CS 469’s Midterm Exam

Coverage: Handouts 1 – 9 and the slides on Malware; Book chapters 1, 3, 4, 8.

Format: I expect the exam to have 6 to 7 questions. There will be an emphasis on the material from Handouts 4-9 / Chapter 8 since we spent the most time discussing them in class. To this end, here are some tips:

- Make sure you understand the differences between encryption algorithms, cryptographic hash functions and digital signatures.

- Make sure you know the pros and cons of symmetric key vs. public key cryptosystems.

- For symmetric key cryptosystems, know the different basic ciphers and their weaknesses. Understand how AES works. Know the different modes of operation.

- For public key cryptosystems, know the underlying math – e.g., using the extended Euclidean algorithm to compute the multiplicative inverse of a number in $\mathbb{Z}_n$, using repeated squaring to compute the modular exponentiation of a number, etc. Expect to do some computation by hand. Make sure you know how the RSA and the Elgamal cryptosystems work.

- For cryptographic hash functions, know the properties they should have and their different applications. Understand the implications of a birthday attack. Know the Merkle-Domgad construction.

- For digital signatures, know how the RSA and Elgamal signature schemes work. (For the latter, there is no need to memorize.)