Extra Q1 (Not in Class) (Diffie-Hellman): Let $p = 11$. Let $g = 10$. Compute $g^1 \mod p$, $g^2 \mod p$, $g^3 \mod p$, …, $g^{20} \mod p$. Also compute $g^{5000} \mod p$. Don’t use a calculator or computer.

Extra Q2 (Not in Class) (Diffie-Hellman): Let $p = 11$. Let $g = 3$. Compute $g^1 \mod p$, $g^2 \mod p$, $g^3 \mod p$, …, $g^{20} \mod p$. Also compute $g^{5001} \mod p$. Don’t use a calculator or computer.

Extra Q3 (Not in Class) (Diffie-Hellman): Let $p = 11$. Let $g = 7$. Alice’s private key is $x=3$. Bob’s private key is $y=8$. What is their shared key?

Q1: Why or how might a user visit a bad website like attacker.com?

Q2: Consider a website site.com that includes a third-party script, e.g.:

<script src="http://otherdomain.com/library.js"></script>

From what origin can this script read cookies?

If this script sets a cookie, under what origin will that cookie be set?

Do you see any security concerns with this?