**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. **9510 (59,873,693,923,837,890,625)** passwords are possible.
   2. **593,307** years (approximately) will be required to crack all **9510** passwords using this computer if password file gets compromised.

Above value was found by dividing 9510 (total passwords) with 3.2 million (max. capacity to compute hashes per second) to get time in seconds and then, converting it into years.

1. It’d take **1,779,921** years (aprproximately) to crack all 3 passwords.

Adding salt to the password helps as:

* The attacker is required to append the salt to every possible password (i.e **9510** passwords) and find the hash value for it, to match exactly with the one stored in password file for each user.
* This would mean that even at the end of trying all passwords with one hash, the attacker will be able to crack only one password.
* Since here, there are **3** distinct salt values, so the attacker will do the same process as above **thrice**. Due to this, time required to crack all passwords is almost **thrice** than the time required to crack password as in question 1.
* For a system with **n** distinct salt values, the attacker will do the same process roughly **n** times to crack all the passwords.

1. The attacker would approximately need following amount of time to crack all 3 passwords:
   1. 1 character + salt – **89 microseconds**
   2. 2 characters + salt –**8 milliseconds**
   3. 3 characters + salt – **0.8 seconds or (80 milliseconds)**
   4. 4 characters + salt – **76 seconds**
   5. 5 characters + salt – **2 hours (or 121 minutes)**
   6. 6 characters + salt – **7.97 days (or 191 hours)**
2. If the users’ have used dictionary passwords, attacker will be able to crack all 3 passwords in **15.62 minutes (or 938 seconds)** approximately.