A Review of Some Popular Cryptography Techniques

Abhijit A. Pachore[1], Prof. Arpit Solanki[2]

[1,2] *Department of Computer Science and Engineering*
RKDFS School of Engineering, Indore

ABSTRACT

The backbone of the modern world is electronic communication. Data is transferred from one place to another in almost no time using the electronic medium. But it also exposes the confidential data to the intruder. RSA is the most common and efficient cryptography technique that is used for the purpose of encrypting the content and then sending it over the channel, then than at receivers end the content is decrypted and converted in to original form. Although there are many security mechanisms are available. But there is a continuous need to improve the existing methods. Cryptography is a security mechanism which caters the security services of world in perfect manner.
Keywords: *cryptography, information security, RSA, AES, encryption, decryption, cryptography techniques.*

---

1. Introduction

The network security becomes more important with the development of various techniques of network development. With the growth in the use of world wide web, this has become even more important as the users can access tools and edit the information. While communicating any information via an unsecure channel to its righteous owner, security issue becomes important. To avoid such problem, cryptography and steganography are the main ways of communicating such information in a stealth mode without anyone knowing what it is.

The global society has faced many changes because of the digital revolution. Along with all, this has also increased the number of hackers and viruses. There is a need of a system which can control the curious eyes from getting in a harm way. In such a situation, steganography and cryptography emerge as a savior for such important information. [1,2]

With the increase in the content on the web, the increase of viruses and bad eyes in the form of hakers, privacy has become an important issue among many. In such situation, Image Steganography has many important roles and application. Specially, when two parties want to communicate secretly.

In today's world, security is a major problem especially when it comes to hiding secret information from total strangers. So, converting a message into a form that cannot be easily cracked is an ultimate option for all. Due to the new and improved techniques used by hackers, sharing information on the internet is less secure now a days. To overcome such problems have evolved techniques like steganography and cryptography.

If we uncover the pages of history we find that in those times too, secret information was passed from one party to another via various means like invisible ink, tattoos and much more and that has become the brain child for the present techniques like cryptography where the online secret information sharing has become more secure for parties who have a sensitive information that cannot fall in wrong hands.

1.1 Cryptography

Cryptography is the art and science of achieving security by encrypting information to make them non-readable format.

Basic terms used in cryptography

- **Plain text**-Clear text is a readable format or original message understand by any person. For example, if A wants to send a message to B + "Hello" then here "hello" is a plain text message.
- **Cipher text**-It is unreadable message or after the encryption the resulting message is called cipher text. For example, "sd45@#$" is a Cipher Text produced for "hello".
- **Encryption**-The process of plain text converts cipher text called encryption
- **Decryption**-The process of cipher text converts plain text called decryption.

2. Related Work:

2.1 Encryption algorithm and key

Every encryption and decryption process has two aspects:

- Algorithm
- key

There are two types of keys in cryptography

Symmetric key -Symmetric key uses a single key for both encryption and decryption.

Asymmetric key –Asymmetric key uses one key for encryption and another key for decryption.

2.2 Comparison of various Symmetric Key Cryptography Algorithms

Also called a private key cryptography, the encrypting and decrypting keys are similar.

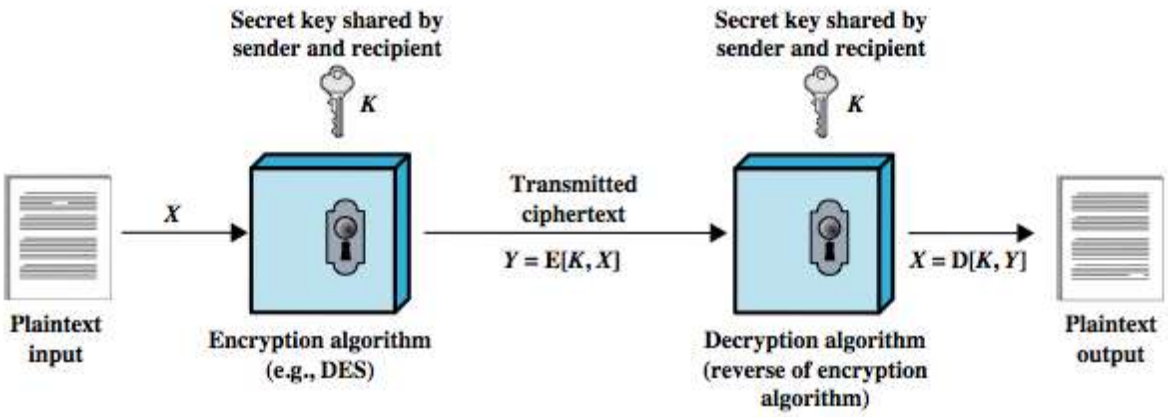

figure 1: symmetric key encryption

Table 1 Different symmetric key encryption algorithm [7]

Algorithm Name	Maximum size of KEY	Use of algorithm/Security
DES	56 bits	Insecure
3DES	168 bits	Replaced by AES
AES	128,192, or 256 bits	US Govt classified information

IDEA	128 bits	Used in PGP, very secure
BLOWFISH	32 to 448	Public domain
RC5	Up to 2040	Secure for 72-bits or more

2.3 Comparison of various Asymmetric Key Cryptography Algorithms[6]

Also called a public key cryptography, the encrypting and decrypting keys are different.

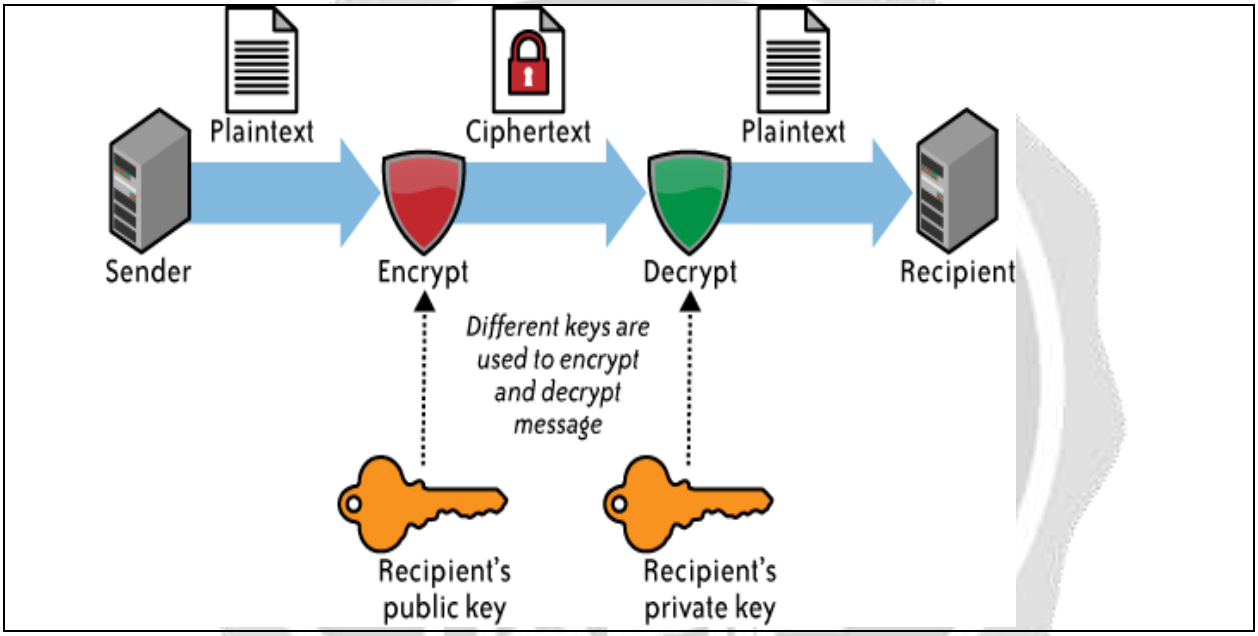

Figure 2: Asymmetric-key cryptography

Table 2 Different asymmetric key encryption algorithm[6]

Algorithm Name	**Use of algorithm/Security**
Diffie-Hellman	Key exchange, not encryption
RSA	Secure, used by SSL
Elgamal	Used in GPG and PGP

- **Rivest Shamir Adleman (RSA)**

A public key encryption algorithm developed by Ronald Rivest, Adi Shamir, and Leonard Adleman in 1977. It widely used in electronic commerce protocols, and is believed that its security depends on the difficulty of decomposition of large numbers. RSA is secure because it is able to Public Key Cryptography is based on the principle of one way functions that can be easily computed while their inverse function is difficult to calculate. It employs two different keys related mathematically such that one is used for encryption and the other for decryption.

Its two main keys are used i.e. in encryption and decryption. RSA is an algorithm based in the theorem of factoring two large prime numbers. [3, 5]

RSA Algorithm has following steps.

1. Select two large prime numbers P and Q.

2. Calculate N=P*Q

3. Select the public key (encryption key) E such that it is not a factor of (P-1) and (Q-1).

4. Select private key (decryption key) D such that the following equation is true:

(D*E) mod (P-1) * (Q-1) =1

5. For encryption, calculate the cipher text CT from the plain text PT as follows:

$CT=PT^E \bmod N$

6. Send CT as the cipher text to the receiver.

7. For decryption, calculate the plain text PT from the cipher text CT as follows:

$PT=CT^D \bmod N$

- **Least Significant Bit(LSB)**

The most widely used algorithm is the Least Significant Bit technique (LSB). In this, the least significant bits of an image are random noise and the quality of the images remains unchanged even if these are changed. There are mainly two methods in this: [4]

- The LBS replacement in which the LBS of the pixels are replaced with the message.
- The LBS Matching in which the pixels are increased or decreased to adjust according to the message.
- It is hard to detect and decode the hidden message due to the distribution of message bits inside the imaged covers.
  Least Significant Bit (LSB) is a technique of hiding a data within an image. For a human eye, a 24 bit true color image will showcase a minimum change. Let's take an example here:-
- we have three adjacent pixels (nine bytes) with the following RGB encoding:
  10010101 10010110 10011111
  00001101 00001111 00010000
  11001001 11001010 11001011
- Now, if we want to hide the following 9 bits of data 101101101. If we overlay these 9 bits over the LSB of the bytes above, we get the following (where bits in bold have been changed) pixels:
  10010101 10010111 10011111
  00001100 00001110 00010000
  11001001 11001011 11001011

- **Peak Signal to Noise Ratio(PSNR)**

Peak Signal to Noise Ratio (PSNR) is calculated to measure the stego image's quality. The quality of a digital image

or video is assessed through this statistical measurement method. The larger the PSNR value is smaller will be the possibility of a visual attack by a human. [8]

Common Problems in Existing RSA Variants [8]:

- The main disadvantage of RSA decryption is its slower speed
- Not secure against wiener's attack
- Problem arise to common modulus attack
- known plaintext attack are possible
- Low decryption exponent attack if we know the decryption exponent.
- The decryption time slow.

Conclusion:
This paper has elaborated the basic concept of cryptography and the key management schemes. A review of modern methods is also done in brief. The most of the modern data security techniques have been reviewed. Each of the method has been analyzed with the advantages and the disadvantages. Then a list of common problems in the current version has been identified. On basis of the research gap identified, the problem was formulated.

References:

1. William Stallings " Network Security Essentials (Applications and Standards)", Pearson Education, 2004.
2. National Bureau of Standards, " Data Encryption Standard," FIPS Publication 46, 1977.
3. Prashant Sharma, "Modified Integer Factorization Algorithm using V-Factor Method", 2012 Second International Conference on Advanced Computing & Communication Technologies, IEEE 2012.
4. Prof.Dr.Alaa Hussein Al-Hamami,Ibrahem Abdallah Aldariseh ,"Enhanced Method for RSACryptosystem Algorithm" 2012International Conference onAdvanced Computer Science
Applications and Technologies, IEEE 2012.

5. V. "Rijndael: The Advanced Encryption Standard." Dr. Dobb's Journal, March 2001.
6. Shashi Mehrotra Seth, 2Rajan Mishra," Comparative Analysis Of Encryption Algorithms For Data Communication", IJCST Vol. 2, Issue 2, June 2011 pp.192-192.
7. Dr. S.A.M Rizvi1 ,Dr. Syed Zeeshan Hussain2 and Neeta Wadhwa" A Comparative Study Of Two Symmetric Encryption Algorithms Across Different Platforms",
8. G. jai Arul jose,research scholar,sathyabama University,Chennai-possible Attackon RSA Signature.