Simple implementation of an ElGamal Digital Signature and a Brute Force attack on it

By Valeriia Laryoshyna (laryoshv@my.erau.edu)

Of Embry-Riddle Aeronautical University – Prescott Campus

In Partial Fulfillment of the Requirements For the Honors Program

In the Degree of Bachelors of Science in Cyber Intelligence and Security

Mentored by Dr. Paul Hriljac, Professor of Mathematics in the College of Arts and Sciences

(hriljap@my.erau.edu)

Abstract

This study is an attempt to show a basic mathematical usage of the concepts behind digital signatures and to provide a simple approach and understanding to cracking basic digital signatures. The approach takes on simple C programming of the ElGamal digital signature to identify some limits that can be encountered and provide considerations for making more complex code. Additionally, there is a literature review of the ElGamal digital signature and the brute force attack.

The research component of this project provides a list of possible ways to crack the basic implementations and classifies the different approaches that could be taken to break the signature. One of those methods, brute force, is taken and applied to effectively break the math behind the digital signature model that was used. Analysis of the brute force attack is provided to show the trends with in the primitive roots. Countermeasures are then developed to show effectiveness and recommendations are included on how to develop the data more effectively.