HW 3

ECE 356/ COMPCSI 356: Computer Network Architectures:

Homework must be done individually. The homework is due at 11:59pm on 04/26/2024. Please submit your solutions as a single PDF file via Gradescope. Show all steps of your derivations.

1. (**TCP attacks**, **3 pts**) This question is about SYN flooding attack.

a. In the SYN flooding attack, why do we randomize the source IP address instead of using the same source IP address? (**1 pt**)

b. What happens if the spoofed source IP address in a SYN flooding attack does belong to a machine that is currently running? (**2 pts**)

2. (**DNS and attacks**, **5 pts**) This question is about DNS and attacks to it.

a. Please use the dig command (dig duke.edu) to get the DNS server information about duke.edu (a screenshot of the results is fine) (**1 pt**)

b. What is DNS cache poisoning attack? (**2 pts**)

c. What are the fundamental problems of the DNS protocol that make it vulnerable to cache poisoning attacks? (**2 pts**)

3. (**SSL/TLS**, **2 pts**)

a. AES is a block cipher. Can we use it as a stream cipher? How? (**1 pt**)

b. Is the hash function f(x) = x mod 2024 a cryptographic hash function? Why? (**1 pt**)