H6: Crypto Homework

INSTRUCTIONS: Read the selections from The Code Book p. 251 - 276. To see which selections, see the front cover of the book at the supplemental readings (read at least those selections in between p. 251 and p. 276). I copied a lot more in case you are interested in reading more. Then discuss the following issues.

1. Discuss the "key distribution" issue.
2. Contrast "asymmetric" keys to "symmetric" keys.
3. Describe the "padlock analogy".
4. What is the history of the RSA method? (as an **extra**, if you would like to, contrast this with the "alternate history" appearing on p. 279,280,289,290).
5. What is a "public" key? And what is a "private" key?
6. Multiplication, as discussed on p. 276, is "one-way". Come up with some other functions, operations, procedures, etc which are "one-way" (this need not be mathematical; e.g. breaking a cup is "one-way").