

Homework #1

Due October 7, 2011, beginning of the class

1. Problem 2, page 92, from the textbook.
Token cards display a number that changes periodically, perhaps every minute. Each such device has a unique secret key. A human can prove possession of a particular such device by entering the displayed number into a computer system. The computer system knows the secret keys of each authorized device. How would you design such a device?
2. In the structure of DES, discuss each of the following:
 - Feistel structure: Why is it significant?
 - Confusion and diffusion: What are these? How are they obtained in DES?
 - Expansion: Why is it needed? Why is it significant?
 - Key schedule: Why may such a simple key schedule be preferable? (For example, instead of filling a key table by a more complex function at cipher initialization, as in RC5 or Blowfish?)
3. Question 2, the midterm exam of Fall 2005.