

COSC 6397 Computer and Network Security

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

Spring 2008, Homework 2, Exercises 1-5 due Friday Mar. 14 by 5pm via email

Keep an organized Excel log of the time spent on each problem, and turn it in as part of the zip archive.

1. In an RSA system, the public key of a given user is $e = 31$ and $n = 3599$. What is the private key of this user?
2. Make a list of known attacks on RSA. Briefly explain each. Limit - 1 page.
3. Design a version of Diffie-Hellman Key exchange protocol that is resistant to the Man-in-the-middle attack described in class or text. Explain how your version resists the attack.
4. In not more than 2 pages, discuss the details of SHA.
5. Read the paper, “Why Johnny can’t encrypt?” by A. Whitten.
 - (a) Make a list of this paper’s criticisms that are still valid for the version of PGP you downloaded in Homework 1. Make a second list of criticisms that have been addressed in your version. State the version you are using as the first line of your answer.
 - (b) Create a public key/private key pair for yourself using PGP if you have not done so already. Send your public key in ASCII-armored format to me with the subject line: My public key.
 - (c) Send an encrypted, signed email to me with the subject “PGP is pretty good” to me. In the body of the message include: (i) operating system and version of PGP you are using, (ii) any public keys you found for me; PGP fingerprint is sufficient. Your mail should be protected so that only I can obtain the plaintext content. You must also sign the message with your private key. Make sure that you get it right the first time, since only your first email to me will be accepted. Are you able to finish the assignment in fewer than 90 minutes as in Whitten’s experiment?

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.