COMPARATIVE STUDY OF CRYPTOGRAPHY WITH DIFFERENT ENCRYPTION ALGORITHMS

[1]Nishi Patel, [2] Prof.Kaushal Gor

[1]Student, [2] Professor
[1]Dept, of MCA, [2] Dept.of MCA,

[1]Parul University, Vadodara, India.

***Abstract*:** Cryptography can be briefly explained as the study of technique for secure communication and data transfer in presence of intruders. Encryption is quite interesting technology which works on the principle of scrambling and converting data into cipher text which is unreadable format of simple data.One of the most vital piece of IT is cryptography techniques as it responsible for securing sophisticated data which is going to transfer through network. This research paper includes overview study of cryptography techniques and algorithms. The algorithms are classified and conclusions are drawn on the basis of the advantage and disadvantages. The main purpose of this paper is to compare the working and viability of different algorithms available in cryptography.

Keywords: **Cryptography, Symmetric, Asymmetric, Encryption-Decryption Algorithms.**

1.INTRODUCTION

A. Cryptography:

In the current orientation of the world, the technologies have advanced so much that most of the individuals prefer using the internet as the primary mean to relegate data from one end to another across the world. There are many possible ways to broadcast data using the internet: via e-mails, chats, etc. The data transition is made very cinch, fast and accurate using the internet. However, one of the main challenge with sending data over the internet is the "security threat" it poses i.e. the personal or privy data can be bagged or hacked in many ways.

Cryptography is the technique of scrambling plain text. This secures data and information from any unessential and essential attacks. Therefore, it give integrity, confidentiality, non-repudiation and authenticity to the secret data. The texts involved in cryptography are plain and cipher texts. Plain texts are human readable texts and the information which the sender intends to send. The plain text is encrypted to an illegible form called the cipher text. Based on the encryption methodology used, it is differentiated as symmetric and asymmetric cryptography.

Therefore it becomes very important to take data security into consideration, as it is one of the most necessary factors that need attention during the process of data transferring. Cryptography is the science or study of techniques of hidden writing and message hiding. Particular encryptionalgorithms require the key that should be the same length as the message to be encrypt, yet other encryption algorithms can operate on much smaller keys relative to the message. Decryption is often restricted along with encryption as it's paradoxical. Decryption of encrypted data results in the actual data. Decryption is the process of taking encoded or incrusted text and changing it back end text that you or the computer can read and understand.

This term could be used to describe a method of decrypting the data manually or with decrypting the data using the proper codes or keys. Data may be encoded to make it difficult for someone to confidential the information. Some corps also encrypts data for general upholding of corps data and interchange secrets. If this data needs to be inspecting, it may require decryption. If a decryption pass code or key is not available, special software may be required to decrypt the data using algorithms to crack the decryption and make the data readable.

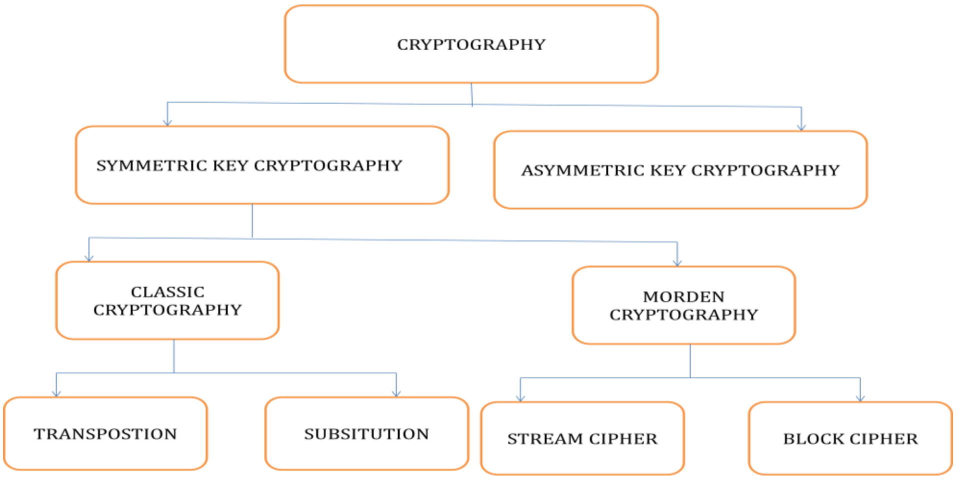


figure 1: division of cryptography

1.1 Symmetric Key Cryptography:

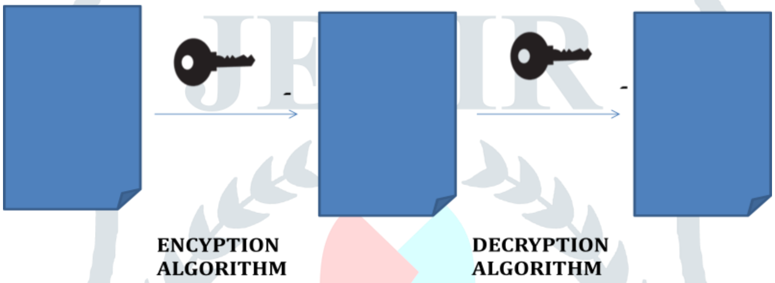


figure 2: symmetric key cryptography

Symmetric key cryptography is also known as secret-key either public key cryptography. In this type of cryptography, the sender and receiver shares a common key for both encryption and decryption. The key used in this technique is certified by oneself. The key is shared through communication. If an intruder obtains the key, the whole process is compromised and the intruder can easily decrypt the message. This method is preferred because of its fast service and less resource requirement.

A symmetric key algorithm uses the concept of a key and lock to encrypt plaintext and decrypt cipher text data. The same “key” is used for both encode and decode the file. They divided further in two types by stream ciphers and block ciphers. In a stream cipher , where plain text and pseudo-random both are combine with each other and create non readable stream which is also known as cipher digit stream. In Block ciphers it will take the number of bits and encode them as a single unit also known as rounds, adding the plaintext so that it’s a multiple of a block size.

The algorithm itself is not kept a secret, here sender and receiver both have duplicates of keys at some safe place. The use of the coequal key is also one of the disadvantage of symmetric key cryptography because if some unknown person can get hold of the key, they can easily decrypt your data and do mischief with that so sometimes it can be dangerous.

1.1.1Algorithms in Symmetric Key

I. DES (DATA ENCRYPTION STANDARD)
II. TRIPALDES (TRIPAL DATA ENCRYPTION STANDARD)
III. AES (ADVANCED ENCRYPTION STANDARD)

I.DES:

DES stands for The Data Encryption Standard; it is the first symmetric algorithmand more well-known algorithms of the modern cryptographic era. Today it is widely prudent insecure. IT was developed in the 1970's by IBM and was later submitted to the National Bureau of Standards (NBS) and National Security Agency (NSA).

The design which is given by NSA gives sparkedcontentions rumours of backdoors, creating widespread research. It was not there until 1976 that DES was approved as a cryptographic standard and published in FIPS.

In the 1990's, computing seventy two quadrillion attainable keys for a fifty six bit DES key appeared extremely inconceivable. This would are true for one pc, however in 1997 a gaggle of pc scientists junction rectifier by Rocke Verser used thousands of volunteer computers to crack DES inside 24 hours, thereby making him and his team the winner of the $10,000 DES Challenge.

After this challenge they named the method as double DES and Triple DES, simply layering the cipher so that it would have to decrypt three times to each data block. Triple-DES continues to be employed in some places, but AES (see below) has become the new standard since then.

II.AES:

The Advanced Encryption Standard or AES was established by the National Institute of Standards and Technology (NIST) in 2001.The key length of AES which was adapted by US government is 128 bit.192bit and 256 bit.

AES features a fairly easy mathematical framework that some argue makes it vulnerable to attack. The theoretical XSL attack was proclaimed in 2002 and since then security researchers like Bruce Schneier have found ways in which they can take advantage of components of the algorithmic rule. However, it's necessary to notice that even in Bruce Schneier's article, he states that there's no reason to panic simply nevertheless since they solely break eleven of the full fourteen rounds of AES-256, taking 2 raise to 7 time.

Itadditionally needs the cryptologist to own access to plaintexts encrypted with connected multiple keys, which still gives AES a higher safety margin but just not as high as previously thought.

III.Triple DES:

Replacing the original Data Encryption standard algorithm was the main task of Triple DES because in DES the hackers adapted to defeat it by using relative cases. There was a time in the lifeline of Triple DES that it was the most used symmetric algorithm worldwide and was highly recommended by field experts.

Three individual keys of 56 bit each is used by Triple DES. The length of the total key goes up to 168 bits but expert recommends using 112 bit key strength for better encryption

Triple DES is still one of the reliable methods in terms of dependable hardware encryption but with passing time it is going to be phased out as new and efficient methods are constantly developing.

1.2 Asymmetric Algorithms:

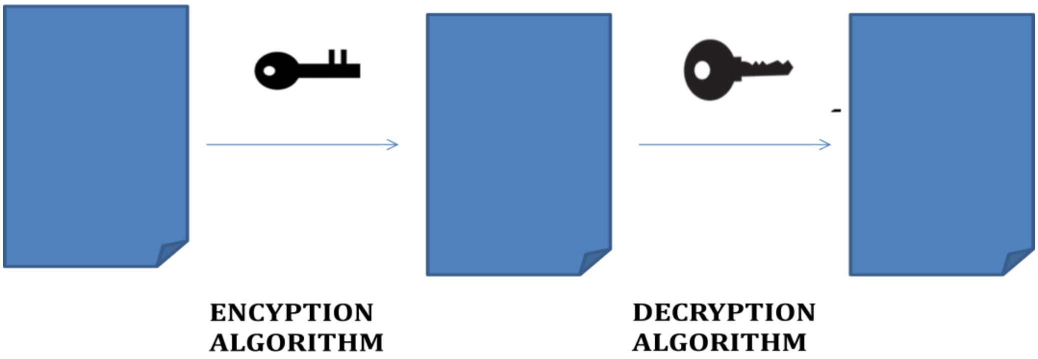


figure 3: asymmetric key

Public key encryption is the other name for Asymmetric Algorithm and it works on the principle of having two key which are mathematically related to each other known as public key and private key. Public can be shared online but sharing private key will be considered a big mistake. Anyone who holds public key can encrypt data but the decryption is only possible by the one who have the private key. The data can only be kept secret if the privacy of the key is maintained.

The conversion of the simple text into cipher is carried out by public key and the vice versa is done using the private key of the receiver. Because digital signatures are used to attach the keys the concept of self-certification is not available here...Better authentication and security can be achieved with this method and the privacy remains intact in this.

I.RSA:

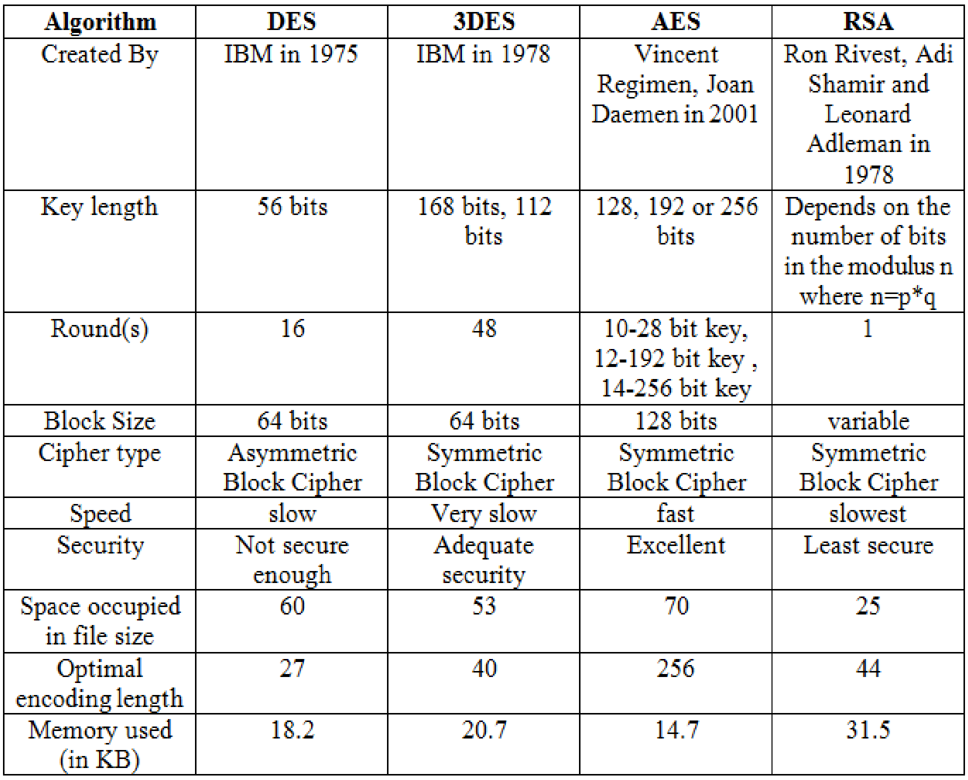
RSA stands for the Rivet-Shammir-Adleman algorithm, as per latest report it is the most widely used standard on internet today. The main algorithm in roots of RSA is that it is based on factorization of prime number and working backward by multiplying that number as the multiplied number will get larger. ‘RSA problem’ is the term used for the challenges of breaking RSA.

RSA is very slow because the it is mainly used to encrypt and then decrypt the symmetric key which will then encrypt the communication, this process requires a lot more time as compared to other algorithms.This amount of work is a huge advantage in terms of security as the end result is a very strong and secure channel for communication.

In 1998, Daniel Bleichenbacher explained how one can exploit PKCS#1 file and he was successfully able to get the private key of the victim and utilize it to recover session and decrypt data.Due to this RSA Laboratories updated the method with new version of PKCS#1. Even after continuous attack on the RSA algorithm it is still one of the most widely used and secure algorithm, this viewpoint might change after Quantum computer becomes mainstream

2.COMPARITION OF ALGORITHM

table 1: comparative study of algorithms



Algorithm	DES	3DES	AES	RSA
Created By	IBM in 1975	IBM in 1978	Vincent Regimen, Joan Daemen in 2001	Ron Rivest, Adi Shamir and Leonard Adleman in 1978
Key length	56 bits	168 bits, 112 bits	128, 192 or 256 bits	Depends on the number of bits in the modulus n where n=p*q
Round(s)	16	48	10-28 bit key, 12-192 bit key , 14-256 bit key	1
Block Size	64 bits	64 bits	128 bits	variable
Cipher type	Asymmetric Block Cipher	Symmetric Block Cipher	Symmetric Block Cipher	Symmetric Block Cipher
Speed	slow	Very slow	fast	slowest
Security	Not secure enough	Adequate security	Excellent	Least secure
Space occupied in file size	60	53	70	25
Optimal encoding length	27	40	256	44
Memory used (in KB)	18.2	20.7	14.7	31.5

3.THE FUTURE OF ENCRYPTION

Cyber-attacks are constantly developed, so security specialists must stay busy in the lab for constructing new schemes to prevent them from attacking. Experts finds new method name as honey pot encryption in which dummy data will be supplied to the hackers which every incorrect key code which will divert the hacker. This method will not only hide the correct key into false hops but also will slow down the attacker by a lot. For the future aspect of Encryption there are emerging technologies such as Quantum key distribution which allows sharing data in form of photon by using fiber optics which might be considered as a viable option in future.

Encryption must be used whenever possible in day to day activities such as Emails, data storage and must be included in essential security tools. It is almost impossible for any security protocol to work as a full-proof shield but without this kind of mechanism it will be an open invitation to the attackers.

4.CONCLUSION

Each of cryptographic algorithms has weakness points and strength points. We select the cryptographic algorithm based on the demands of the application that will be used.

From the experiment results and the comparison, the blowfish algorithm is the perfect choice in case of time and memory according to the criteria of guessing attacks and the required features, since it records the shortest time among all algorithms. Also, it consumes the minimum memory storage.

If confidentiality and integrity are major factors, AES algorithm can be selected. If the demand of the application is the network bandwidth, the DES is the best option.

5. REFERENCES

1. http://etutorials.org/Linux+systems/unix+internet+security/Part+II+Security+Building+Blocks/Chapter+7.+Cryptography+Basics/7.2+Symmetric+Key+Algorithms/
2. https://blog.storagecraft.com/5-common-encryption-algorithms/
3. https://www.globalsign.com/en-in/blog/glossary-of-cryptographic-algorithms/
4. https://www.edureka.co/blog/what-is-cryptography/
5. http://www.laits.utexas.edu/~anorman/BUS.FOR/course.mat/SSim/life.html
6. https://resources.infosecinstitute.com/basics-of-cryptography-the-practical-application-and-use-of-cryptography/#gref
7. https://symbiosisonlinepublishing.com/computer-science-technology/computerscience-information-technology32.php
8. http://www.electrodummies.net/en/asymmetric-encryption/
9. https://www.ssh.com/manuals/server-zos-product/55/ch06s02s02.html

http://www.uobabylon.edu.iq/eprints/paper_1_2264_649.pdf