CSE 565 Solution to Homework 4

1. (25 points total; 10 points for (a) and (b) and 5 points for (c))

   (a) The mask corresponds to the maximum set of permissions that users from the owner's group (except the owner), named users, and named groups (but not others) can have. When the mask is not explicitly set, the default value is computed as the union of the permissions of the owner's group, named users and named groups (modifying permissions of others can, however, change the mask).

   (b) i. The permissions are exactly as set: the owner has `rw`, `abc` has `rw`, the owner's group has `r`, and others have no permissions.

   ii. Now the mask affects all users and groups except the owner and others; the permissions are: the owner has `rwx`, abc has `x`, the owner's group has `x`, and others have no permissions.

   (c) The command will need to use `-d` or `d:` options to set the default value. For the given example, the following will work:

   ```
   setfacl -m d:u:abc:rw dir
   ```

   Setting any default value will result in default values for the owner, group, and others to be set as well. To ensure that permissions are as expected for all types of users, it might be desirable to specify them all, e.g.,

   ```
   setfacl -m d:u:abc:rw,d:u::rwx,d:g::r,d:o::- dir
   ```

2. (35 points total; 8 points for the logic in (a)–(c), 14 points for the logic in (d), 5 points for the logic in answering parts (3) and (4), and 2 points each for computing numbers in (a)–(d) correctly)

   (a) There are the total of $127^6 + 127^7 + 127^8 \approx 6.8 \cdot 10^{16}$ passwords of this form and $127^6 \approx 4.2 \cdot 10^{12}$ passwords of the shortest length. Testing them all (with 100% success) takes about 6821230597 seconds or about 216 years, while testing the shortest passwords takes 419587 seconds or almost 5 days.

   (b) The total number of characters that can be used in a password are $26 + 26 + 10 = 62$. Therefore, the total number of passwords is $62^6 + 62^7 + 62^8 \approx 2.2 \cdot 10^{14}$ and $62^6 \approx 5.7 \cdot 10^{10}$ passwords of the shortest length. Testing all of them takes about 22,191,852 seconds or about 257 days, while testing the shortest passwords takes 5680 seconds or slightly more than 1.5 hours.

   (c) When passwords are comprised of only digits, there are only $10^6 + 10^7 + 10^8 = 1.11 \cdot 10^8$ possibilities and 10^6 possibilities of the shortest size. Testing all of them can be accomplished in about 11 seconds, while testing the shortest passwords takes only 0.1 second.

   (d) We know that there are 52 choices for the first password character. The rest of the password can be comprised of letters and digits so that that the number of digits is at least one and at most the length of the password minus one, and the digits can be at any positions in the password. This gives us that for 6-character passwords, characters $2 - 6$ can contain any combination of letters and digits except that they all cannot be letter. This gives us the total of $52(62^5 - 52^5) \approx 2.8 \cdot 10^{10}$ possibilities. By computing the number of 7-character and 8-character passwords in a similar fashion, we obtain that the total number of passwords is $52(62^5 - 52^5 + 62^6 - 52^6 + 62^7 - 52^7) \approx 1.3 \cdot 10^{14}$. Testing all

of them takes about 13,161,764 seconds or 152 days, while testing the shortest passwords takes 2787 seconds or less than an hour.

3. (30 points total; 10 points each)

   (a) Since there are only 2^{12} possible salt values, in a system with 2^{24} users many salt values will occur more than once. This means that running the dictionary attack against all users will succeed in 2^{12} runs of the original dictionary attack (2^{12} time units).

   (b) The time needed to run a dictionary attack strongly depends on the permitted length of passwords. The question doesn't contain enough information to determine how much longer the dictionary attack against a single user becomes in this case (but it will certainly increase), and the new time for the dictionary attack is treated as a modified time unit. Then the dictionary attack against 2^{24} users will succeed in 2^{12} modified time units.

   (c) Now there are 2^{24} possible salts. Since each salt is chosen uniformly at random, the 2^{24} users will utilize most of the 2^{24} available salts. This means that the dictionary attack against all users will take close to 2^{24} time units.