**CS4770 Midterm Fall 2022**

**Study Guide**

**1. Which standards body that is part of the Department of Commerce issues Federal Information Processing Standards?**

**2. What are the three elements of the C-I-A model?**

**3. What is the term for the ability to prove that you sent a message?**

**4. Give two examples of intrusion in a cybersecurity setting.**

**5. In order for a bug to be a vulnerability, it must have what two qualities?**

**6. Give an example of a symmetric encryption algorithm discussed in class.**

**7. Using a brute force attack, how many combinations of secret key would have you to try, on average, to break DES?**

**8. What is the name of the Dutch algorithm used as the Advanced Encryption Standard?**

**9. Give 3 properties of a good hash function.**

**10. Name the inventor(s) of public key cryptography.**

**11. Give the truth table for XOR.**

**12. Summarize the steps of AES.**

**13. List one of the top 6 certificate authorities.**

**14. What is 23^-1 mod 5?**

**15. Give twos examples of a way to perform a Denial-of-Service attack.**

**16. How do you produce a digital signature for a message?**