CSE 484 In-Class Worksheet #14 – Autumn 2018
Name: _____ UWNetID: _____ Date: _____
Email address: _____
Partner names for this activity: _____
Will you want to pick up your worksheet later? Circle one: Yes / No

Q1 (RSA): Given these RSA parameters: p=5, q=7, e=5

What is N?

What is $\phi(N)$?

What is d?

Given these parameters, encrypt 16.

Given the parameters, decrypt 12.

Q2: Why or how might a user visit a bad website like `attacker.com`?

Q3: 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?