

## PivotTable Datasets

Row Labels	Sum of Count
Only Letters	446
Only Numbers	40
Number and Letters	14
<b>Grand Total</b>	<b>500</b>

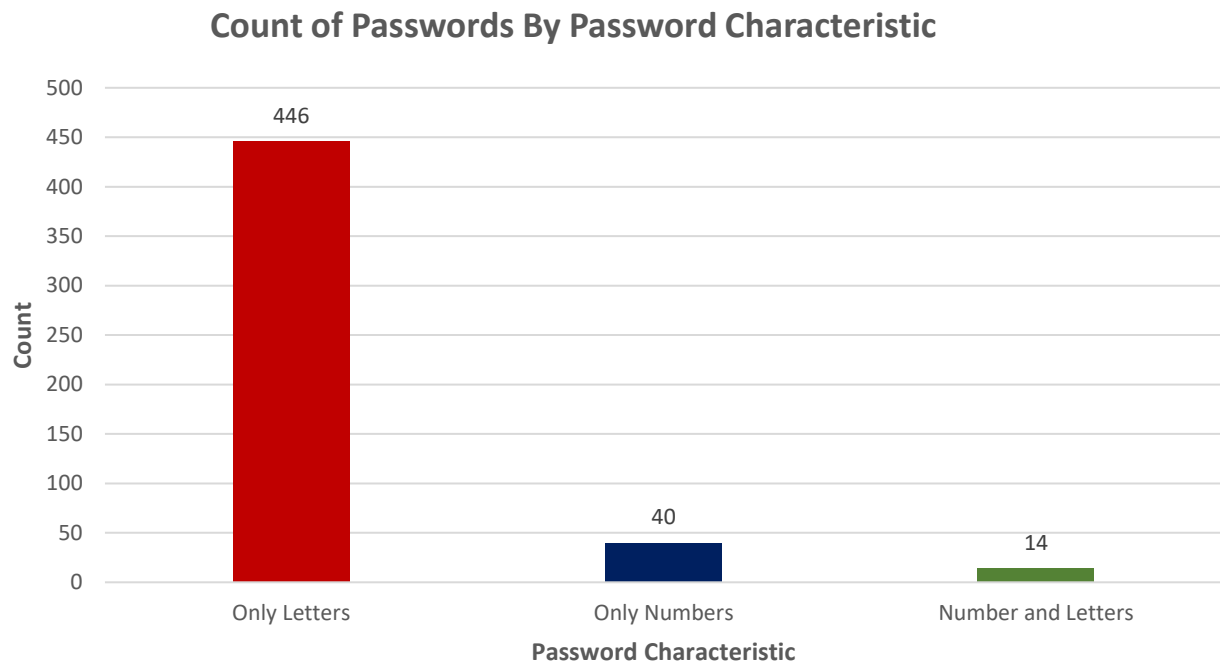
Row Labels	Average of online_crack_sec
animal	24455949.75
cool-macho	34856572.5
fluffy	16143166.46
food	20074434.55
name	28060743.95
nerdy-pop	129236674.5
password-related	225387775.8
rebellious-rude	40616754.43
simple-alphanumeric	61415689.88
sport	110313924.2
<b>Grand Total</b>	<b>50123598.93</b>

Row Labels	Average of strength_normalize
4	4.571428571
5	5.744186047
6	6.570866142
7	7.968421053
8	7.923076923
<b>Grand Total</b>	<b>6.773547094</b>

Row Labels	Average of online_crack_sec
1	6310227.499
2	4353461.36
3	92170.28571
4	15080279.82
5	13084598.12
6	636510.5326
7	8234126.088
8	31561469.58
9	85819866.24
10	569245186.1
<b>Grand Total</b>	<b>50123598.93</b>

Row Labels	Average of online_crack_sec
Only Letters	29166131.63
Only Numbers	43095.74525
Numbers and Letters	41267404.8
<b>Grand Total</b>	<b>27061476.99</b>

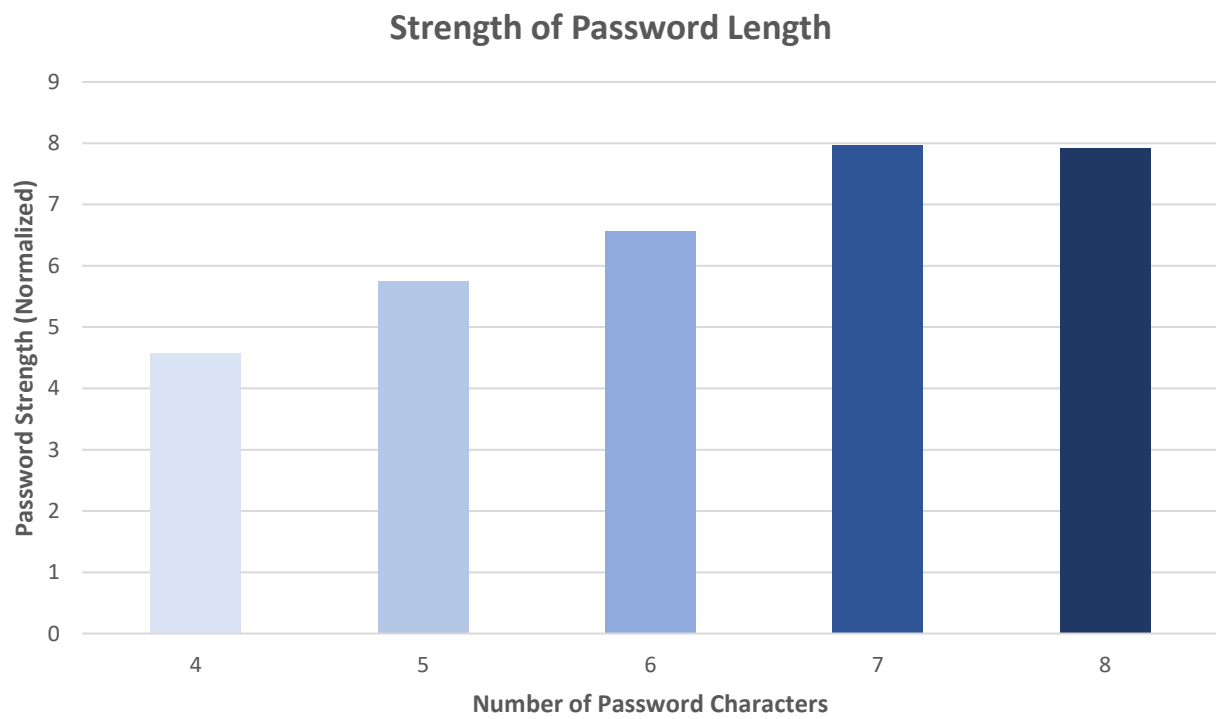
Sum of Count



Password Feature

Figure 1

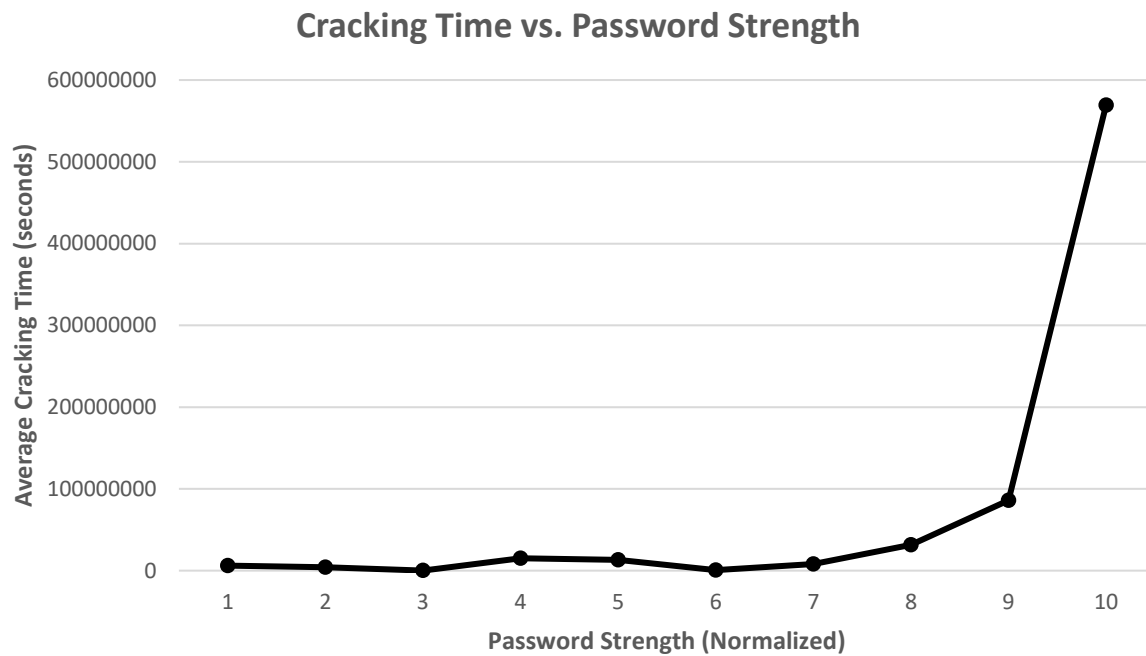
Average of strength\_normalize



password\_length

Figure 2

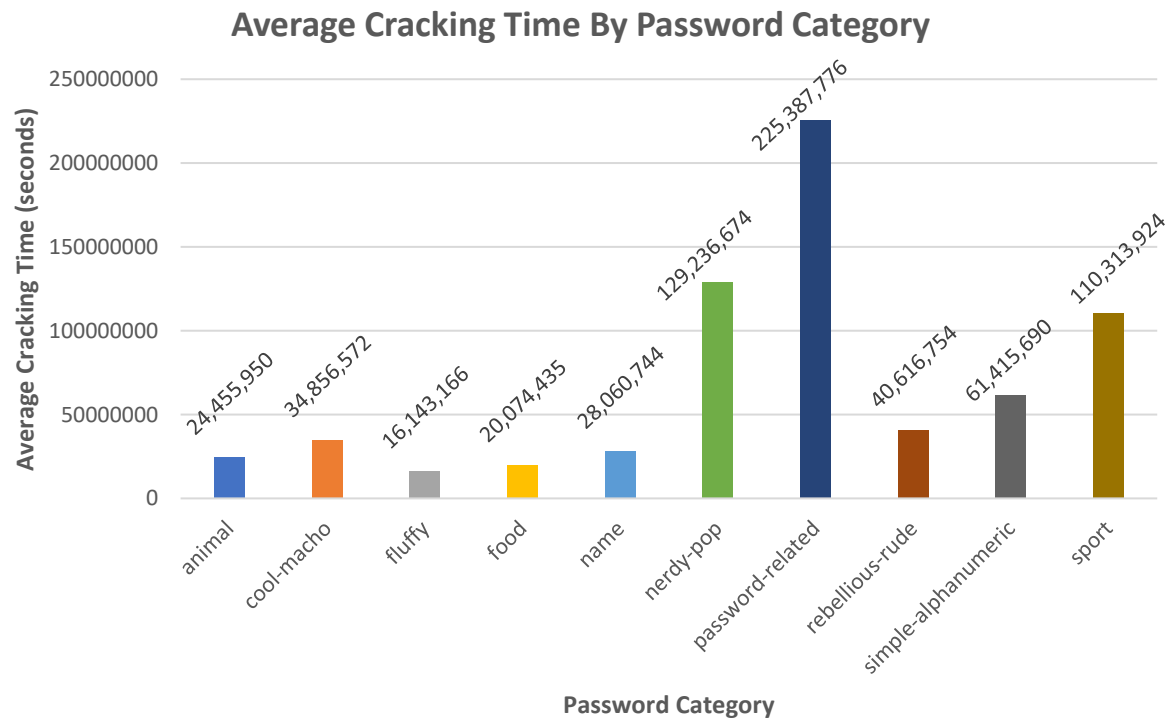
Average of online\_crack\_sec



strength\_normalize

Figure 3

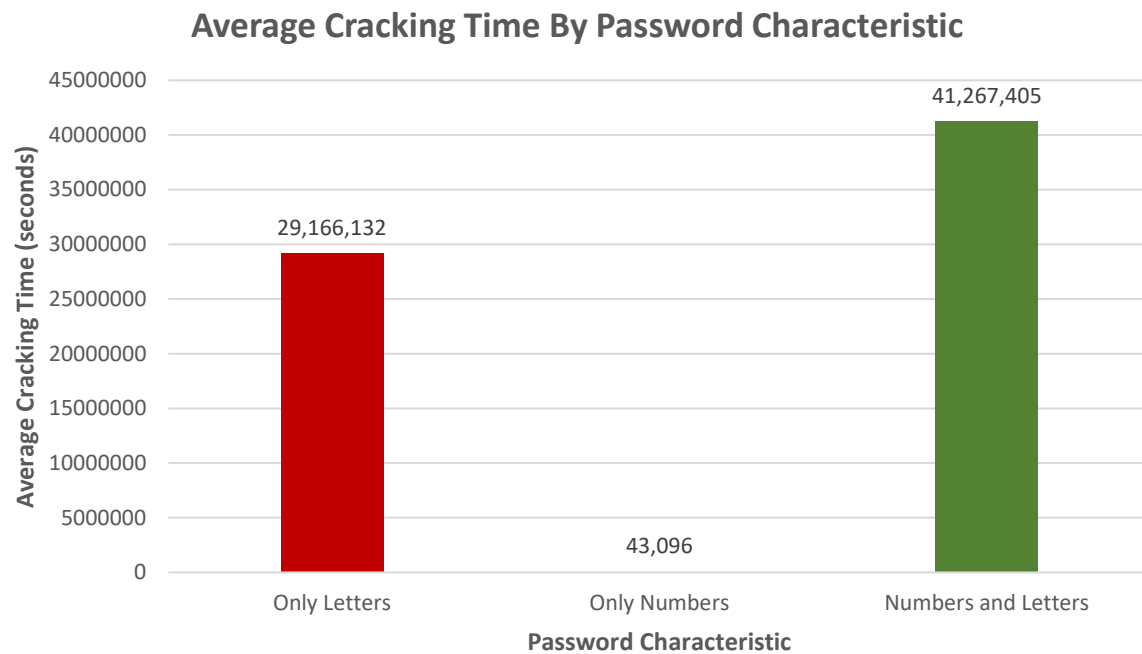
Average of online\_crack\_sec



category

Figure 4

Average of online\_crack\_sec



password characteristic

Figure 5

### Summary and Findings

The dataset used in this project showed the top 500 most commonly used passwords on the internet. The feature for the time required to crack each password is transformed into seconds for analysis. The feature for password strength is normalized into a scale of 1 to 10. Outliers for password strength and cracking time were removed.

Figure 1 shows that the most commonly used passwords are those with letters only, while the least common passwords are those that contain both letters and numbers. It should also be noted that there are no passwords with special characters in this dataset likely because passwords with special characters are not common enough to appear in a dataset for commonly used passwords.

Figure 2 shows that the password strength increases as the number of characters a password has also increases.

Figure 3 shows that average time required to crack a password increases as password strength increases. This indicates that the 'strength' feature in this dataset is a good indicator of password strength.

Figure 4 shows that the hardest passwords to crack fall in the category of 'password-related', while the easiest fall in the category of 'fluffy', based on average cracking time.

Figure 5 shows that passwords with both numbers and letters take the longest to crack, on average. Interestingly, passwords with only letters also take quite long to crack, but not as long as passwords with both numbers and letters. Meanwhile, passwords with only numbers are significantly easier to crack. This could be because there are only 10 digits, while there are at least 26 letters in the alphabet, allowing for more password combinations. A higher number of password combinations likely leads to a longer cracking time.