Yaroslav Kechkin

Project Rationale

Gulf Coast State College

MAN 4900

Wendy Payne, Guy Garrett

February 9, 2012

The problem that is being addressed by me is a creation of encryption program based on several simple algorithms. These algorithms come as a combination of Vigenere encrypting scheme (with added randomization), hash based encryption and one-time pad encryption. Later in the project I am planning on expanding the program to work with current encrypting schemes based on public/private keys. The more sophisticated the way of encryption the harder it would be to break.

Cryptography is used to secure telephone, Internet, and email communication and to protect software and other digital property. It also comes in handy with electronic banking and e-commerce as more businesses introduce electronic way of transferring money. Secure payment systems are necessary in order for electronic commerce on open networks to exist. “One way to make electronic payments is to use a modified version of the existing credit card system. Cryptography can be used to protect the confidentiality of a message containing a credit card number and to confirm that the message was indeed sent by the card holder. While this method is currently being used, it leaves the credit card number vulnerable to improper use after the message containing it has been decrypted. Another design involves verifiable security mechanisms for the transaction to occur electronically which are not simply based on the exchange of a credit card number -- such as independent confirmation by digital signature -- as well as an authorisation process that is not tied to any proprietary network so that purchases can be made on open networks.” (Department of Justice, 2000)

Cryptography plays an important role in developing information infrastructures. With accommodation of e-commerce, Internet, as an open network, presents a big challenge for making electronic contact and transactions secure. Cryptography provides the integrity of the information that is traveling the Internet and offers a solution to secure interaction and transactions between parties by providing ways for authentication and non-repudiation – proving identity of the sender/receiver and limiting the ability of others to alter the data.

“Cryptography can also provide technical solutions for the protection of intellectual property in digital form. For example, a digital signature together with a verifiable time-stamp can give authors some control over their work, by tying an electronic document to the issuer and ensuring that the document is not modified without detection. The same technology can be applied to ensuring the authenticity and integrity of documents archived electronically.” (Department of Justice, 2000)

Organizations are more and more affected by electronic information and communications systems, and there is an increasing dependence on their availability and functioning. These systems should be trustworthy and secure so that customers and user would trust in them with the confidential information (credit cards, address, and social security number). Lack of either confidence or security will harm the organizations that are involved in e-commerce. There is a need to build consumer confidence in data security mechanisms, like cryptography, so that they will be widely used for electronic commerce.

The timeline of the course will be enough to introduce the scope of the problem. It will be possible for me to create encrypting/decrypting algorithm in a month and modify it in order to meet the requirements of today’s security with large keys. I do not think it would be possible (but I will try) to create the algorithm based on the integrals and differentials and make them secure, but creation of sophisticated program will not be a problem. Creation of separate algorithm would take a long time and it would not fit the timeline of the course, but I would do my best to address the problem in full.

**References**

Department of Justice (May 8, 2000). Oecd Guidelines For Cryptogrpahy Policy: Report on Background and Issues of Cryptography Policy. Retrieved from <http://www.justice.gov/criminal/cybercrime/oeback.htm>