Perspectives in Communication, Embedded-Systems and Signal-Processing (PiCES)
ISSN: 2566-932X, Vol. 1, Issue 2, May 2017.

Cryptography: A Review

Prof. Vasanthi S[1], Surekha M H[2], Vachana G N[2], Vandana C[2], Vathsala V[2]

[1.] HOD, Dept. Of ECE, Atria Institute of Tech., Bangalore, India.

[2.] Electronics & Communication Engineering, Atria Institute of Tech., Bangalore, India.

Abstract--In today's Internet world security plays a very important role in securing data. After noticing constant reports of data theft and hacking, enhancing security of the data has become mandatory. Before a secure algorithm is proposed, it is necessary to review the existing technologies. This paper deals with information related to existing cryptographic techniques

Keywords-- Encryption, Decryption, AES, Visual Cryptography.

I. Introduction

Cryptography is a technique which involves the enciphering and deciphering of messages in secret code. It is a technique where information is hidden in plain sight in order to secure it from unauthorized party. It involves many protocols that prevent third parties or public from accessing private information.

As the number of commercial online transactions is increasing, it is necessary to provide security to these transactions. So the better method to ensure security to these transactions is Cryptography. Cryptography gives secure websites and allows safe electronic transactions. For a secured website, the data transmitted between the computers where the data is transmitted and received is encrypted. Hence, Cryptography provides Confidentiality, Integrity, Non-repudiation and Authentication.

II. TYPES OF CRYPTOGRAPHY

A. Symmetric Key Cryptography (Secret Key Cryptography):

It is a cryptographic technique which uses the same keys for both encryption of plain text and decryption of cipher text. It includes AES (Advanced Encryption Standard), DES (Data Encryption Standard) and 3-DES (Triple-Data Encryption Standard).These techniques have been found out to be fast.

B. Asymmetric Key Cryptography (Public Key Cryptography):

It is a cryptographic technique which uses different keys for both encryption of plain text and decryption of cipher text. It includes RSA (Rivesd-Shamir-Adleman) and ECC (Elliptic Curve Cryptography). It is highly secured but the process is comparatively complex.

C. Hash function:

Cryptographic hash function takes an input and returns a fixed size alphanumeric string which is called as hash value. It is a one way encryption and uses no key for encryption and decryption. For any given data, it is very easy to calculate its hash value.

III. Literature Survey

In [1], for authentication of user to serve a new protocol is developed using an encryption technique based on visual cryptography. Here the secret which is to be shared is a binary image. In a k-out-of-n scheme of VCS, a secret binary image is cryptographically encoded into n shares of random binary patterns. On transparencies the shares are xeroxed respectively and it is distributed as one for each participated. Each participant are unaware of shares given to other participants. By superimposing any transparencies together, any k or more participants are visually able to reveal the secret image. Even if infinite computational power is available to any participant, it is impossible for them to decode the secret image by any k-1 participants. It provides a different and better encryption which requires less computing. A new protocol suggested here will authenticates user to server without any previously established any secure communication channel requires less computing. A new protocol suggested here will authenticate user to server without any previously established any secure communication channel.

In paper [2]**,** Advanced encryption standards(AES) and RGB cryptographic technique is used for good encryption process. Here to generate shared secret key AES is made use and for encryption process visual cryptography is made use. Based on RGB pixel shuffling and displacement an encryption is done. Using image encryption algorithm, the ciphering of plain image is done but depending on keys used. The key used for image encryption is generated by using AES-256 algorithm. The numerical pixel values of the plain image were shifted and displayed from their respective positions and by using the key generated from the AES-256 algorithm, the RGB values are interchanged and shuffled for the image encryption process. There was no pixel loss or pixel expansion at the end of the encryption process. Hence the quality of the image will remain the same after decryption.

[3] discusses architectures for AES-128 implementation. Here, AES algorithm is developed for encryption and decryption using lookup table and composite field arithmetic. It explains AES that works on 128 bits of data undergoing ten rounds of processing to give 128 bits of cipher text. Encryption and decryption is done by outer pipeline and to the same encryption further stages of inner pipeline are applied and compared with

respect to throughput and area. For different area requirements large range of throughput is observed. It has resulted in different range of operating speeds. This makes AES compatible with different ranges of data communication rates.

The paper [4], combination of visual cryptography and steganography in association with QR codes to strengthen the security is explained. Visual cryptography creates two shares where one share is rotated clockwise direction for about 180^0 and other share for about 270^0. Steganography is implemented by using two's complement on both the share image. Then one of the steganoimage is converted into QR code which will be kept secret to user. For the authentication of user QR code is required. It has resulted in highly secured, confidential and efficient technique with unpredictable human vision taking less duration.

IV. Conclusion

If we implement visual cryptography alone by using key more than once the security will be lost. The area occupied by AES implementation using LUT is very large. Byte Substitution implementation using CFA gives large throughput by consuming less area.

If we use these methods individually, they are applicable only for some special criteria like user authentication for a website. Thus for generalised secure system, combination of these techniques can be proposed for enhanced security.

REFERENCES

[1] William Stallings, "Advanced Encryption Standards ", Cryptography & Network Security, 3rd ed., Asoke K. Ghosh, New Delhi, India, 2003.

[2] Praveen Kumar P & Sabitha S: “User Authentication using Visual Cryptography”. 2015 International Conference on Control, Communication & Computing India (ICCC)|19-21 November 2015|

[3] Quist-Aphetsi Kester, Laurent Nana & Anca Christine Pascu: “A Novel Cryptographic Technique for Securing Digital Images in the Cloud using AES & RGB pixel displacement”.2013 European Modelling Symposium. DOI 10.1109/EMS.2013.51

[4] Disha Yadav & Arvind Rajavat: “Area and Throughput Analysis of Different AES Architectures for FPGA Implementations”. 2016 IEEE International Symposium on Nanoelectronic and Information Systems. DOI 10.1109/iNIS.2016.61

[5] Himanshu Gupta & Nupur Sharma: “A Model for Biometric Security using Visual Cryptography”. 2016 5th International Conference on Reliability, Infocom Technologies & Optimization (ICRITO)(Trends and Future Directions), Sep. 7-9,2016.