ClassicCryptJ – E-Learning Platform for Non-Digital Secret Writing

Nikhil S. Bhalla
Master of Computer Applications
Project Intern, Pad. Dr. D.Y. Patil ACS College, Pimpri

Abstract

In the quest for better digital security in the internet age, we are often found neglecting our past at our own peril. Most students pursuing professional degrees and certifications in information security go only as far as associating classical cryptography with terms like substitution or transposition, Caesar Cipher or Playfair Cipher primarily due to the focus of the most reputed institutions resting, somewhat rightly so, on digital cryptology. However, there stand some questions viz. What alternatives could be explored to achieve secure communication in areas not connected by power supply? What is the extent of the threat when an attacker, in situations concerning regional or national security chooses to use a secure enough non-digital cipher that takes just about detrimentally long to break? It is the aforesaid reasons that compel us to revisit our information security past and delve into traditional secret writing techniques so as to establish a more concrete platform for students to rocket launch their careers and for professionals to enhance their skill sets.

This paper, as a solution to learning traditional secret writing, describes ClassicCryptJ - a multi-lingual desktop-based e-learning software in Java Swing, based on the API designed using Java's object oriented paradigm for implementing and analyzing non-digital secret writing to facilitate teaching and research for information security students and professionals. ClassicCryptJ's API, apart from being an improvement over the paper 'A Java API for Historical Ciphers' by Ralph Morelli, which utilizes object oriented design patterns viz. Interface Pattern, Factory Method Pattern, Delegation Pattern and Searchable Container Pattern to implement secret writing techniques and which has been modeled closely on the Java Cryptography Extension (JCE), goes a step further by incorporating not only historical ciphers but also cryptographic codes, nomenclators, non-digital steganographic techniques and statistical cryptanalytic tests. ClassicCryptJ's API again improves over Morelli's rendition by integrating a detailed taxonomy of each technique by enabling any class that implements a particular secret writing algorithm to expose the hierarchy of the family that the technique belongs to.