Data Security Using Cryptography

Mahesh Sanjay Ghorpade MIT Polytechnic,Yeola

Harshal Sonawane MIT Polytechnic,Yeola

Bhad Vishakha MIT Polytechnic,Yeola

Tambe Ganesh MIT Polytechnic,Yeola

Vaidya Archana MIT Polytechnic,Yeola

Abstract

In separate used systems, the computers are exposed to the other users. To keep the data secured from different users various encryption algorithms are entered. As computer systems become more pervasive and complex, security is increasingly important. Cryptographic algorithms and protocols constitute the central component of systems that protect network transmissions and store data. Encryption is the translation of data to a secret code. Apart from its uses in Military and Government to facilitate secret communication, Encryption is used in protecting many kinds of civilian systems such as Internet e-commerce, Mobile networks, automatic teller machine transactions, copy protection (especially protection against reverse Engineering and Software piracy), and many more. The Encrypted data can only be deciphered if one has the password or the Key. The Encryption algorithm is a set of well defined steps to transform data from a readable format to an encoded format using the Key. This set of well defined steps is also called cipher.

Keywords- Cryptography, Steganography, Data Security.

INTRODUCTION

In data security web application, we provide users with security of important data. which is stored in the file is created by the user and the key (pass) is also set by the user. The created file is encrypted using the Advance Encryption Standard (AES) algorithm and the Data Encryption standard (DES) algorithm. Before creating a file,the user must allocate a file size for data storage. Then the user can insert any type of data into the created file.No one reads data without a password or special key. Another advantage of this web application is that in caseyou move or copy an encrypted file, it can be opened using the same key used to create the file. An encrypted file never shows how much data is stored in itIn the last few years, the amount of information shared on electronic media has increased significantly. With increasing technology, there is a threat to data that is transmitted using the unsecured channel. Data needs to be hidden from unauthorized access, protected from unauthorized change, and available to an authorized entity when it is needed. Hence to ensure the Security and Confidentiality of data to be transmitted is very important and necessary. This requirement can be achieved by different data security techniques, some of the well-known techniques are Steganography and Cryptography. Cryptography techniques can be basically classified into two types' Symmetric-key cryptography and Asymmetric-key cryptography. In Symmetric-key, only one key is used by the sender as well as the receiver. In Asymmetric-key, two different keys are used: a public key which is disclosed to all, and a private key which is secretly known only to the authorized recipient of data.In Cryptography, even though the secret data is sent in an unreadable format, it gives the hint of the existence of secret data to the unauthorized recipient. However, in Steganography, such a hint is not given to the unintended recipient as the secret data is hidden inside another data. Therefore, Steganography can be more useful and advantageous when the use of cryptography is risky or prohibited .Cryptography provides security for the message transmitted over the network whereas steganography protects both message and the communicating parties Various secure methods are present but with increasing technology these methods become weak so there is a need to enhance these security methods for better and securely transmission of data

LITERATURE SURVEY

Cryptography is the art of hiding information by encryption and decoding it by decryption. Cryptography provides integrity, authentication, and maintain the secrecy of information. Steganography in Greek means "covered writing". Steganography is the art of concealing the existence of information within seemingly innocuous carriers .In a broad sense, the term Steganography is used for hiding a message within an image. There are varieties of steganography techniques available to hide the data depending upon the carriers used. Steganography and cryptography both are used to send the data securely. The same approach is followed in Steganography as in cryptography like encryption, decryption, and secret key. Steganography kept the message secret without any changes while in cryptography the original content of the message differs in different stages like encryption and decryption. Each technique in steganography as well as cryptography has its own advantages and disadvantages and is applicable for different domain of application. The main objective while providing security to the data is to achieved Security, robustness, imperceptibility and capacity.Different techniques available for Security of data are discussed here.
Ramya, G.- "Steganography Based Data Hiding for Security Applications", proposed a method of LSB algorithm in which the data to be transmitted are converted into binary values and hidden in the pixels of a cover image using an LSB Algorithm. Hidden data along with the cover image is called a stego image. To provide more security, the stego-image is further hidden within an audio signal. Then DWT is applied for the original audio signal and the audio's DWT coefficients and stego image pixels are both converted into binary values. The LSB of binary audio is replaced by binary pixel values. Thus, both the image and audio steganography method is utilized.
Aparna, V. S.-"Implementation of AES Algorithm on Text And Image using MATLAB", Proposed an encryption algorithm for the secure transmission of data. Advanced Encryption Standard (AES) a symmetric block cipher of 128-bits that uses the same key for encryption as well as for decryption is used. Here encryption and decryption are done on character message, string-text message, and image message. Plain text is inputted to encryption algorithm and output is an encrypted message i.e. ciphertext, then this ciphertext is given to decryption algorithm to get the decrypted message where plain text is reconstructed. This algorithm is highly efficient as decrypted output is the same as the input and there is no distortion in the output.
Cryptographic goals Cryptography can also defined as the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication. Cryptography is not the only means of providing information security, but rather one set of techniques. Of all the information security objectives the following four form a framework upon which the others will be derived:
(i) privacy or confidentiality
(ii) data integrity
(iii) authentication
(iv) non-repudiation.
I. Confidentiality is a service used to keep the content of information from all but those authorized to have it. Secrecy is a term synonymous with confidentiality and privacy. There are numerous approaches to providing confidentiality, ranging from physical protection to mathematical algorithms which render data unintelligible.
II. Data integrity is a service which addresses the unauthorized alteration of data. To assure data integrity, one must have the ability to detect data manipulation by unauthorized parties. Data manipulation includes such things as insertion, deletion, and substitution.
III. Authentication- is a service related to identification. This function applies to both entities and information itself. Two parties entering into a communication should identify each other. Information delivered over a channel should be authenticated as to origin, date of origin, data content, time sent, etc. For these reasons this aspect of cryptography is usually subdivided into two major classes: entity authentication and data origin authentication. Data origin authentication implicitly provides data integrity (for if a message is modified, the source has changed).
IV. Non-repudiation is a service which prevents an entity fromdenying previous commitments or actions. When disputes arise due to an entity denying that certain actions were taken, a means to resolve the situation is necessary. For example, one entity may authorize the purchase of property by another entity and later deny such authorization was granted. A procedure involving a trusted third party is needed to resolve the dispute.

SECURITY MECHANISMS

Three basic building blocks are used: Encryption is used to provide confidentiality, can provide authentication and integrity protection Digital signatures are used to provide authentication, integrity protection, and nonrepudiation Checksums/hash algorithms are used to provide integrity protection, can provide authentication One or more security mechanisms are combined to provide a security service. 2.1 ENCRYPTION Encryption and decryption Data that can be read and understood without any special measures is called plaintext or cleartext. The method of disguising plaintext in such a way as to hide its substance is called encryption. Encrypting plaintext results in unreadable gibberish called ciphertext. You use encryption to ensure that information is hidden from anyone for whom it is not intended, even thosewho can see the encrypted data. The process of reverting ciphertext to its original plaintext is called decryption.

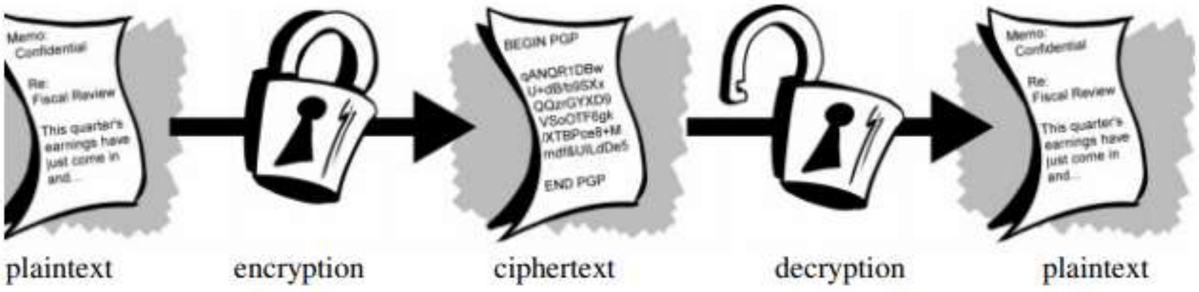


Fig. Encryption and Decryption

In conventional cryptography, also called secret-key or symmetric-key encryption, one key is used both for encryption and decryption. The Data Encryption Standard (DES) is an example of a conventional cryptosystem that is widely employed by the Federal Government.

METHODOLOGY

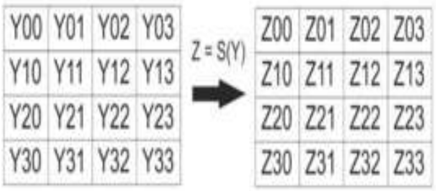
AES algorithms is one of the most complex algorithms of the recent times and takes a really long time to be broken. The complexity of this AES algorithm is hidden in it's complex working [9]. AES algorithm follows the given to convert our Plain Text to Cipher Text.

A. Transformation Step

The processing steps are known as Transformation steps in which the Plaintext is changed into an array before proceeding further with the steps.

B. Substitution Step

In this step each and every byte in the array is swapped with its sub byte.



Y00	Y01	Y02	Y03
Y10	Y11	Y12	Y13
Y20	Y21	Y22	Y23
Y30	Y31	Y32	Y33

Z00	Z01	Z02	Z03
Z10	Z11	Z12	Z13
Z20	Z21	Z22	Z23
Z30	Z31	Z32	Z33

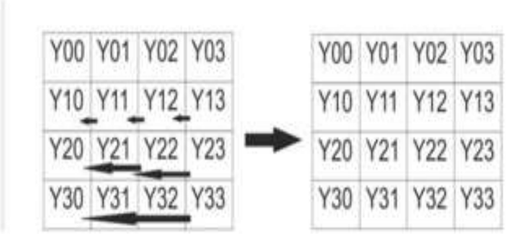
For Example-

Y12 is replaced with Z12, whereZ12=S(Y12) = Sub Byte of Y12Y12. Z12 = A Array Byte

S = Sub Byte

C. Row-shifting Step-

The initial row remains the same in this step but thesecond row is moved from Right to Left single stepat a time. These number of rounds keeps on increasing by one for every next row.

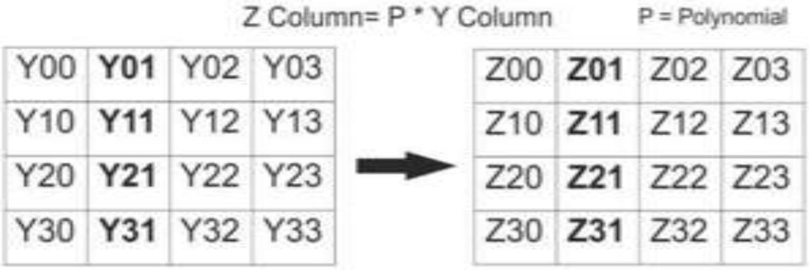


Y00	Y01	Y02	Y03
Y10	Y11	Y12	Y13
Y20	Y21	Y22	Y23
Y30	Y31	Y32	Y33

Y00	Y01	Y02	Y03
Y10	Y11	Y12	Y13
Y20	Y21	Y22	Y23
Y30	Y31	Y32	Y33

C. Column Mixing Step

In the following step the columns are selected one by one and each column is multiplied by a polynomial P.



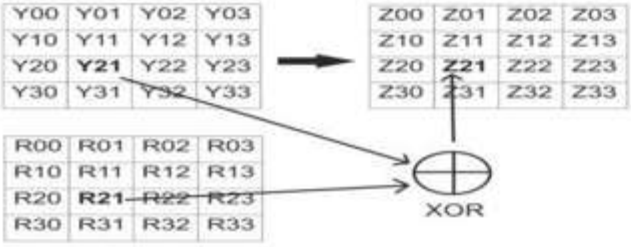
Y00	**Y01**	Y02	Y03
Y10	**Y11**	Y12	Y13
Y20	**Y21**	Y22	Y23
Y30	**Y31**	Y32	Y33

Z00	**Z01**	Z02	Z03
Z10	**Z11**	Z12	Z13
Z20	**Z21**	Z22	Z23
Z30	**Z31**	Z32	Z33

D. Round-Key Addition Step

In the final step a round key is added in each byte of an array. A XOR gate is used for the purpose of adding of round key in the array.

Y, Z = Array Byte R = Round Key



Y00	Y01	Y02	Y03
Y10	Y11	Y12	Y13
Y20	**Y21**	Y22	Y23
Y30	Y31	Y32	Y33

Z00	Z01	Z02	Z03
Z10	Z11	Z12	Z13
Z20	**Z21**	Z22	Z23
Z30	Z31	Z32	Z33

R00	R01	R02	R03
R10	R11	R12	R13
R20	**R21**	R22	R23
R30	R31	R32	R33

In the above process we can convert the Plain text into Cypher Text (encryption process). To convert the Cypher Text into Plain Text (decryption process) we have to reverse the same process and we will acquire the Plain Text.

Software Requirement:

- Csharp
- .Net,
- MySql
- Javascript

Hardware Requirement

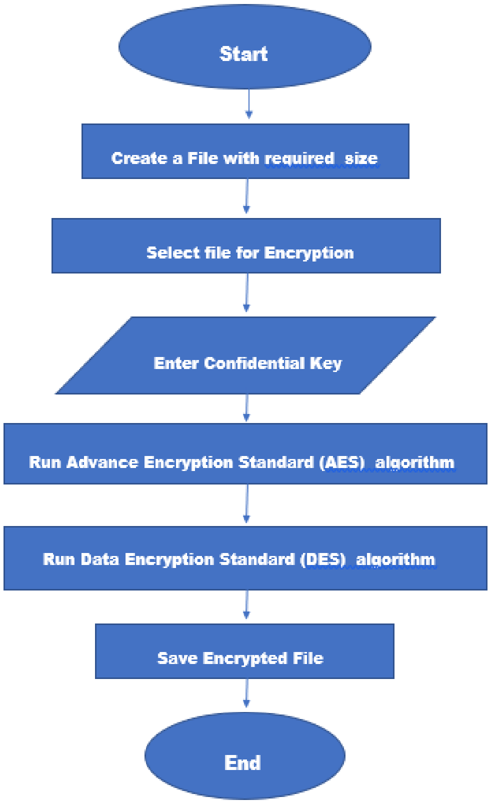
-HDD-100 GB or Higher

-RAM-4 GB or Higher

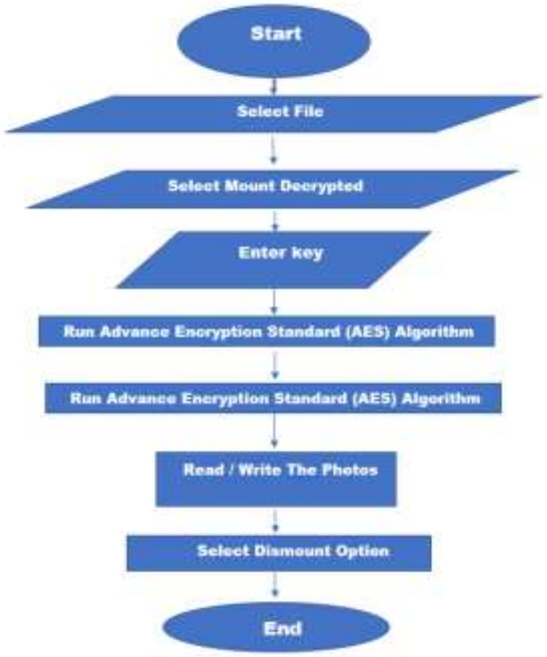
-Windows 10

FLOWCHART

1.Encryption


Start
Create a File with required size
Select file for Encryption
Enter Confidential Key
Run Advance Encryption Standard (AES) algorithm
Run Data Encryption Standard (DES) algorithm
Save Encrypted File
End

2.Decryption



CONCLUSION

We checked several cryptographic techniques and it is their components on which the whole method of cryptography works. Although, many difficulties arise in carrying out different cryptographic algorithms but there is always a technique that overpowers the concerns of threats. In our research paper we even conversed about diverse areas and sub techniques of cryptography. But although how hard we may try there's always a scope of error and threat. The systems, techniques and algorithms are getting advanced no doubt but we have to keep in mind that malicious persons are also using advanced techniques to steal the information by every fair or foul means. While enabling Transparent data Protection, it is a prudent idea that you should immediately backup the private key associated with the certificate and the certificate. If our certificate somehow gets inaccessible then you must attach the database on a different server, you must have backups of both: the certificate and the private key or else you will not be able to access the database. Deploying and integrating this system to its maximum potential requires massive funding and research.

REFERENCES

1. W. Stallings. Cryptography and Network Security: Principles and Practice 3rd Edition, Prentice Hall.
2. A .J. Menezes. Handbook of Applied Cryptography, 1996, CRC Press.
3. S. Singh. The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptograhy. Anchor Books, 2000.
4. B. Schneier. Applied Cryptography. John Wiley & Sons, New York, 1996.
5. D. Stinson. Cryptography (Theory and Practice), CRC Press,2002.
6. D. Gollmann. Computer Security. Wiley, 2000.
7. Arthur E. Hutt, Seymour Bosworth, Douglas B. Hoyt. Computer Security Handbook. John Wiley & Sons, 1995.
8. Data Encryption Standard. FIPS PUB 46, Appendix A, Federal Information Processing Standards Publication, January 15, 1977, US Dept. of Commerce, National Bureau of Standards.
9. J. Daemen and V. Rijmen. AES proposal: Rijndael. http://csrc.nist.gov /encryption/aes /rijndael/Rijndael.pdf.