IVs:

* Filter type
* Password type
* Entry number

DVs:

1. Levenshtein distance (usability task 1) - how close the entry and the actual password are
2. Entry time (usability task 1) - time taken to enter the password
3. Distance to typo (usability task 2) - distance between where the user has put the x and where it should have been
4. Editing time (usability task 2) - time taken to add the x
5. Levenshtein distance (security) - how well they performed in the shoulder surfing task

## A. Levenshtein distance (usability task 1)

* Interaction between filter type and entry number (p<0.05). ([report](https://drive.google.com/open?id=0BwxIc9E2K1b4SnhnMWgwbFVhVEE))
  + Looking into first entries only, we found the following ([report](https://drive.google.com/open?id=0BwxIc9E2K1b4MU1GWC16MlpLSFk)):
    - Filter type:
      * Significant effect of filter type (p=0.037 i.e. p < 0.05)
      * None of the pairs were significantly different
    - Password type: no evidence of significant effect of password type on Levenshtein distance
  + Looking into second entries only, we found the following ([report](https://drive.google.com/open?id=0BwxIc9E2K1b4OTZiYVBkNEZMWFE)):

## B. Entry time (usability task 1)

* Significant effect of password type on entry time (p < 0.001). ([report](https://drive.google.com/open?id=0BwxIc9E2K1b4Q0I3RDc3ZGRXdUU))
  + Pairwise comparisons using Bonferroni correction show significant differences between all pairs. → report mean and standard deviation of each condition in the paper. This means that more complicated passwords take longer times to enter. This result is obvious but you can report it and say that the expected results mean that your setup was correct.
* Significant effect of entry number on entry time (p < 0.001). ([report](https://drive.google.com/open?id=0BwxIc9E2K1b4Q0I3RDc3ZGRXdUU))
  + Pairwise comparisons using Bonferroni correction show significant differences between all pairs. → report mean and standard deviations. This means that there is a *learning effect* i.e. people enter passwords faster across all conditions.
* Interaction between password type and entry number. ([report](https://drive.google.com/open?id=0BwxIc9E2K1b4Q0I3RDc3ZGRXdUU))
  + We can look deeper into this to find that, for example, the learning effect is steeper with certain password types and marginal with the others. From the means, it seems that for password types 1 and 2, the learning effect is stronger.
* Check the graphs in the [report](https://drive.google.com/open?id=0BwxIc9E2K1b4Q0I3RDc3ZGRXdUU)

## C. Distance to typo (usability task 2)

* Significant effect of filter type on distance to typo (p < 0.001). ([report](https://drive.google.com/open?id=0BwxIc9E2K1b4VkhuUEdsbVVrMzg))
  + Significant differences between
    - Filter 1 vs filter 3 (p<0.001)
    - Filter 1 vs filter 4 (p<0.005)
    - Filter 2 vs filter 3 (p<0.001)
    - Filter 2 vs filter 4 (p<0.005)
    - Filter 3 vs filter 5 (p<0.001)
    - Filter 3 vs filter 6 (p<0.001)
    - Filter 4 vs filter 5 (p<0.001)
    - Filter 4 vs filter 6 (p<0.005)
    - Show the means and standard deviations in a table along with the p values. Interpret the results in the discussion section of your paper.
* Significant effect of password type on distance to typo (p < 0.05). ([report](https://drive.google.com/open?id=0BwxIc9E2K1b4VkhuUEdsbVVrMzg))
  + No significant differences between any pairs (p > 0.05)
* Interaction between filter type and password type (p < 0.01). ([report](https://drive.google.com/open?id=0BwxIc9E2K1b4VkhuUEdsbVVrMzg))
  + This means that if we dig deeper, we might find that one a filter results in a shorter distance to the typo based on the password type.
  + By looking at the graphs (password\_type \* filter\_type), it seems that in password type 3, the distance to the typo is closer when using filters 1 and 2, than when using the asterisk
* Interaction between password type and entry number (p < 0.01). ([report](https://drive.google.com/open?id=0BwxIc9E2K1b4VkhuUEdsbVVrMzg))
  + Not really interesting

## D. Editing time (usability task 2) - time taken to add the x

* Significant effect of filter type on editing time (p < 0.001). ([report](https://drive.google.com/open?id=0BwxIc9E2K1b4eFVQZjJvV1dLQUU))
  + Significant differences between
    - Filter 1 vs filter 3 (p<0.05)
    - Filter 1 vs filter 6 (p<0.005)
    - Filter 2 vs filter 6 (p<0.05)
    - Filter 3 vs filter 5 (p<0.005)
    - Filter 3 vs filter 6 (p<0.001)
    - Filter 5 vs filter 6 (p<0.001)
    - Show the means and standard deviations in a table along with the p values. Interpret the results in the discussion section of your paper.
* Interaction between filter type and password type (p < 0.05). ([report](https://drive.google.com/open?id=0BwxIc9E2K1b4eFVQZjJvV1dLQUU))
  + This means that if we dig deeper, we might find that one a filter results in faster editing time based on the password type.
  + Examine the graphs and see if there are any tendencies similar to the one in point C
* Interaction between password type and entry number (p < 0.05). ([report](https://drive.google.com/open?id=0BwxIc9E2K1b4eFVQZjJvV1dLQUU))
  + Not really interesting

## E. Levenshtein distance (security) - how well they performed in the shoulder surfing task

* Significant effect of filter type on Levenshtein distance (p < 0.001). ([report](https://drive.google.com/open?id=0BwxIc9E2K1b4MmhxRW9odUQwZXM))
  + Significant differences between ALL CONDITIONS **EXCEPT**
    - Filter 1 vs filter 2
    - Filter 1 vs filter 3
    - This means you can generalize the results from this part.
* Significant effect of password type on Levenshtein distance (p < 0.01). ([report](https://drive.google.com/open?id=0BwxIc9E2K1b4MmhxRW9odUQwZXM))
  + Significant differences between
    - Password type 1 and 3 p < 0.005
    - Password type 2 and 3 p < 0.05
* Interaction between filter type and password type (p < 0.001).
* Interaction between filter type and entry number (p < 0.001).
* Interaction between filter type, password type and entry number (p < 0.001).
* Check the graphs for any other interesting insights.