Chritopher LaJon Morgan

Oct 23, 2013

Homework 9 CS 465

**Weak RSA Moduli bug**

Earlier this year, researchers reported flaws in the public keys in certificates on the Internet. Here is an excellent blog post on the issue, with pointers back to the original two articles that discuss the problem.

<http://dankaminsky.com/2012/02/17/primalfear/>

Read the blog article and write a 1/2 page summary on what you learned. This article refers to many of the topics we have been learning about in RSA and certificates.

Ideas of questions you might answer in your brief response:

* What is the error that was discovered?
* How serious is the problem in practice?
* What lessons did you learn from this incident?
* What questions arose from your reading of the article?