A survey of various Cryptographic techniques and their Issues

Dr. Vivek Kapoor
Asst.Professor, Dept.Of Information Technology,
Institute Of Engineering & Technology ,
Devi Ahilya University, Indore, India.

Sandeep Verma
Dept. Of Computer Engineering ,
Institute Of Engineering & Technology,
Devi Ahilya University, Indore, India.

***Summary*- Cryptography is an art of hiding the data from illegal users. It converts the data from readable format that is known as plain text into unreadable format called as cipher text and vice versa. There are various types of cryptographic algorithms proposed over the years based on different techniques. These techniques uses various approaches to implement the basic functionality of cryptography i.e. to hide the information from unauthorized user. This survey describes various aspects of cryptographic algorithm and various issues related to cryptography. Along with it, a proposed work is there which addresses some of the core issues of cryptography along with their solutions.**

Key words- Encryption, symmetric and asymmetric cryptography, cryptanalysis, MD5 hash technique.

.

1. INTRODUCTION

Data security comprises of two parts i.e. data and its security. Data means collection of raw facts that are stored in databases, servers or various storing devices. In the age of Internet more and more data is being generated, hence it becomes very important to manage and secure the data. Data Security means securing the data from unauthorized access as well as securing it from corruption. With the growing technology, more and more data is being transmitted over the network hence it is essential to provide proper security measures to protect the data from being stolen or altered. Data security deals with various aspects of data security to provide a secure environment for data storage as well as transmission. There are number of examples over the Internet where vital information is either stored or transmitted over the network such as online banking, personal data in social media etc. Hence it is very important to device a way to protect these data from being compromised. Data security provides the best way to secure data from being compromised and also maintains privacy

1.1 SECURITY ASPECTS

As the data being transmitted goes through public network there are various security aspects that needs to be checked while transmission. Various security aspects are as follows:-

1.1.1 Authentication

It ensures that the identity of the individual is same as that of its claimed identity. It is one of the most important aspect of security, in order to ensure authenticity in public key cryptography sender encrypts the data with his private key which is exclusively with him only. Receiver decrypts the message with sender public key, here authenticity is insured as message can only be decrypted by someone's public key only if it was encrypted by same persons' private key.

1.1.2 Confidentiality

It ensures that message is available only to the intended users. As the message is being transmitted over the public network, it may get compromised. In order to ensure confidentiality encryption is used. The message is encrypted firstly and then sent over the network. Encrypted message cannot be understood by illegitimate users even if the message gets compromised. In this way confidentiality is achieved.

1.1.3 Integrity

It means the content of message should not be changed while transmitting. Sometimes some middle men between sender and receiver change the content of the message. To prevent this type of attack hash function can be used. Before sending the message its hash is calculated and then appended with the message. After receiving the message its hash is again calculated and compared with the appended one. If both the values are same there is no alteration in the content of message or else message has been altered. In this way we can check the integrity of the message.

1.1.4 Non-Repudiation

It means that the proof of origin of the message is ensured and sender cannot claim that the message doesn't belongs to him. Digital certificate can be used to ensure it. Message being transmitted is digitally signed by the sender and he cannot deny it later as his digital sign is there with the message.

1.1.5 Access Control

Itensures that only authorized person gets the permission to access the resources. It prevents the misuse of resources. It is achieved using various methods such as password protection, biometric identification etc.

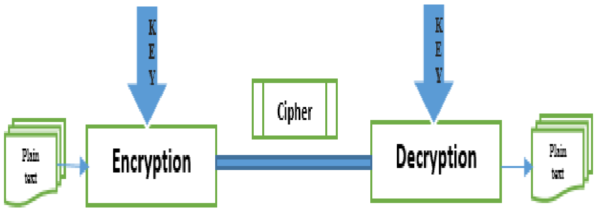
1.1.6 Availability

It ensures that the resources are always available for legitimate or intended user. Every time user wants the access to the resources it should get the resources.

2. CRYPTOGRAPHY

As stated earlier it is one of the oldest technique to secure data but it still provides the best way to hide information over the network. It is an art of hiding the data and to make it unreadable for unauthorized user. It works with following components:-

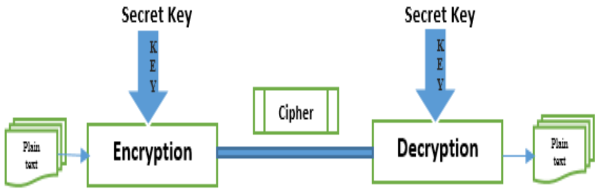
- Plain text –This is the original message that needs to be stored or transmitted over network.
- Cipher text – This is the unreadable message.
- Encrypt – It is the process of converting plain text into cipher text.
- Decrypt – It is the process of converting cipher text into plain text.
- Cryptographic Algorithm – This is the algorithm which converts plain text into cipher text.
- Public key – This is public that means known to everyone.
- Private Key – It is only known to sender.



Cryptographic system

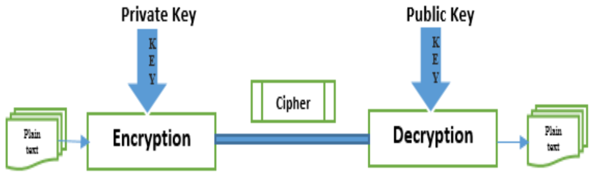
Cryptography can be broadly categorized into two different types depending on the nature of key being used i.e.

- Symmetric key Cryptography –As its name suggests it uses same key for both encryption and decryption. A common key is shared between the sender and receiver and both of them also uses the same algorithm.



Symmetric Key Cryptography

- Asymmetric key Cryptography –Here pair of keys i.e. public as well as private key are used to encrypt and decrypt the data. While encrypting the data private key whereas during decryption public key is used.



Asymmetric Key Cryptography

3. CRYPTANALYSIS

It is an art of deciphering the cipher text without knowing the key or encryption. Some of the methods related to this are as follows [7]:

 Cipher text Only: In this type of attack an attacker can access only cipher text or decrypted data but cannot access plain text. This type of attack is done on simple cipher like Caesar cipher where frequency analysis can be used to break the code.

- Known Plain text: In this type a cryptanalyst have plaintext and their corresponding cipher text. Attacker tries to find out the relation between these two.

- Chosen Cipher text: The attacker obtain the various plaintext corresponding to an arbitrary set of cipher text.

- Chosen Plain text: The attacker obtain the various cipher text corresponding to an arbitrary set of plain text.

- Adaptive Chosen Plain text: This is similar with the Chosen Plaintext, except in this attacker chooses subsequent set of plaintext which is based on the information obtain from previous encryption methods.

- Adaptive Chosen Cipher text: This is similar with the Chosen Cipher text, except in this attacker chooses subsequent set of cipher text which is based on the information obtain from previous encryption methods.

- Related Key Attack: Like the chosen plaintext, attack in which attacker can obtain only cipher text encrypted with the help of two keys. These keys are unknown but the relationship between these keys is known. Example two keys differ by a single bit.

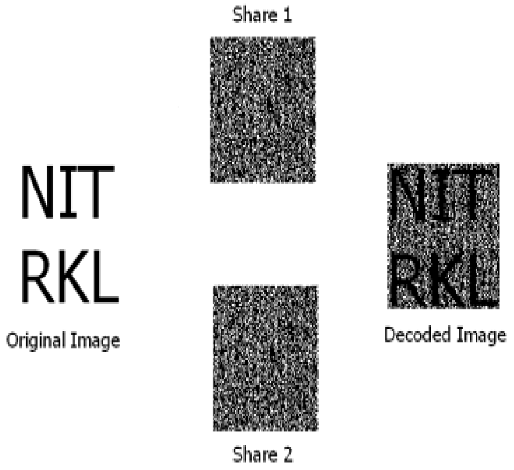
4. LITERATURE SURVEY

Here a brief introduction to various approaches of cryptography are discussed as a result of survey. They are as follows –

4.1 Characteristics of Visual Cryptography [1]

Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that the decryption can be performed by humans (without computers). The first visual cryptographic technique was developed by Moni Naor and Adi Shamir in 1994 [2]. It involved breaking up the image into n shares so that only someone with all n shares could decrypt the image by overlaying each of the shares over each other. Practically, this can be done by printing each share on a separate transparency and then placing all of the transparencies on top of each other. In their technique n-1 shares reveals no information about the original image. Fig 1 shows the working of visual cryptography. We can achieve this by using one of following access structure schemes [3]. 1:(2, 2) – Threshold VCS: This is a simplest threshold scheme that takes a secret image and encrypts it into two different shares that reveal the secret image when they are overlaid. No additional information is required to create this kind of access structure. 2 :(2, n) – Threshold VCS: This scheme encrypts the secret image into n shares such that when any two (or more) of the shares are overlaid the secret image is revealed. The user will be prompted for n, the number of participants. 3 :(n, n) – Threshold VCS: This scheme encrypts the secret image into n shares such that only when all n of the shares are combined will the secret image be revealed. The user will be prompted for n, the number of participants. 4:(k, n) – Threshold VCS: This scheme encrypts the secret image into n shares such that when any group of at least k shares are overlaid the secret image will be revealed. The user will be prompted fork, the threshold, and n, the number of participants.

This scheme also has drawbacks as the quality of the revealed image is not rich. Since it uses second phase takes the input as the result of first phase i.e. visual cryptographic encryption so definitely it will have the low contrast. But it provides the more secure shares so we can compromise with this.



Working of visual cryptography

.

4.2 Quantum Cryptography and its Issues [4]

Quantum cryptography is an emerging technology in which two parties may simultaneously generate shared, secret cryptographic key material using the transmission of quantum states of light. This paper consists of the main aspects of quantum cryptography and it investigates the information about where and all quantum cryptography takes place. Classical Cryptography suffers from Key Distribution problem, how to communicate the key securely between two pair of users. For years, it was believed that the only possibility to solve the key distribution problem was to send some physical medium – a disk for containing the key. In the digital era, this requirement is clearly unpractical. In addition, it is not possible to check whether this medium was intercepted – and its content copied –

or not. Public key cryptography came as a solution to this, but these too are slow and cannot be used to encrypt large amount of data. Public key cryptography suffers because even though one way functions have not been yet reversed with technological and mathematical advances it is possible. The steps of this method protocol are as follows.

- Alice communicates with Bob via a quantum channel sending him photons.

- Then they discuss results using a public channel

- After getting an encryption key Bob can encrypt his messages and send them by any public channel.

- One with the 0-90 degree basis and one with 45-135 degree basis. Alice uses her polarizer's to send randomly photons to Bob in one of the four possible polarizations 0, 45, 90,135 degree.

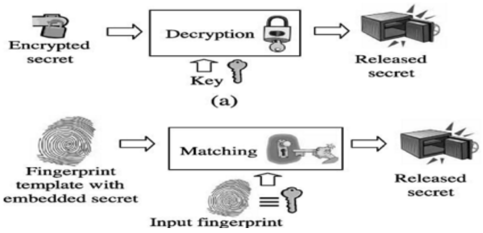
- Bob uses his polarizer's to measure each polarization of photons he receives.

- He can use the basis or but not both simultaneously.

Quantum cryptography, usually known as Quantum Key Distribution (QKD) provides powerful security. But it has some limitations. Following no-cloning theorem, QKD only can provide 1:1 connection. So the number of links will increase N (N-1)/2 as N represents the number of nodes. If a node wants to participate into the QKD network, it will cause some issues like constructing quantum communication line.

4.3 Bio Cryptosystems [5]

In this technique, various methods that monolithically bind a cryptographic key with the biometric template of a user stored in the database in such a way that the key cannot be revealed without a successful biometric authentication are used. This technique assess the performance of one of these bio- metric key binding/generation algorithms using the fingerprint biometric. The challenges involved in biometric key generation primarily due to drastic acquisition variations in the representation of a biometric identifier and the imperfect nature of biometric feature extraction and matching algorithms.



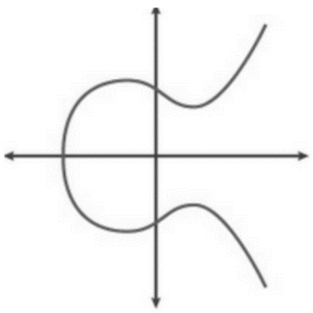
(a) In password-based authentication, a cryptographic key is the “secret” and the password is the “key.” (b) In the fingerprint-based authentication, a cryptographic key is the “secret” and fingerprint is the “key.”

A naive attack on a biometric system could be launched by successively presenting biometric samples from a representative population (either synthetically generated or actual samples) and the success of the attack is likely to be bounded by the weakest link in the security chain, i.e., operating point of the biometric matcher. In this regard, we believe it is more critical to focus on increasing the accuracy of the individual biometric matcher performance and on devising effective multibiometric strategies to deliver acceptable end-to-end system performance.

4.4 Elliptic curve cryptography (ECC) [6]

It is one of the most powerful branch of cryptography. ECC secure everything from HTTPS (Hyper Text Transfer Protocol Secure) connections to data transfer between data centers. An elliptic curve is a set of point-the smooth curve on the Cartesian plane, described by the following equation y2 + a1xy + a3y = x3 + a2x2 + a4x + a6,that was called as originally elliptic curve. If all unknown variables — real numbers, by replacement of variables the equation can be transformed to y2= x3+ ax+ b.

Basic view of elliptic curve is given on the



ECC is considered to be much more secure and useful than RSA and other first-generation public key cryptography systems. Public key cryptography means that we use two separate keys, public and secret key. The public key is used to encrypt plaintext and the private key is used to decrypt cipher text. In general public key algorithms are based on mathematical problems which admit no efficient solution, as integer factorization, discrete logarithm.

5. ISSUES OF CRYPTOGRAPHY

There are several issues related to cryptographic algorithm such as space complexity, time complexity and its resistance to various types of attacks. In order to implement an effective cryptographic algorithm all these aspects needs to be considered in order to make it robust. Let's discuss these issues:-

Time Complexity: It is the amount of time required to encrypt and decrypt the data. The algorithm should be designed in such a way that it should take as less time as possible for its execution. Time complexity plays an important role in modern cryptography as more and more systems are working in a real time environment nowadays. Hence while implementing a cryptographic algorithm it is necessary to consider its time complexity.

Space complexity: It is the amount of space consumed by cipher text as compared with plain text. As more and more mobile devices with limited connectivity in terms of data rate are being used nowadays, it is very essential to keep the size of cipher text being produced as small as possible as to deal with variable data rates. Thus it is very important to device a way to reduce the size of cipher text as much as possible to increase data transmission efficiency.

Security: The very purpose of cryptography is to secure the data being transmitted over the network from various types of attacks. The data being transmitted is always vulnerable to various types of attacks such as men in the middle attack, brute force attack etc. Thus in order to prevent the data from being compromised it is necessary to protect the data from unauthorized users. The feasibility of cryptography must be tested against such attacks so as to secure the data being sent. Hence providing security is one of the major issue of cryptography.

6. PROPOSED WORK

The proposed system is a cryptographic algorithm which accepts any kind of data for processing. In addition of that the simulation of the proposed methodology enable a user to send and receive data using the application. The proposed simulation first accepts the data form the user and then compress it in order to reduce the data size. After doing that it uses the proposed cryptographic algorithm data to manipulate the data into cipher text. The generated cypher text is compressed again and using file splitter utility and then it is transmitted much efficiently on network. On the other end the receiver follows the same procedure in reverse direction to decrypt it.

The essential features and objectives to accomplished during the proposed study.

1. Providing the simulation of secure file transfer utility via hybrid cryptographic algorithm.

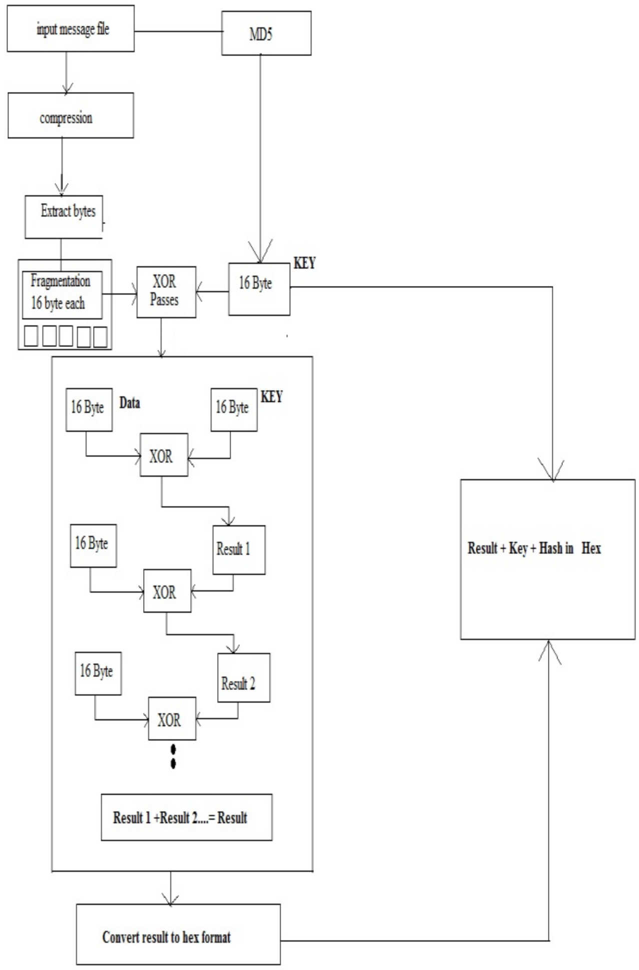
2. Designing and implementing the hybrid cryptographic technique in order to reduce the space and time complexity by compressing the data being sent.

3. Cross validating the data integrity using the MD5 hash function.

4. Reducing the size of cipher text so as to make data transmission more efficient.

7. PROPOSED METHODOLOGY

The overview of the proposed systems components and discussed in this section of document.



Input file: This is the input file to be sent over the network.

Zip compressor: It compress the data in zip format.

MD5: The compressed zip file is produced before the MD5 algorithm to generate 128 bit hash. This hash is used to check the data validity at the receiver end. If the sender generated hash matched with the receiver end hash than the data is valid otherwise data is corrupt.

Key (16 bytes): This is MD5 generated hash which is separately treated as key form encryption.

Extraction and Fragmentation: The data after compression is extracted in the form of bytes and is further fragmented to chunks of 16 byte each.

XOR passes: In this phase the 16 byte data blocks and 16 byte key blocks are treated using XOR operator. The resultant of each pass is input for new 16 byte data and the process goes on until whole data is processed. The combination of result of each phase is combined to form final result.

Convert result to hex code: In this phase the XOR passes outcome i.e. result is converted into hexadecimal encoding. The encoding of message also reduces the amount of XOR results.

Transmission: in this phase the entire results of XOR passes are organized into one file and then the generated hash code are added to data file and send to the receiver end.

Convert result to hex code: in this phase the XOR passes outcomes are converted into hexadecimal encoding. The encoding of message also reduces the amount of XOR results.

8. CONCLUSION

With the advancement in technology, more and more valuable data is now being transmitted over the public network. There are number of possible vulnerabilities which could compromise the data. Hence to protect the data from unauthorized users various measures need to be taken. We have seen various aspects of security, how these measures can be implemented. We have discussed the importance of cryptography, its types and its issues. Later we have done a survey on different techniques of cryptography. Then, we have discussed some issues related to the performance of cryptography. We have studied all the above aspects of cryptography and proposed our technique of cryptography which is supposed to enhance the performance as well as security. In this survey paper we have proposed a method, later we will implement it to analyze its performance.

REFERENCES

[1] A Novel Visual Cryptography Scheme -Debasish Jena1, Sanjay Kumar Jena2 1Centre for IT Education, Biju Pattanaik University of Technology, Orissa 751010, India 2Department of Computer Science & Engineering, National Institute of Technology Rourkela, Orissa 769 008, India debasishjena@ieee.org, skjena@nitrkl.ac.in

[2] M.Naor and A. Shamir “Visual cryptography”. Advances in Cryptology EUROCRYPT ’94. Lecture Notes in Computer Science, (950):1–12, 1995.

[3] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, Visual Cryptography for General Access Structures, Information and Computation, Vol. 129, No. 2, (1996), pp. 86-106.

[4]A Survey on Recent Security Trends using Quantum Cryptography- T. Rubya1 Lecturer, Karpagam University N. Prema Latha2 Lecturer, Karpagam University B. Sangeetha3 Lecturer, Karpagam University.

[5]Biometric Cryptosystems: Issues and Challenges-UMUT ULUDAG, STUDENT MEMBER, IEEE, SHARATH PANKANTI, SENIOR MEMBER, IEEE, SALIL PRABHAKAR, MEMBER, IEEE, AND ANIL K. JAIN, FELLOW, IEEE

[6] ELLIPTIC CURVE CRYPTOGRAPHY O. O. Meleshko, O. O. Kovalskiy

[7] A Survey Report on Various Cryptanalysis Techniques Ashish Kumar Kendhe, Himani Agrawa