CALIFORNIA STATE SCIENCE FAIR
2013 PROJECT SUMMARY

Name(s)

Sohil Bammi; Brandon Betkolia; Eric Zhou

Project Number

33992

Project Title

The Automated Creation of Randomized Relational Languages as a Web Application

Abstract

Objectives/Goals

The goal of this program is to offer an engine for creating new, phonetically-correct languages via a web service. Furthermore, this program should effectively be used as an encryption device when paired with hashing algorithms. This should be further proven by experiments which will be carried out following the creation of the website.

Methods/Materials

The website MyVernacular was set up by purchasing a domain name. The engine was created in Perl and then implicated into the website. Then, a list of the 100 most popular passwords were taken and run through two industry standard hashing algorithms, MD5 and SHA1. Using an online decrypter we tested whether the hashes could be reversed and the password revealed. We repeated the same test three more times, but translated any English words to Italian, German, and a language generated by MyVernacular. Also, in order to test the memorability of the language we gathered 48 randomly selected students who were willing to participate in a memory test. They were randomly given a word chosen from three sets of words: English, German, and a randomly generated language from MyVernacular. All subject were told to spend one minute memorizing the word, and to not write down that word for later records. After three days, the subjects wrote down what they remember of the word. The number of successes (the word that the subjects remember matched exactly the word they were assigned) of each set of words was recorded.

Results

We were able to completely construct a website that allows a user to create a randomized relational language. In encryption test, all English passwords were cracked, and most of the German and Italian ones were effectively cracked as well. However, only two of the MyVernacular passwords were cracked. Furthermore, in a test of memorability, 91.7% of the test subjects given an English word remembered their designated word. 83.3% remembered the MyVernacular word. 66.7% remembered the Italian word. 50.0% remembered the German word.

Conclusions/Discussion

Overall, the engine was able to randomly create a language based on phonetics. MyVernacular was clearly used effectively in cryptography as an extra layer of abstraction between a password and a hash algorithm. Additionally, words served a practical function because of their memorability when compared to the original language (English) and the control languages (German and Italian).

Summary Statement

This is a web service that creates a phonetically-correct and memorable language which can be implicated as an extra layer of abstraction in cryptography.

Help Received

Students participated in the memorization tests

Preliminary