Networks and Distributed Systems **Homework 10**
CS3700 Fall 2022

This homework is due at 11:59:59 PM on December 12, 2022 and is worth 3% of your grade.

Name: _____

NUID (with leading zeros): _____

Problem	Possible	Score
1	25	
2	15	
3	15	
4	30	
Total	85	

1. Using your web browser, analyze the TLS certificate for `https://www.bankofamerica.com`.

1a. Who signed the certificates in this chain? How many certificates are there in the chain to the root? (5 pts)

1b. On what other domain(s) besides www.bankofamerica.com is this certificate valid (hint: look at the Subject Alternate Names field of the certificate)? (5 pts)

1c. When will this chain no longer be valid? How do you know? (5 pts)

1d. What public key encryption algorithm did Bank of America use to generate their public/private key pair? How many bits is the key size? (5 pts)

1e. What distinguishes a root certificate from other TLS certificates? (5 pts)

2a. Suppose that using your web browser, you connect to a HTTPS web site where the root certificate in the chain is not in your browser's trust store. What should happen? (5 pts)

2b. Sometimes it is necessary to use untrusted self-signed certificates in practice. When might this be the case? What security guarantees would doing this provide? (5 pts)

2c. Suppose you are an attacker, and during a break-in, you discover that you can obtain either the private key corresponding to Bank of America's certificate, or the private key corresponding to the root CA certificate that signed Bank of America's certificate? Given that you are an attacker, which would you pick to download and why? (5 pts)

3. There are online tools that let you measure the TLS implementations used by websites. These tools tell you whether a given website's TLS implementation is vulnerable to specific security problems; whether they are following best practices; etc.

For the next set of questions, we will use the testing tool provided by Qualys that is available at `https://www.ssllabs.com/ssltest/`. Open the Qualys testing tool in two tabs: in one tab, analyze `fidelity.com`, in the other tab analyze `cbw.sh`. If Qualys says multiple servers are available for Fidelity, you may choose any available server.

3a. Qualys grades the security of Fidelity as a "F", while cbw.sh gets an "A+". Explain **one** reason why cbw.sh gets a better grade than Fidelity. What is the problem area, and why is it a problem? (10 pts)

3b. cbw.sh supports HSTS and HSTS preloading, whereas Fidelity does not. What is HSTS and HSTS preloading? What security problem is HSTS meant to address? (5 pts)

4. Recall the RSA Algorithm from the Transport Layer Security Lecture.

Consider the two prime numbers $p = 23$ and $q = 17$ and your encryption exponent, $e = 3$. Make sure to show all of your work.
Hint: *Writing out the equations should help.*
Hint: *Use the Python Interpreter, or tool that supports arbitrary precision calculations, e.g., dc, to help find solutions to the problems below.*

4a. Compute the decryption component $\boldsymbol{d}$. (10 pts)

4b. Encrypt $M = 4$ (10 pts)

4c. Decrypt $C = 2$ (10 pts)