CS 4235 / CS 8803IIS Homework 3

Assigned: 28 February 2011
Due: 9 March 2011, 5:00pm Atlanta time. Students submitting solutions after that time but by 5:00pm Atlanta time on 11 March will have their scores scaled by 0.8. No solutions will be accepted after 5:00pm on 11 March.
Teaming: Work individually.

Solutions should be typewritten and submitted as a PDF file on T-Square. Be sure to include your name and GTID number on your submission. Scores will be posted on T-Square.

Although you may use outside sources for information, you:

- **must not** copy-and-paste text or figures from those sources, and
- **must** cite the sources. A citation should provide sufficient information for myself or anyone else to find the source that you used.

You do not need to cite the textbook or any course materials. If you are unsure whether or not you are using outside material appropriately, please ask me rather than guessing.

This homework has one written part worth 190 points. Please solve the following problems.

Written exercises

1. From Chapter 2:
   (a) (10 points) #32.
   (b) (5 points) #34.
2. From Chapter 3:
   (a) (10 points) #4.
   (b) (10 points) #14.
   (c) (15 points) #15.
3. From Chapter 7:
   (a) (5 points) #19.
   (b) (10 points) #27.
   (c) (15 points) #29 (list at least three).
   (d) (10 points) #38.
   (e) (10 points) #40.
   (f) (10 points) #64.

4. (20 points) Explain how an attacker could convert each of the following into a covert channel:

   (a) Spam email

   (b) Non-spam email

   (c) Images in Facebook

   (d) The directory of temporary files on a system

5. (20 points) An RSA key modulus must be large to prevent an attacker from computing the private key. Suppose Alice publishes a public key of $\langle 23, 18721 \rangle$. What is Alice's private key? Explain how you determined your answer.

6. (30 points) Even strong cryptosystems will fail when improperly used. Let Alice communicate with Bob using RSA. Bob publishes a public key $\langle e, n \rangle$ where n is large and cannot be easily factored. Alice converts each character in her message into a number as follows:

   $$A \to 0, B \to 1, \cdots, Z \to 25$$

   She then encrypts each character using Bob's public key and transmits the sequence of encrypted characters to Bob over a public channel.

   (a) Suppose Trudy observes the encrypted traffic. Explain how she can easily recover the plaintext message even without knowledge of Bob's public key.

   (b) Let Bob's public key be $\langle 65537, 633716677687 \rangle$. Decrypt the message

   233693858096 193958983283 432441959920 609908539402

   504368733985 49228377800 611329886849 606386987048

   1 163738436281 284245269089 462695579160 17328906363

   191328218008 284245269089 119466115470.

   Give the decrypted message and explain how you performed the decryption. (Hint: There are at least three different ways to answer this question. A short computer program might be helpful.)

7. (10 points) A protocol for efficient, secure data transmission across a network needs to both encrypt and compress data. Should the protocol encrypt-then-compress, or compress-then-encrypt? Justify your response.