**Cryptology for Security**

**A SIMPLE ENCRYPTION AND DECRYPTION Technique**

ABSTRACT

The internet generates very large amount of data on a daily basis. While some of the information are trivial others are sensitive. As a matter of fact, the security of some information traversing the internet is critical to the survival of the owner.

In this study, we implement the RSA algorithm to produce a simple system for encryption and decryption of files with .txt extension. The system also incorporates digital signature to authenticate the sender of a message.

STATEMENT OF PROBLEM

The underlying respective architecture of most IT systems, including the desktop computer and internet, does not guarantee security. Users with malicious intents have always found a way of exploiting one vulnerability or the other. An attack that affects the confidentiality of information often presents the platform for the integrity of such information to be compromised.

Intercepted information on transit would make little or no sense to an interceptor if he is not able to decipher the content of the information. This explains why it is very necessary to ensure that even when an intruder or unauthorised user successfully obtains access to some information the confidentiality and integrity of the information remain uncompromised.

OBJECTIVE

The objective of this paper is to design and implement an application that encrypts and decrypts plain text files using R.S.A algorithm and utilizes digital signature technique to verify the integrity and authenticity of the message sent.

EXISTING SYSTEM

Designing an encryption/decryption system, amongst other things, requires decision on the basic functionality of the software, and the choice of cryptographic algorithm to be used. While the functionality supports the attractiveness of the system, the type of cryptographic algorithm actually determines how much security the system would actually provide.

Hence, this forms the major component in the system design.

SYSTEM DESIGN

Functional/Operational Requirements

This requirement outlines the functional/operational capability that the system can be able to provide and reaction to a particular problem. The data encryption and decryption system has the following functional requirements:

1. The system shall be able to identify documents with .txt extension, for encryption.
2. The system shall be able to generate public and private keys to be used by registered users for both encryption and decryption.
3. The system shall be able to encrypt and decrypt text files stored in the computer system.
4. The system shall be able to save the encrypted plain text as .txt files.

Security Requirements

The security requirement entails the capacity to control user access, manage data and also support the three security concept (e.g. confidentiality, integrity and availability of data). The security requirements of the new data encryption and decryption systems are listed below:

1. The system shall be able to authenticate users.
2. The system must be able to deny access to illegitimate users to the system.
3. The system must be able to retrieve the forgotten key by asking for some security question in order to verify user’s authenticity. This is achieved via email matching and secret questions supplied by the user during registration.
4. The system shall be able to verify the sender of a message through authenticating the user’s digital signature.

Architectural Design

The system is divided into two sessions, the use application and admin session. The major components design of admin sessions includes register new user, view user information, delete user, and configure server/ client system. The registered user session includes encryption of plain text and decryption of cipher text. Figure 1 below show the architecture overview of our proposed system.



