Auburn University – Fall 2015
COMP 5730/6730
Instructor: A. Skjellum; TA: A. Ravipati
September 9, 2015

Note: "SHORT WRITE UPS" comprise 4-5 complete English sentences; diagram if helpful; bullet points OK too. Cite any sources (you can assume that we know you will read and reference the articles given below).

Start in-class, finish by Friday night, turn in via Canvas by 11pm on 9/11/15.

**All Students:**

1) SHORT WRITE-UP: Read about discrete logarithm (10pts)

https://en.wikipedia.org/wiki/Discrete_logarithm

Write a brief summary of how it works, and how you might use it; experiment with the prototype code provided.

How might this be relevant to encryption computations?

2) SHORT WRITE-UP: Read about Diffie-Hellman Key Exchange (20pts)

D-H allows for two parties with no prior knowledge of each other to establish jointly a shared secret key (e.g., a session key for symmetric key crypto) over an insecure channel.

https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange

a) Explain when this can work safely, when it will have limitations (see discussion of Eve in the article). Are there improvements?
b) Relate to the discrete logarithm
c) Why bother with public-key crypto if this works?

Another variation is Elliptic Curve Diffie-Hellman.

https://en.wikipedia.org/wiki/Elliptic_curve_Diffie%E2%80%93Hellman

Why is this different or better? Why is Elliptic Curve Crypto?

(3) Quick answers: Read about "Secret Sharing" (10pts)

https://en.wikipedia.org/wiki/Secret_sharing

a) Define it
b) When useful?
c) What limitations?

**Grad students (undergrads may do also for more points):**

4) SHORT WRITE-UP: Read about Montgomery multiplication (10pts):

http://www.hackersdelight.org/MontgomeryMultiplication.pdf
https://en.wikipedia.org/wiki/Montgomery_modular_multiplication

Write a brief summary of how it works, and how you might use it; experiment with the prototype code provided.

How might this be relevant to crypto computations?