Ind. JNT
(Indian Journal in Number theory)

Received: *11.05.2015*
Published: *30.11.2017*

Year: *2017*, ***Pages:*** *54-58*
*Original Article***

A SURVEY ON ENCRYPTION AND DECRYPTION TECHNIQUES

Ashish Somkule[1], Swapnil Bhandurge[2], Dhraramraj Garad[3], Arpit Sarode[4]

Department of Computer Science & Engineering,

Abha Gaikwad-Patil College of Engineering Nagpur, Maharashtra (India)

Abstract- This paper presents an Encryption/Decryption application that is able to work with any type of file; for example: image files, data files, documentation files, Audio and Video files…etc. The method of encryption is simple enough yet powerful enough to fit the needs of students and staff in a small institution. The application uses simple key generation method of random number generation and combination. The final encryption is a binary one performed through rotation of bits and XOR operation applied on each block of data in any file using a symmetric decimal key. The key generation and Encryption are all done by the system itself after clicking the encryption button with transparency to the user. The same encryption key is also used to decrypt the encrypted binary file.

Keywords: - Compression, Image compression, lossy compression, lossless compression, encoding, decoding.

INTRODUCTION

The high growth in the networking technology leads a common culture for interchanging of the file very drastically. Hence it is more vulnerable of duplicating of file and re-distributed by hackers. Therefore the file has to be protected while transmitting it, Sensitive information like credit cards, banking transactions and social security numbers need to be protected. For this many encryption techniques are existing which are used to avoid the information theft. In recent days of Internet, the encryption of data plays a major role in securing the data in online transmission focuses mainly on its security across the internet. Different encryption techniques are used to protect the confidential data from unauthorized use. Encryption is a very common technique for promoting the image security. Image encryption, video encryption, chaos based encryption have applications in many fields including the internet

communication, multimedia systems, medical imaging, Tele-medicine and military Communication, etc. The evolution of encryption is moving towards a future of endless possibilities. Everyday new methods of encryption techniques are discovered. This paper holds some of those recent existing encryption techniques and their security issues.

LITERATURE SURVEY:

To study and analyze more about the encryption techniques, the following literature survey has done.

Encryption: Encryption can be defined as the conversion of plain message into a form called a cipher text that can't be read by any people without decrypting the encrypted text. Decryption is the reverse process of encryption which is the process of converting the encrypted text into its original plain text, so that it can be read. Dahua Xie and Jay Kuo have proposed an encryption technique with enhanced Multiple Huffman Table (MHT) by key hopping method. The previously developed Multiple Huffman Table (MHT) has good desirable properties but it was highly vulnerable to the chosen plaintext attack (CPA). Whereas this enhanced MHT encryption method faces all such limitations. As the result shown, that the algorithm is secure for the chosen plaintext attack and proved mathematically by the key hopping method.

1. Suhaila O. Sharif, L.I. Kuncheva, S.P. Mansoor has jointly framed a manuscript for Classifying the Encryption Algorithms in accordance with the Pattern Recognition method. In this discussion the authors focuses on the limitations of the algorithms which are used for encryption scheme and for generating the keys for encryption process. Here the pattern recognition method to identify the block ciphers in encryption process. The block cipher algorithms like AES, DES, IDEA, and RC were used to identify the good classification technique. As the result shown, that the performance of RoFo (Rotaion Forest) classifier has the very good classification accuracy.

2. A Study on OMAP (Open Multimedia Applications Platform) Digital Fingerprint Encryption technique has done by Zhu Yuxi. In this study the author deals with the identification of the fingerprint and the security in transmission for the embedded systems. Here a digital fingerprint technique was used with the structure of the OMAP (Open Multimedia Applications Platform). The author designed an integrated software structure with an application platform.

3. Huang Jinga b Zheng Zhen-zhuc has developed an optical encryption technique for secure real time image transmission. Because of any image hold a huge amount of data or information, which results in very less efficiency of the real time image encryption. The authors has proposed a new scheme for image

encryption which is used in optical computing technologies that apparently focuses on images and large amounts of data simultaneously, as the result of this high speed is attained. Hence this scheme was implemented by using a stream cipher on the polarization encoder as the optical logic gates. The results states very good security for the images with histogram.

4. Mort Naraghi-Pour and his colleagues have developed a simple encryption standard for secure detection in the wireless sensor networks. Only the authorized user or the ally fusion center (AFC) is aware of the encryption method its features, and no unauthorized or any third party fusion centers (TPFC) are not aware of such encryption features. As the result shown, the exact threshold value was found and the numerical results were evaluated for the error probabilities of the two fusion centers (AFC and TPFC).

5. An iterative speech encryption scheme basis of subspace method was proposed by AtefMermoul. Blind source separation (BSS)-based encryption schemes have been built up using the intractability of the under determined BSS problem. In this paper, the author designed a novel encryption scheme that is iterative and based on the idea of subspace technique, by the nonlinear functions and the key signals. It is proved here that only a part of the secret key parameters were used in encryption process is needed for the decryption process. Also this technique gives no contents if no plain-text is fed in the input.

TYPES OF ENCRYPTION & DECRYPTION TECHNIQUE:

We can divide the entire cryptography algorithm (cipher) into two groups:

1. Symmetric Key
2. Asymmetric Key

Symmetric Key: In symmetric-key cryptography, the same key is used by both parties. The sender uses this key and an encryption algorithm to encrypt data; the receiver use's the same key and corresponding decryption algorithm to decrypt the data.

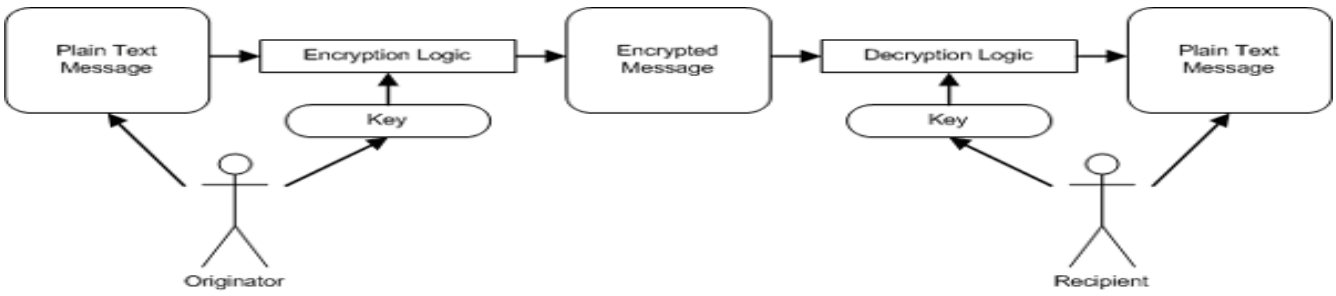
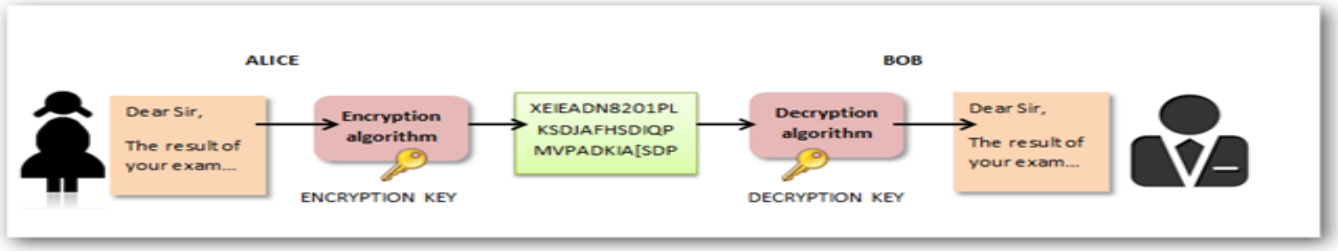


Diagram 1. Symmetric Encryption

Asymmetric Key: In asymmetric or a public key cryptography, there are two keys: a private key and a public key. The private key is kept is kept by the reciver.The public key is announced to the public. For ex: - Alice wants to send a message to Bob. Alice uses the public key to encrypt the message. When the message is received by Bob, the p-private key is used to decrypt the message**.**



SOFTWARES AVAILABLE:

There are several kinds of Encryption software in the market categorized by their functions and target groups. For example, some are single Encryption applications for files and database security; some are for messenger security or email Encryption applications that hide the actual text in the medium between the sender and the receiver. One of the first types of Encryption was made by Julius Caesar. In his system, Caesar wrote B instead of A and C instead of B… so to a sentence "ABC" will be written in "BCD".

- DsCrypt is AES/Rijndael file Encryption software with simple, multi-file, drag-and-drop operations. It features optimal implementation, performance and safety measures. dsCrypt uses an advanced Encryption algorithm and offers unique options for enhanced security.
- NeoCrypt is a free, open-source File Protection Utility for Windows. It helps to protect sensitive information easily by encrypting it with password or key. It yields fast, reliable and unbreakable Encryption and supports many popular ncryption algorithms. All types of files can be encrypted like Audio, Video, Documents and Executables programs .
- Neekprotect is a software in the market right now with the ability to make Encryption on any files in the window platform, a key is set when one try to encrypt a files and the key will be used again when someone else trying to open the files been decrypted through decryption on the certain files.
- Neek Protect is a good software operated under Microsoft window because of the flexibility of this program's advanced features integration such as double click, file icons, .npt file extension

etc. This paper reports on a similar encryption technique that uses binary rotation of bits with XOR logical operation using a custom made encryption key that operates on any type of a file.

CONCLUSION

In this internet world nowadays, the security for the digital images has become highly important since the communication by transmitting of digital products over the open network occur very frequently. In this paper, it has been surveyed that the existing works on the encryption techniques. Those encryption techniques are studied and analyzed well to promote the performance of the encryption methods also to ensure the security proceedings. To sum up, all the techniques are useful for real-time encryption. Each technique is unique in its own way, which might be suitable for different applications. Everyday new encryption technique is evolving hence fast and secure conventional encryption techniques will always work out with high rate of security.

References:

1. Freeman J. Neely R. and Megalo L. "Developing Secure Systems: Issues and Solutions", IEEE Journal of Computer and Communication, Vol. 89.