**MIS 6330: IT Security**

**Individual Homework 2**

**(Write in your own words. Do not copy/paste from online resources or the text. This is an individual assignment, so if I receive identical answers, I will treat them as instances of academic dishonesty.)**

1. How many secret keys are required for two people to communicate via a *symmetric* cipher? In the case of *stream* cipher, what is this key used for?
2. What is a *message authentication code*? Can a *digital signature* be used as a *message authentication code*?
3. Which property of a *secure hash function* is critical to implementing *digital signature*? Explain your choice.
   1. One way
   2. Weak collision-resistance
   3. Strong collision-resistance
4. How can you use a *public-key* cryptosystem to exchange a *secret key*?
5. Check Amazon’s *public-key certificate*. List some of the details you can find out about it, e.g., *certification authority* (CA) and Amazon’s *public key*. In Chrome, you can use Developer tools and then select the Security tab to view your certificate.

