**MIS 6330: IT Security**

**Prof. A. Lahiri**

**Individual Homework 3**

1. Assume that passwords in a system are limited to the use of 95 printable ASCII characters and that all passwords are 10 characters in length.
   1. How many different passwords are possible? Hint: for each character in the password, there are 95 possible choices. So, as far as 2 character long passwords are concerned, you have 95x95 choices.
   2. Consider a computer with an encryption rate of 3.2 million encryptions per second (i.e., it can compute 3.2 million hash values in one second). How long will it take to crack all possible passwords using this computer in the event the password file is compromised? Assume that the system is not using any salt values and the users are not using dictionary passwords.
2. Now, suppose that there are only 3 users in the system and each user has a different salt value (stored as plaintext in the password file). If the same computer as the one above is used, how long will it take to crack all three passwords? Does using salts help even when they are stored in plaintext and therefore immediately visible to the hacker upon a successful attack on the password file?
3. For this question, assume the following: The system does not impose any restrictions on the password length. As a result, the users are able choose short passwords, and they always choose 6 characters or less. The hacker knows this and proceeds accordingly. How does this change the time the hacker needs to crack all 3 passwords? Continue to assume that each user uses a different salt.
4. For this question, assume the following: The system does not check passwords against a dictionary when they are first chosen. As a result, the users are able choose dictionary passwords. The hacker knows this and proceeds accordingly using a large password dictionary containing 1 billion passwords. How does it change the time the hacker needs to crack all three passwords? Continue to assume that each user uses a different salt.

\*\*\* Use a proper time unit for each part above. For example, 0.05 years make much less sense than 18 days. Likewise, 11.5 days is much easier to understand when compared to 1 million seconds.