Homework 3

Due Date: February 20, 1998 at 11:59PM **Points**: 150
Late Date: February 23, 1998 at 11:59PM (20% penalty)

1. (*10 points*) One author has stated that the four key concepts of security are preventing interruption, interception, modification, and fabrication. Are these concepts equivalent to the three discussed in class (preserving confidentiality, integrity, and availability)? If so, which ones; if not, is there any relationship between the sets of concepts?
2. (*10 points*) The Morris-Thompson scheme with the n-bit random numbers was designed to make it difficult for an intruder to discover a large number of passwords by hashing common strings in advance. Does the scheme also offer protection against an attacker who is trying to guess one particular user's password on his or her machine?
3. (*20 points*) Many public key cryptosystems can provide both authenticity and confidentiality. But we usually think of classical (secret key) cryptosystems as providing only confidentiality. How can a classical cryptosystem provide authentication of a user instead of confidentiality of a message?
4. (*20 points*) In the UNIX file system, could a mandatory access policy be defined so that a user has access to a file. only if the user has access to all subdirectories higher (closer to the root) in the file structure? What would be the effect of this policy?
5. (*20 points*) Consider the following protection mechanism. Each object and each process is assigned a number. A process can only access an object if the object has a higher number than the process. Which of the mechanisms discussed in class (ACL, capabilities, lock-and-key, the MULTICS ring protection scheme) does this most closely resemble, and why? In what essential way does it differ from the scheme discussed in class?
6. (*20 points*) A problem with segmented and paged address translation is I/O. Suppose a user wishes to read some data from an input device into memory. For efficiency during data transfer, often the actual memory address where the data is to be placed is provided to the I/O device. The real address is passed so the time-consuming translation does not have to be performed during a very fast data transfer. What security problems does this approach bring?
7. (*10 points*) Does the system of all subsets of a finite set, under the operation "subset of" ($\subseteq$) form a lattice? Why or why not?
8. (*20 points*) Suppose a Kasiski analysis identifies the following pairs of repeated sequences: (10, 34), (21, 62), (37, 109), (49, 105), (58, 162), and (72, 132). What can you conclude about the number of alphabets used to encipher this message? What additional information about the pairs would be useful? Explain your answer.
9. (*20 points*) The following function is to open the file named *filename*, and read *lengthline* characters into the array *line*. It then returns the file pointer to the opened stream. Please identify any non-robust programming practices in this routine, and fix them.

```
FILE * read1stline(char line[], int lengthline, char *filename)
{
          int c;      /* input character */
          int i = 0;  /* counter in a for loop */
          FILE *fp;   /* pointer to open file */

          /* open the file */
          fp = fopen(filename, "r");
          /* read the first line, or up to EOF, whichever comes first */
          while((c = getc(fp)) != EOF && c != '\n' && i < lengthline)
                line[i++] = c;
          /* smack on a nul byte */
          line[i] = '\0';
          /* return the file pointer */
          return(fp);
}
```