Brent Williams
Drew Schulz

Intro to Cryptology Final Project Proposal

Problem Statement:

Ciphertexts can come in many different forms. When receiving a ciphertext, an adversary may be able to decrypt the message if they know the specific cipher that was used to encrypt it. If the adversary does not know of the specific cipher, is it still possible to decrypt the message?

We will create a “black box” program that can take any ciphertext, created by a set of historical ciphers, and decrypt the message. To cover a breadth of ciphers, we will be working with at least one cipher from the following categories: transposition ciphers (e.g. Rail Fence Cipher), monoalphabetic substitution ciphers (e.g. Caesar Cipher and simple substitution cipher), polyalphabetic ciphers (e.g. Vigenere Cipher), and polygraphic substitution ciphers (e.g. playfair cipher).

Milestones:

11/5/14 - Working implementation identifying and decrypting the Caesar and Vigenere ciphers

11/19/14 - Working implementation identifying and decrypting the simple substitution cipher

11/22/14 - Working implementation identifying and decrypting the Rail Fence cipher

12/3/14 - Have a working “black box” decrypter program that identifies and implements all of the above ciphers and the playfair cipher

Website on Identifying unknown ciphers:
http://practicalcryptography.com/cryptanalysis/text-characterisation/identifying-unknown-ciphers/