

COSC 6397 Computer and Network Security

Computer Science Department, University of Houston, Instructor: Rakesh Verma

Spring 2009, Homework 2, Due April 29, 2009 at 1pm.

Keep an organized Excel log of the time spent on each problem, and turn it with the homework.

1. In not more than 2 pages, discuss the details of SHA-2 family of algorithms. Choose one of the options such as SHA-256.
2. Read the paper, “Why Johnny can’t encrypt?” by A. Whitten. Among the reasons - for Johnny’s inability to encrypt - cited by the author, list the top three in your opinion.
3. Read the paper “Know Your Enemy: Sebek2” and prepare two summaries of the article. One summary should consist of sentences from the article and contain exactly 100 words (chop last sentence if necessary). The other summary should be in your own words and also exactly 100 words. Should such articles be posted on the internet? Justify your position in at most half a page. Email only the summaries to me as *plain text* files by the deadline - send only one email with subject line: Hw 2 Question 3. Make sure to put your name and label the summaries in the text files.
4. In no more than 6 sentences discuss the limitations of a firewall.
5. What are rootkits? How can a Windows user protect against rootkits? Explain in no more than a page.
6. SSL, IPsec, and SSH have all adopted different policies for message integrity and confidentiality. Depict these policies as a table of 3 rows. Are they all equivalent in terms of security properties? Explain.

Academic Honesty Policy: No collaboration with anyone or anything in or outside the course is allowed on any homeworks, exams and programming assignments (yes, that excludes the internet as well) except if it is **explicitly allowed** on a problem. The *appropriate* help of the instructor and (if applicable) the TA is of course allowed and encouraged.