



**CALIFORNIA STATE SCIENCE FAIR  
2017 PROJECT SUMMARY**

<b>Name(s)</b> <b>Jonathan W. Weakliem</b>	<b>Project Number</b> <b>J0817</b>
<b>Project Title</b> <b>How Secure Are Your Passwords?</b>	
<p style="text-align: center;"><b>Abstract</b></p> <p><b>Objectives/Goals</b> The objective is to see what makes a password hard for password cracking software to recover and what variables of a password make it most secure.</p> <p><b>Methods/Materials</b> Laptop, John the Ripper software, Python software, Command prompt. Encrypted sample passwords with python and ran John the Ripper against them while timing it.</p> <p><b>Results</b> Adding anything to a password makes it harder to crack. I found that adding symbols was the variable that made passwords most secure.</p> <p><b>Conclusions/Discussion</b> The data showed that adding anything to a password made it (on average) take longer to crack. It also showed that adding symbols made passwords the hardest to crack on the order of several hours.</p>	
<b>Summary Statement</b> I showed that adding anything to your password makes it harder to crack.	
<b>Help Received</b> I got some basic information about encryptions and passwords from a grad student in computer science and some basic computer assistance from a family member. I ran the programs, created the lists of passwords, and analyzed/ recorded results.	