# Secure Spreadsheet Data File Transferring System

Chaw Nanda Tun, Khin Than Mya
*University of Computer Studies, Yangon*
*chawlay08@gmail.com*

## Abstract

*Advent technology of security for secret important data and information is called the Cryptography. Cryptography is an important aspect of communications security and is a basic building block for computer security. However, the term today refers to the science and of transforming message to make them secure. The Advanced Encryption Standard (AES) is computer security standard. SHA cryptographic hash function is that a hash-value serves as a message digest of an input string. This thesis provides the encryption and decryption system for desire cells in excel (spreadsheet file) that can be used to build a secure and hash code for one or more files of person identifiable data. The proposed system is a data transferring system, which send encrypted excel data file from one place to another on network. This system implements AES-128 and SHA-256 algorithm improve the security of excel data file even on insecure network.*

Keywords: Spreadsheet File Security System, Cryptography, AES 128, SHA 256

## 1. Introduction

In the wired and wireless communication area, more and more increases the performance of sensitive information transferring. When sensitive information is transmitted over the network (or) internet, they need to ensure information security and safety. It becomes necessary to protect the information security is important in that case, widely uses the cryptography. Cryptography was created as a technique for securing the secrecy of communication integrity and many different methods have been developed to encrypted and decrypted data in order to keep the message secret.

Computer science world, everybody use the Microsoft Office Document. Microsoft Office Excel represents 90% of office suites for home use and 80% of office suites for professional use. Office excel still represents a small part of the market. Sometimes, secret data or information to store using spreadsheet excels. Spreadsheets allow you to organize information in rows and tables (which create cells). Every single cell in the spreadsheet can be modified (or) repairs easily. Secret data or information can be changed easily when accidentally click on another cell. It is necessary to prevent this happening. In Microsoft Office Excel (spreadsheet file), the cells can be protected with cryptography system. This thesis implements data file encryption and decryption system and hash code system to prevent the hacker.

The rest of this paper is organized as follows: Section 2 discusses the related work. Section 3 describes background theory. Section 4 presents system design and implementation. Experimental results are presented in Section 5. Finally, conclude this paper in Section 6.

## 2. Related Work

Oi-Shang Chok et al., [5] described their experience in developing an active learning course module to help students understand DES and AES algorithms using Microsoft Office Excel XP learned in their computer literacy class. The user document with snapshots gives details for a user to input and use. These DES and AES learning tools. Testing and security issues had been suggested. Hongjum Wu [4] reported their point out a serious security flaw in Microsoft Word and Excel to protect the documents. But when an encrypted document gets modified and saved, the initialization vector remains the same and thus the same key stream generated versions of that document. The consequence is disastrous since a lot of information of the document could be recovered easily. [8], this paper discussed improvements in document encryption found in the Microsoft 2007 Office system. They discussed scenarios in which document encryption is valuable to the user, technical information regarding the Microsoft 2007 Office system document encryption is greatly improved over encryption methods used for previous versions of Microsoft Office and introduces industry-standard AES encryption support. In this paper, we describes encryption and decryption by using AES (Advance Encryption Standard) 128 algorithm for cells in the spreadsheet data file, and then SHA256 algorithm is used for encrypted spreadsheet data file to verify. This paper, we perform the desire cells are protected

with encryption in the Excel spreadsheet data file. We use the cryptography for confidentiality and integrity. This paper will indicate the probability of successful securely transfer the spreadsheet data file on the un-trusted network using the cryptographic algorithm.

## 3. Background Theory

### 3.1. Cryptography

Cryptography is the study of the message secrecy. Technique used to hide the meaning of a message. Considered to be branch of both mathematics and computer science. The mathematical techniques real Considered to be branch of both mathematics and computer science. The mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication and data origin authentication.

The fundamental goal of cryptography:

- Privacy or confidentiality
- Integrity
- Authentication
- Non-repudiation

### 3.2. AES Algorithm

The Advanced Encryption Standard (AES) is a symmetric encryption algorithm which was selected in 2001 by the National Institute of standards and Technology (NIST) as the Federal Information Processing Standard FIPS-197 [3]. The AES algorithm operates on 128 bits of data and generates 128 bits of output. The length of the key used to encrypt this input data can be 128, 192 or 256 bits [6]. Our implementation uses fixed key size of 128 bits which is used both for Encryption and Decryption.

**AES Encryption**: the length of input block, the output block and the state is 128 bits. This is represented by Nb=4, which reflects the number of 32 bits words (number and columns) in the state. The length of the Cipher Key, K is 128 bits. The key length is represented by Nk=4, which reflects the number of 32 bits words (number and columns) in the Cipher Key. The number of rounds is represented by Nr=10. The AES algorithm consists of four byte oriented transformation. Theses transformations are:

a. Byte Substitution using S box table (S-box)
b. Shifting rows of the state array using different offsets (Row transformation)
c. Mixing the data within each column of the state array (Mixing Column)
d. Adding a round key to state(Add-round key)

The set of these four transformations is also called as around transformation [7]. So the pseudo code for round transformation is:

```
State Round Transformation (state-round key)
  {
      S-box;
      Row shifting;
      Column mixing;
      Add round key;
  }

State final Round (state-round key)
  {
      S-box;
      Row shifting;
      Add round key;
  }
```

Different keys are generated for all the iterations by the key Expansion module. The first round key is equal to the cipher key. The computation of all other round keys is based on the S-Box functionality and the Rcon operation [2, 7].

**AES Decryption**: is not identical to encryption since steps done in reverse but can define an equivalent inverse cipher with steps as for encryption by using inverse of each step and with different key schedule. The transformations used are:

a. Inverse Shift Row
b. Inverse Sub Bytes Transformation
c. Inverse Mix Column Transformation
d. Add Round Key Transformation

The pseudo code for the Inverse Cipher is

```
State Inverse AES (state-key)
  {
      Key Expansion;
      Add round key;
      Loop Nr-1 times:
          Begin
            Inverse shift rows;
            Inverse Sub bytes transformation;
            Inverse Mix Column Transformation;
            Add round Key transformation;
          End
                Inverse shift rows;
                Inverse Sub bytes transformation;
                Add round Key transformation;
  }
```

### 3.3. Secure Hash Algorithm (SHA)

This standard specifies four secure hash algorithms, SHA 1, SHA 256, SHA 384 and SHA512 for computing a condensed data (message). When a message of any length $2^{64}$ bits (for SHA 1 and SHA 256) or $2^{128}$ bit (for SHA 384 and SHA 512) is input

to an algorithm, the result is an output called a message digest. The message digests range in length from 160 to 512 bits, depending on the algorithm. We implement SHA 256 hash algorithm. The properties of SHA 256 hash function are given below in Table 3.1.

Table 3.1 Properties of SHA 256 hash function

| Algorithm | Message Size (bit) | Block Size (bit) | Word Size (bit) | Message Digest Size (bits) | Security (bits) |
|---|---|---|---|---|---|
| SHA 256 | $<2^{64}$ | 512 | 32 | 256 | 128 |

SHA 256 calculation is complete in 64 rounds and 8 hash variables each of 32 bit are used. The word size of all the calculations is 32 bits. The padded message is processed by 512 bit blocks. This 512 bit block is composed of 16 message words. These 16 message words are expanded by means of function and in each of the total 64 rounds a new message word is used. The computation is done in [1].

## 4. System Design and Implementation

The Excel spreadsheet file includes sheets. The sheets combine with many cells. Data or information can be stored in the cells. The important data or information can be protected with cryptographic system in the cells. We make security on the spreadsheet file to be protected from attack of hacker.

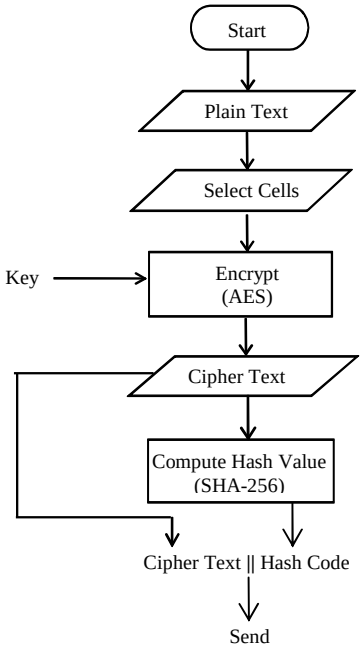



Figure 1 Flow diagram of encryption process

We create an Excel spreadsheet file which contains data in each cell. We select the desire cells consist of data are encrypted by using AES 128 algorithm in the spreadsheet file. When the data encryption finished in the selected cells, continue we compute hash value to this spreadsheet file is made to be strong security by using SHA 256 algorithm. Encrypted spreadsheet file and hash value are send to receiver over the network. That process is shown in Figure 1.

Encrypted spreadsheet file and hash value are received. The receiving encrypted spreadsheet file is computed hash value by SHA 256 algorithm. If tow hash values are equal, the desire cells are selected to be decryption in the encrypted spreadsheet file. Data are decrypted in the selected cells by AES 128 algorithm. If two hash values are not equal, encrypted spreadsheet file is rejected. Receiver's process is shown in Figure 2.

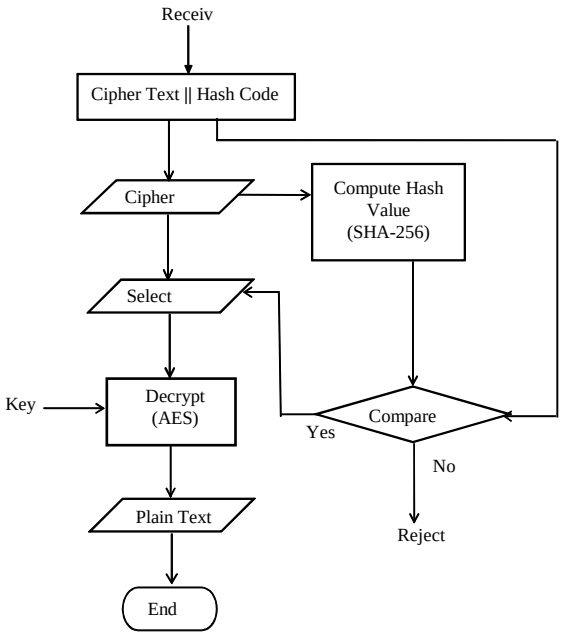



Figure 2 Flow diagram of decryption process

## 5. Experimental results

In this paper, the various cells (Row and Column) are made encryption and decryption in the spreadsheet file. This process, first open the spreadsheet file and then the desire cells were select to be protected in the spreadsheet file. In Figure 3 shows we selected the cells (D6: I12) were made encryption.

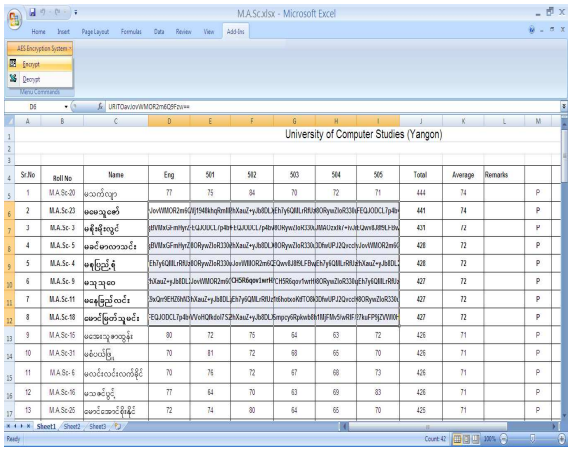



Figure 3. View of Encrypted Data

In the encrypted spreadsheet file, the desire cells are made decryption. Figure 4 shows we select the cells (D6: I12) are made decryption.

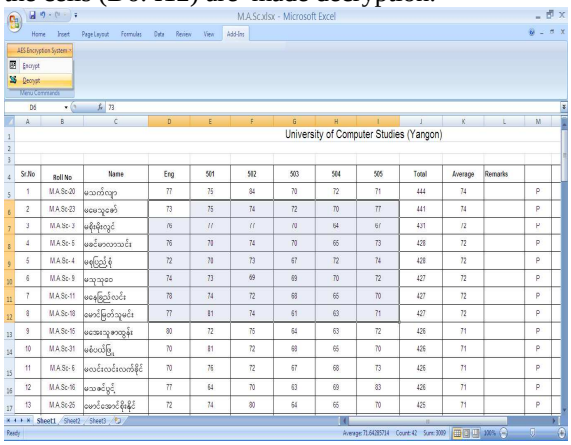
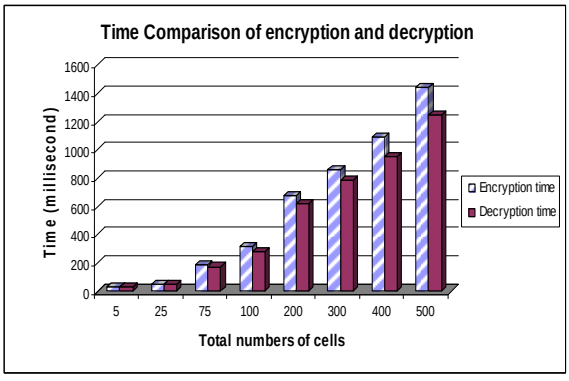



Figure 4. View of Decrypted Data

We use computer model Core (TM) 2 Duo CPU E8400 3.00 GHz and memory has 2 G for our experimental results. Figure 5 shows time comparison of encryption and decryption depend on the total numbers of selected cells in the spreadsheet file.




Figrure 5 Time comparison of encryption and decryption process

The time taken of encryption and decryption are different depend on the total numbers of selected cells in spreadsheet file. We perform comparison of encryption time and decryption time. If a few cells are made encryption and decryption, time taken has a little difference but time taken has the more difference when the many cells are made encryption and decryption. When become more and more increase cells, the encryption and decryption time taken have become more and more differences. In these results, the decryption time is faster than encryption time.

## 6. Conclusion

Security system is every useful in the computer and network field. Most people perform the spreadsheet file transmission over computer network. The spreadsheet files are made strong security when they send files one place to another on network. In this paper, the cells were protected with security system in the spreadsheet file. The user chose desire cells are protected in the spreadsheet file. Then these cells were protected with AES 128 algorithm. These spreadsheet file was made more and more strong security using SHA 256 algorithm. Spreadsheet file can be made to travel over the network securely using the techniques described in this paper.

## References

[1] Amouncing the SECURE HASH STANDARD, Federal Information Processing Standards Publication 180-2 (+Change Notice to include SHA-224), 2002 August.

[2] Announcing the ADVANCED ENCRYPTION STANDARD (AES), Federal Information, Processing Standards Publication 197, November 20, 2001.

[3] FIPS-197: Advanced Encryption Standard, National Institute of Standards Technology (NIST), l November 2001.Available online at http:// www.itl.nist.bovifipspubs/.

[4] Hongjum Wu, the Misuse of RC4 in Microsoft Word and Excel, Institute for Infocomm Research, Singapore, 2002.

[5] Oi-Shong et al., Computer Security Learning Laboratory: Implementation of DES and AES algorithms using Spreadsheets, St. Cloud State University, St. Cloud, MN 56301, 2005.

[6] P.Chown Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TlS), Request for Comments: 3268, June 2002.

[7] Sam path, Sowrirajan. M.S.E, PPGA based Hardware Implementation of Advanced Encryption Standard, Department of Electrical Engineering Wright State University, 2007.

[8] www.microsoft.com/office/.