Due electronically by midnight July 21st, 2025***.

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.

Jamie Harris

*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 these encryption schemes.

RSA uses the fact that it’s easy to multiply two prime numbers together, but hard to determine what two primes multiply to get a given number

Diffie-Hellman uses the fact that it’s easy to take a number to a power mod some prime, but it is hard to find that exponent, ie a^x=y mod p, it is easy to get y given a and x, but hard to find x given a and y.

Elliptical curve cryptography uses the fact that it is easy to multiply a curve point by a scalar to get some new point, but it is hard to find the scalar given the initial and starting points. I.e. P=k\*G, where k is a scalar and P and G are points on a curve, it is easy to find P given k and G, but it is hard to find k given P and G.

1. (10 points) You are sent a ciphertext message 7 using your public key using RSA. Your private key is 5 and n=35. What is the plaintext number? Show all your work.

d=5 n=35 C=7

M=7^5 mod 35 = 7

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 you would need to calculate in order to find this person’s private key. It should be a simple equation in modular arithmetic, but you do not need to solve this equation.

φ(56153)=(233-1)(241-1)=55,680

e=23

d=e^(-1)=23^(-1) mod 55,680

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.

2^1=2 mod 11

2^2=4 mod 11

2^3=8 mod 11

2^4=5 mod 11

2^5=10 mod 11

2^6=9 mod 11

2^7=7 mod 11

2^8=3 mod 11

2^9=6 mod 11

2^10=1 mod 11

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

9=2^x mod 11 -> x=6

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

K=3^6=729=3 mod 11

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?

Just because the hashes are equal does not mean you can immediately feel safe. If the website or file has been the victim of a man-in-the-middle attack, the hash used could be changed, meaning you would have no way for sure of knowing that the file has not been tampered with.