

## Experimentation and Methodology: -

The algorithm generates passwords based on the information provided by the user like their first name, last name, date of birth, and father's name. After the generation each password is tested by the algorithm that how strong each password is, and a score is provided to the password according to its strength tested by the algorithm.

The password strength estimation algorithm tests the algorithm against various methods used by the attackers to crack the password.

- First the algorithm checks the length of the password, whether its 6 characters long or more than that.
- Then the algorithm checks if the password contains any commonly used words that are generally used by majority of users while creating a password and a score is provided according to the test.
- Then the algorithm checks whether the password contains the information of the user without encrypting it in some way or how much the password is predictable based on the information provided by the user.
- Then the password is checked against brute-force attacks i.e., how much time would it take to crack the password.
- After the brute-force attacks, the randomness of t+he password is checked, checking how predictable can the password be based on how many times a character is repeating in the password.
- Each step provides a relative score to the password and based on the score the password is rated as Easy, Moderate or Hard.

The demonstration of above steps is as follows: -

First Name:

Last Name:

Age:

Date of Birth:

Father's Name:

Do you want to enter your own password?

☐ Yes

☒ No

Generated Passwords:

Password:- kAr030 Score:- -6 'Bad'  
Password:- <vkA200 Score:- -5 'Easy'  
Password:- Kc3r@V;2 Score:- -19 'Hard'  
Password:- =}3a0VAf Score:- -11 'Moderate'

After estimating the strength by the program algorithm, a survey is taken to see how each password is usable and user-friendly with respect to different users as different users can have different opinions on the same password. To do so a sample space of 60 passwords is generated and each password is first estimated by the machine. In the survey, every participant is asked to rate the passwords generated by the algorithm as Easy, Moderate or Hard as they see fit in terms of how easy it is to remember the password and how good the password will be if the users want to use them as their password.

Based on the survey it is observed how well a password performed with respect to different users.