Lewis University
STEM Undergraduate Research Experience (S.U.R.E.) 2019
Faculty Mentor – Project Application

Faculty Name: Dr. Jason Perry

Department: Computer and Mathematical Sciences

Research Project Title: *Cracking Encryption with Graph Matching Algorithms*

There are a number of security products currently on the market that will encrypt your personal files when you store them in the cloud, protecting them from prying eyes, while at the same time giving you the ability to perform searches on the encrypted data. These products employ algorithms from the research area of *Searchable Encryption*. However, cryptographers have found that these algorithms have weaknesses that can be exploited by the service provider to breach your privacy. Specifically, an eavesdropping service provider can observe the *access pattern* of results returned from your searches, even though the search terms themselves are encrypted. With this data, the provider may be able to deduce the words you've searched for, violating your privacy.

In this research project, you will help determine exactly how much such a snooping service provider can learn, by carrying out computational experiments that simulate *query reconstruction attacks* on real-world datasets. The task of reconstructing search terms can be formulated in a general way as a problem from graph theory called *weighted graph matching*. Though there's no efficient algorithm to solve this problem exactly, researchers have developed approximation algorithms that perform quite well. You will learn to use a code library that implements state-of-the-art graph matching techniques, run the attack experiments, and analyze the results, revealing the weaknesses of searchable encryption and contributing to better understanding of privacy in our data-saturated society.