© 2019 IJSRSET | Volume 6 | Issue 5 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section : Engineering and Technology
DOI : https://doi.org/10.32628/IJSRSET

A Survey on Comparison of Various Encryption Algorithms for secured data Communication

Masood Ahmad, Ravi Pratap Singh
Department of Computer Science and Engineering, Azad institute of Management and Technology Luck now
Uttar Pradesh, India

ABSTRACT

In this paper survey is Encryption is the process of encoding information or data in order to prevent unauthorized access. These days we need to secure the information that is stored in our computer or is transmitted via internet against attacks. There are different types of cryptographic methods that can be used. Basically, the selecting cryptographic method depends on the application demands such as the response time, bandwidth, confidentiality and integrity. However, each of cryptographic algorithms has its own weak and strong points. In this paper, we will present the result of the implementation and analysis that applied on several cryptographic algorithms such as DES, 3DES, AES, RSA and blowfish. Also, we will show the comparisons between the previous cryptographic techniques in terms of performances, weaknesses and strengths.

Keywords : Probabilistic Encryption , Encryption, Decryption, Cryptography

I. INTRODUCTION

How Encryption Works

Encryption is an interesting piece of technology that works by scrambling data so it is unreadable by unintended parties. Let's take a look at how it works with the email-friendly software PGP (or GPG for you open source people).Say I want to send you a private message, so I encrypt it using either one of these programs. Here's the message:

“wUwDPglyJu9LOnkBAf4vxSpQgQZltcz7LWwEquh
dm5kSQIkQlZtfxtSTsmaw
q6gVH8SimlC3W6TDOhhL2FdgvdIC7sDv7G1Z7pC
NzFLp0lgB9ACm8r5RZOBi
N5ske9cBVjlVfgmQ9VpFzSwzLLODhCU7/2THg2iDr
W3NGQZfz3SSWviwCe7G
mNIvp5jEkGPCGcla4Fgdp/xuyewPk6NDlBewftLtHJ
Vf
=PAb3”

Once encrypted, the message literally becomes a jumbled mess of random characters. But, equipped with the secret passcode I text you, you can decrypt it and find the original message.

“Come on over for hot dogs and soda!”

Whether it's in transit like our hot dog party email or resting on your hard drive, encryption works to keep prying eyes out of your business – even if they happen to somehow gain access to your network or system. If you want to learn more about how encryption helps protect business data, you can read our article on how encryption aids cloud security.

The technology comes in many forms, with key size and strength generally being the biggest differences in one variety from the next.

Data Encryption is the process of converting the plaintext into Encoded form (non-readable) and only authorized person/parties can access it. Data security is an essential part of an Individual/organization; it can be achieved by the using various methods. The encrypted data is safe for some time but never think it is permanently safe. After the time goes on there is chance of hacking the data by the hacker. Fake files are transmitted in the same manner as one can sends the encrypted data. There are many algorithms available in the market for encrypting the data. Encryption Key has the major role in the overall process of data

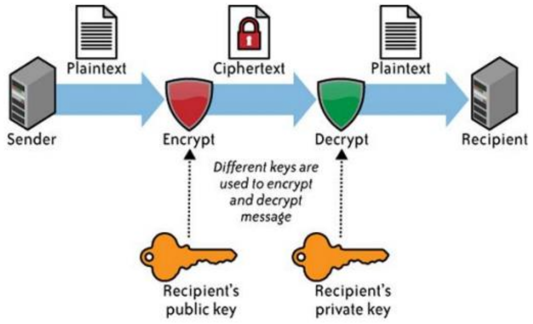


Fig1 Encryption and Decryption process

II. METHODS AND MATERIAL

A. Types of Encryption algorithms

1. Triple DES

Triple DES was designed to replace the original Data Encryption Standard (DES) algorithm, which hackers eventually learned to defeat with relative ease. At one time, Triple DES was the recommended standard and the most widely used symmetric algorithm in the industry.

Triple DES uses three individual keys with 56 bits each. The total key length adds up to 168 bits, but experts would argue that 112-bits in key strength is more like it.

Despite slowly being phased out, Triple DES still manages to make a dependable hardware encryption solution for financial services and other industries.

2. RSA

RSA is a public-key encryption algorithm and the standard for encrypting data sent over the internet. It also happens to be one of the methods used in our PGP and GPG programs.

Unlike Triple DES, RSA is considered an asymmetric algorithm due to its use of a pair of keys. You've got your public key, which is what we use to encrypt our message, and a private key to decrypt it. The result of RSA encryption is a huge batch of mumbo jumbo that takes attackers quite a bit of time and processing power to break.

3. Blowfish

Blowfish is yet another algorithm designed to replace DES. This symmetric cipher splits messages into blocks of 64 bits and encrypts them individually.

Blowfish is known for both its tremendous speed and overall effectiveness as many claim that it has never been defeated. Meanwhile, vendors have taken full advantage of its free availability in the public domain.

Blowfish can be found in software categories ranging from e-commerce platforms for securing payments to password management tools, where it used to protect passwords. It's definitely one of the more flexible encryption methods available.

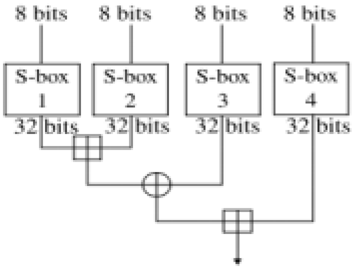


Fig 2 : Blowfish Cryptographic Algorithm

4. Twofish

Computer security expert Bruce Schneier is the mastermind behind Blowfish and its successor Twofish. Keys used in this algorithm may be up to 256 bits in length and as a symmetric technique, only one key is needed.

Twofish is regarded as one of the fastest of its kind, and ideal for use in both hardware and software environments. Like Blowfish, Twofish is freely available to anyone who wants to use it. As a result, you'll find it bundled in encryption programs such as PhotoEncrypt, GPG, and the popular open source software TrueCrypt.

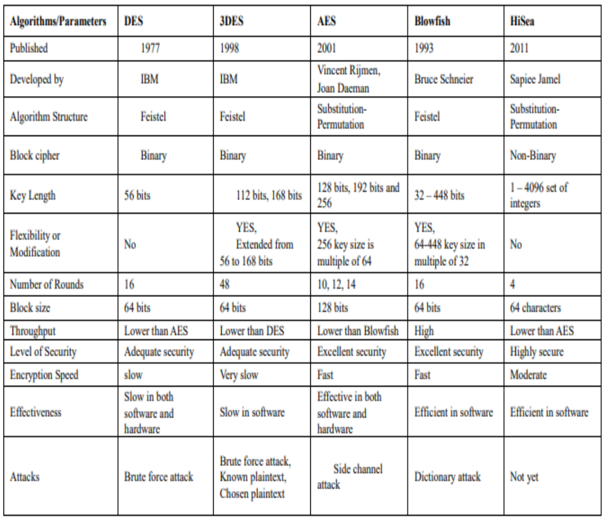
5. AES

The Advanced Encryption Standard (AES) is the algorithm trusted as the standard by the U.S. Government and numerous organizations.

Although it is extremely efficient in 128-bit form, AES also uses keys of 192 and 256 bits for heavy duty encryption purposes.

AES is largely considered impervious to all attacks, with the exception of brute force, which attempts to decipher messages using all possible combinations in the 128, 192, or 256-bit cipher. Still, security experts believe that AES will eventually be hailed the de facto standard for encrypting data in the private sector.

B. Comparative Analysis Of symmetric Encryption Algorithm



Algorithms/Parameters	DES	3DES	AES	Blowfish	HiSea
Published	1977	1998	2001	1993	2011
Developed by	IBM	IBM	Vincent Rijmen, Joan Daeman	Bruce Schneier	Sapiee Jamel
Algorithm Structure	Feistel	Feistel	Substitution-Permutation	Feistel	Substitution-Permutation
Block cipher	Binary	Binary	Binary	Binary	Non-Binary
Key Length	56 bits	112 bits, 168 bits	128 bits, 192 bits and 256	32 – 448 bits	1 – 4096 set of integers
Flexibility or Modification	No	YES, Extended from 56 to 168 bits	YES, 256 key size is multiple of 64	YES, 64-448 key size in multiple of 32	No
Number of Rounds	16	48	10, 12, 14	16	4
Block size	64 bits	64 bits	128 bits	64 bits	64 characters
Throughput	Lower than AES	Lower than DES	Lower than Blowfish	High	Lower than AES
Level of Security	Adequate security	Adequate security	Excellent security	Excellent security	Highly secure
Encryption Speed	slow	Very slow	Fast	Fast	Moderate
Effectiveness	Slow in both software and hardware	Slow in software	Effective in both software and hardware	Efficient in software	Efficient in software
Attacks	Brute force attack	Brute force attack, Known plaintext, Chosen plaintext	Side channel attack	Dictionary attack	Not yet

Case Study

Symmetric (also known as secret-key) ciphers use the same key for encrypting and decrypting, so the sender and the receiver must both know -- and use -- the same secret key. All key lengths are deemed sufficient to protect classified information up to the "Secret" level with "Top Secret" information requiring either 192- or 256-bit key lengths. There are 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys -- a round consists of several processing steps that include substitution, transposition and mixing of the input plaintext and transform it into the final output of cipher text.

During the encryption process of a message, if the message is not divisible by the block length, then the Padding is used. Padding is the method of adding additional Dummy data. E.g. if the message consists of 426 bytes, then we need 7 additional bytes of padding to make the message 432 bytes long, because 432 is divisible by 16. Three key sizes can be used in AES and depending on key sizes the number of rounds in AES changes. Standard key size in AES is 128 bits and no of rounds are 10. for AES encryption two sub keys are generated and in 1st round a round key is added.

For 128 bits plain text and 128 bits key is used and 10 rounds are performed on plain text to find the cipher text. In first step, 10 round keys are generated for each round there is separate round key. But in first round an extra round key which is initial round is added to the round and then transformation is started. Transformation consists of four steps. 1. Substitute Bytes 2. Shift Rows 3. Mix Columns 4. Add Round Key The Following figure explain all the stages of Encryption from plain text to Cipher text.

III.CONCLUSION

Each of cryptographic algorithms has strong points and weak points. We select the cryptographic algorithm based on the demands of the application that will be used. From the surveys 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. We can consider that blowfish and AES algorithms are used to prevent the application from guessing attacks and it can be applied on top of all the internet protocols that are based on IPv4 and IPv6 and the examinations recoded in this paper showing that all the algorithms and the classes are functioned well with different execution time and memory consumption.

IV. REFERENCES

[1]. Z. Haider, M. Saleem, and T. Jamal, "Analysis of Interference in Wireless", in Proc. of ArXiv, arXiv:1810.13164 cs.NI], Oct. 2018.

[2]. T. Jamal and P. Mendes, “Relay Selection Approaches for Wireless Cooperative Networks”, in Proc. of IEEE WiMob, Niagara Falls, Canada, Oct. 2010.

[3]. T. Jamal, P. Mendes, and A. Zúquete, “Opportunistic Relay Selection for Wireless Cooperative Network”, in Proc. of IEEE IFIP NTMS, Istanbul Turkey, May 2012.

[4]. T. Jamal and P. Mendes, “Cooperative relaying in user-centric networking under interference conditions”, in Proc. of IEEE Communications Magazine, vol. 52, no. 12, pp. 18–24, Dec 2014.

[5]. P. Mendes, W. Moreira, T. Jamal, and Huiling Zhu, “Cooperative Networking in User-Centric Wireless Networks”, In: Aldini A., Bogliolo A. (eds) User-Centric Networking. Lecture Notes in Social Networks. Springer, Cham, ISBN 978-3-319- 05217-5, May 2014.

[6]. T. Jamal, P. Mendes, and A. Zúquete, “Relayspot: A Framework for Opportunistic Cooperative Relaying”, in Proc. of IARIA ACCESS, Luxembourg, June 2011.

[7]. T. Jamal, and SA Butt, "Malicious Node Analysis in MANETS", in Proc. of International Journal of Information Technology, PP. 1-9, Springer Publisher, Apr. 2018.

[8]. T. Jamal, and P. Mendes, “COOPERATIVE RELAYING FOR DYNAMIC NETWORKS”, EU PATENT, (EP13182366.8), Aug. 2013.

[9]. T. Jamal, and P. Mendes, “802.11 Medium Access Control In MiXiM”, in Proc. of Tech Rep. SITILabs-TR-13- 02, University Lusófona, Lisbon Portugal, Mar. 2013.

[10]. T Jamal, M Alam, and MM Umair, "Detection and Prevention Against RTS Attacks in Wireless LANs", in Proc. of IEEE C-CODE, Islamabad Pakistan, Mar. 2017.

AUTHOR’S PROFILE

Ravi Pratap Singh pursuing M.tech from Computer Science in 2016 from Azad institute of Management And Technology Lucknow. Completed B.tech in Information Technology in 2013 from Accurate Institute of Management And Technology Gr .Noida Currently Working as an Android Developer in NIIT Technologies . My area of interest cryptography.

Masood Ahmad working as an Assistant Professor (Computer Science Dept) Azad institute of Management And Technology Lucknow. Completed B.tech in Information Technology in 2008 from Babu Banarasi Das National Institute of Technology & Management Lucknow .Completed M.tech in computer Science in 2014 from Azad institute of Management And Technology Luck now.

Cite this article as :

Masood Ahmad, Ravi Pratap Singh, "A Survey on Comparison of Various Encryption Algorithms for secured data Communication ", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 6 Issue 5, pp. 298-302, September-October 2019.
Journal URL : http://ijsrset.com/IJSRSET196517