Comparative Analysis of standard Cryptographic Algorithms for better implementation of cryptographic Technique

Bhumika Kantilal Charnanand [1] and Dr. Ashish Chaturvedi

[1] Research Scholar, Department of Computer Science Sabarmati University,
[2] Associate Professor, Department of Computer Science Sabarmati University.

Abstract. In our daily life there is considerable expansion in replace of millions of data over the internet as well as other media platforms. This data may contain a number of private and reasonable information that needs to be secured from any other outsider i.e. 3rd party access or intruders. Encryption algorithms plays main task for securing these type of data. All encryption algorithms differ in their performance. In this paper we will evaluate and compare different encryption algorithms like: RSA, AES, Triple DES, Blowfish and Twofish.

Keywords. Cryptography, network security, algorithm, data security, RSA, Triple DES, AES, Blowfish and Twofish, comparison, encryption.

1. Introduction:

In modern era, we are enclosed by several electronic devices and most of communication links created with other devices, data exchange can be possible between two or more than two devices. This inter linking of devices acts as a channel between them and this linking further merges more devices and creates a network. This network connection can be through WAN, LAN, MAN, WLAN or any other medium. Network needs the security for transmitting the data and keeping it secured until it reaches from source to the final destination. Flow of data can be done using several security protocols and policies among which most of them is used in OSI (Open System Interconnection) model. Sometimes it may happen that hackers or any intruders may hack the network or breach the channel passing the data. So to secure the data transmission and making it difficult for hacker or intruder to breach the channel we need cryptographic algorithms that can provide more layer of security over data transmission medium. Process of cryptography is used for covering the content of message from all other users except dispatcher and recipient. Most of the common cryptographic algorithms are categorize into i.) Symmetric (private) and ii.) Asymmetric (public) key encryption. At this point Symmetric uses same key for both Encryption and Decryption of messages whereas, Asymmetric involve different keys for Encryption and Decryption. In Symmetric Cryptography algorithms like: Triple-DES, AES, Blowfish, Twofish are included. In Asymmetric Cryptography algorithms like: RSA, Digital signature and Message Digest Algorithms are involved. This paper evaluates and compares amongst Triple-Des, AES, Blowfish, Twofish and RSA based on the several parameters.

1.1 Triple DES

DES is acronym as Data Encryption Standard. Triple DES has been developed to replace the original Data Encryption Standard (DES) algorithm. The recommended norm and the most frequently used symmetrical algorithm in the industry was triple DES. Three independent keys with 56 bits each are used by Triple DES. The overall key length is up to 168 bits, but experts will argue that it is more like 112 bits of key power. For financial services and other fields, Triple DES also manages to render a secure hardware encryption solution. Triple DES, is a symmetric-key block cipher, which is used to apply the DES cipher algorithm three times to each data block.

Advantages

- Triple DES is simple to incorporate in both hardware and software applications.
- Triple DES is everywhere: the majority systems, libraries, and protocols support for it

1.2 RSA

RSA (Rivest–Shamir–Adleman) is a public-key cryptosystem commonly used for secure data transmission. RSA is the standard for the encryption of data transmitted over the Internet. RSA is known as an asymmetric algorithm because of the use of a pair of keys. It applies the prime number to produce the public and private key depend on the scientific fact and taking the product of huge numbers collectively. The result of RSA encryption is a large batch of mumbo jumbo that takes an attacker somewhat a bit of time and computing power to hack down. An RSA user produces and publishes a public key along with an auxiliary value dependent on two large prime numbers. In RSA sender knows about the encryption key and receiver knows about decryption key.

Advantages

- Very fast and simple encryption
- Easier to implement
- Easier to understand
- Widely deployed
- Better industry support

Disadvantages

- RSA is a slow relative to symmetrical cryptography.
- It takes more resources on the machine compared to single key encryption
- The complexity of the algorithm i.e. the key is too big and the computation time is too long.
- Really slow generation of keys.

1.3 Blowfish

Another algorithm planned to replace DES is Blowfish. This symmetric cipher splits messages into 64-bit blocks and encrypts them separately. Blowfish is known both for its unbelievable speed and in general performance, as many say it has not at all been overwhelmed. Blowfish algorithm obtains simple text and key as input. Seller has completed good use of its free of charge sharing in the public domain. Blowfish can be used in tech categories vary from e-commerce payment security platforms to password revival applications, where password protection is used. This is probably one of the most versatile encryption approaches available.

Advantages:

- One of the best block excluding when the changing keys.
- Every new key requires pre-processing equal to encrypting around 4 kilobytes of text, which is very dawdling compared to the other block ciphers.
- It is not subject to licenses and is therefore freely available for use by everyone.
- It has played a great role for the success of cryptographic applications.

Disadvantages:

- It cannot have both authentication and non-repudiation as two people have the same key.
- It also has a restriction in the decryption process as compare to other algorithms in terms of time consumption and serial throughput.

1.4 Twofish

The Twofish cipher has not been copyrighted and the reference execution has been put in the public domain. Twofish is a symmetric key block cipher with a block size of 128 bits and a key size of up to 256 bits. Twofish is considered as one of the fastest of its type, and perfect for use in both hardware and software environments. Twofish is freely presented for any person who wants to make use of it.

Advantages

- Extensively cryptanalyzed
- Unpatented
- Uncopyrighted
- Free

1.5 AES

The Advanced Encryption Standard (AES) is a U.S. standard trustworthy algorithm. It is particularly creative in 128-bit form. AES also uses 192 and 256-bit keys for high sense of duty encryption purposes. It is found at least six times faster than triple DES.

Advantages:

- It is more secure
- It supports larger key sizes
- It is quicker in both hardware and software.
- It is 128-bit block size makes it less open to attacks
- It is necessary by the latest U.S. and international standards.

2. Review of Literature:

Fabien Teytau and Cyril Fonlupt(2014) have implemented metaheuristics with cryptanalysis of the simplified data encryption standard algorithm and concluded that as compare to genetic algorithm accomplish worse result than a random search on the cryptanalysis of the simplified data encryption standardalgorithm [1].

NirmaljeetKaur, SukhmanSodhi(2016) have concluded that DES technique maintain secure transmission of data while sustaining the authenticity and truthfulness of the message. This encrypts the message before the data broadcast process starts. Encryption and decryption of data is done using the standard data encryption algorithm [2].

IndumathiSaikumar (2017) has concluded from his research that Data Encryption Standard has increased the level of security due to 16 rounds of operation. It's hard for the unauthorized party to attack and crack [3].

Ali E. Taki et al.(2014) have done comparative analysis of different encryption techniques and resolved that the time taken to use RSA mathematical relations makes the steps quicker than DES and Blowfish algorithms and with more safe data than symmetrical systems[4].

Ali Saleh AL Najjar (2017) have designed a proposed system that gives special types of image Encryption Image Security, Cryptography using an RSA Encrypted Image Algorithm by HEX to extract HEX Code and use an RSA public key algorithm to produce cipher image text. This technique gives extraordinary security and will be appropriate for the safe transmission of images over the Internet [5].

S.Anandakumar (2015) has used RSA algorithm to encrypt image files to enhance data transmission security in the communication area. They have selected image file to perform encryption and decryption using the key generation technique for transferring data from one destination to another [6].

Gurjeevan Singh et al. (2012) have concluded that Blowfish has better presentation in terms of Encryption Time, Decryption Time and Throughput as compare to other techniques and also concluded that DES has the slightest presentation in expressions of throughput of decryption process [7].

VeenaParihar andMr.AishwaryKulshrestha (2016) have stated that Blowfish takes much less time to process than any other encryption technique. All types of image with different sizes as well as with different format can be encrypted. Lower correlation and higher entropy can also be achieved by using this algorithm [8].

Ms NehaKhatriet al. (2014) have also proposed a system by using Blowfish and concluded that Blowfish is used repeatedly due to its high security and fast processing [9].

HebaHarahsheh and Mohammad Qatawneh (2018) have concluded that simultaneous Twofish has better execution time for large date sizes than small data sizes, but with a large number of small data processors, running time will increase rather than decrease execution time, because the amount of communication between processors will be massive [10].

ChadalavadaLasyaChowdaryet al.(2020) have compared Blowfish and Twofish and from the results concluded that Twofish for Image Encryption and Decryption requires more time as compared to the Blowfish algorithm so finally conclude that the Blowfish algorithm is the best technique to use for image encryption when compared to Twofish[11].

AkoMuhamad Abdullah (2017) has stated that Advanced Encryption Standard (AES) algorithm is capable of handling different key sizes such as 128, 192 and 256 bits with 128 bit block ciphers [12].

Table 1. Comparative Analysis of Algorithms

	Triple DES	RSA	Blowfish	Twofish	AES
Year in Developed	1995	1977	1993	1998	2001
Developed By	Diffie and Hellman	Ron Rivest, Adi Shamir, and Leonard Adleman	Bruce Schneier	Bruce Schneier	Vincent Rijmen and Joan Daemen
Key Length	**168** bits	512 or 1024 or 2048 bits	32 to 448 bits	128 bits 192 bits 256 bits	128,192 or 256 bits
Cipher Type	Symmetric block cipher	asymmetric cryptography	Symmetric block cipher	asymmetric cryptography	Symmetric block cipher
Bits/byte for optimal encoding (avg)	40	44	128	128	256
Speed	Very Slow	Slowest	Very fast	Fast	Fast
Structure	Feistel	Factorization	Feistel	Feistel	Substitution – Permutation
Mathematical Operations	XOR ,Fixed S-boxes	Exponentiation and Modulo Arithemetic	Logical XOR,Addition,Modulo Arithmetic	XOR	Substitution byte, Shift row, Mix-column and Addround key
Throughput	Lower than AES	High	Very High	High	Lower than Blowfish
Level of Security	Adequate Security	Good Level of Security	Highly Secure	Secure	Excellent
Types of Attacks	Brute Force Attack, Chosen Plaintext, Known Plaintext	Factoring the public key	Dictionary Attack	Impossible Differential Attack	Side Channel Attack
Block size	64 bits	1024 bits	64 bits	128 bits	128 bits
Round	48	1	16	16	10/12/14

References:

1. Fabien Teytau and Cyril Fonlupt,"A CRITICAL REASSESSMENT OFEVOLUTIONARY ALGORITHMS ON THECRYPTANALYSIS OF THE SIMPLIFIED DATAENCRYPTION STANDARD ALGORITHM", International Journal on Cryptography and Information Security (IJCIS), Vol. 4, No. 2, June 2014
2. NirmaljeetKaur, SukhmanSodhi," Data Encryption Standard Algorithm (DES) for Secure Data Transmission", International Journal of Computer Applications (0975 – 8887) International Conference on Advances in Emerging Technology (ICAET 2016)
3. IndumathiSaikumar," DES- Data Encryption Standard", International Research Journal of Engineering and Technology (IRJET), Volume: 04 Issue: 03 | Mar -2017
4. Ali E. TakiEl_Deen, El-Sayed A. El-Badawy, Sameh N. Gobran," Digital Image Encryption Based on RSA Algorithm", *IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 9, Issue 1, Ver. IV (Jan. 2014)*
5. Ali Saleh AL Najjar,"Implementation Color-Images Cryptography Using RSA Algorithm ",International Journals of Advanced Research in Computer Science and Software Engineering ISSN: 2277-128X (Volume-7, Issue-11),2017
6. S.Anandakumar," Image Cryptography Using RSA Algorithm in Network Security", IJCSET(www.ijcset.net) , September 2015.
7. Gurjeevan Singh, Ashwani Kr. Singla, K.S. Sandha," Superiority of Blowfish Algorithm in Wireless Networks", International Journal of Computer Applications (0975 – 8887)Volume 44– No11, April 2012
8. VeenaParihar ,Mr.AishwaryKulshrestha,"BLOWFISH ALGORITHM: A DETAILED STUDY",International Journal For Technological Research In Engineering Volume 3, Issue 9, May-2016.
9. Ms NehaKhatri – Valmik, Prof. V. K Kshirsagar,"Blowfish Algorithm",IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 2, Ver. X (Mar-Apr. 2014).

10. HebaHarahsheh, Mohammad Qatawneh,"Performance Evaluation of Twofish Algorithm on IMAN1 Supercomputer",International Journal of Computer Applications (0975 – 8887) Volume 179 – No.50, June 2018.
11. ChadalavadaLasyaChowdary, PavithraNallamothu, MarthalaCharan Reddy, Burra Vijay Babu,"COMPARATIVE STUDY ON BLOWFISH AND TWOFISH ALGORITHMS FOR IMAGE ENCRYPTION AND DECRYPTION",International Research Journal of Engineering and Technology (IRJET),Volume: 07 Issue: 11 | Nov 2020
12. ***AkoMuhamad Abdullah," Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data".***
13. Archisman Ghosh," Comparison of Encryption Algorithms: AES, Blowfish and Twofish for Security of Wireless Networks", International Research Journal of Engineering and Technology(IRJET), Volume: 07 Issue: 06 | June 2020
14. Gautam, Shivani & Gaur, Shailendra & Kalsi, Hemanpreet. (2019). A Comparative Study and Analysis of Cryptographic Algorithms: RSA, DES, AES, BLOWFISH, 3-DES, and TWOFISH. 7. 996.
15. Kumar K , Dr. K. Sasikala, "Comparative Study of Cryptographic Algorithms", International Journal of Engineering Research & Technology, Volume 09, Issue 11 (November 2020)
16. Gaurav Yadav, Mrs. Aparna Majare ," A Comparative Study of Performance Analysis of Various Encryption Algorithms", International Conference On Emanations in Modern Technology and Engineering (ICEMTE-2017), Volume: 5 Issue: 3
17. Shaza D. Rihan, Ahmed Khalid, Saife Eldin F. Osman, "A Performance Comparison of Encryption Algorithms AES and DES" , International Journal of Engineering Research & Technology (IJERT), Vol. 4 Issue 12, December-2015