ISSN 2229-3531 (Print)

JUCIT Vol. 8(1), 5-9 (2017). Periodicity-2-Monthly

ISSN 2455-9997 (Online)

JOURNAL OF ULTRA COMPUTER & INFORMATION TECHNOLOGY
An International Open Free Access Peer Reviewed Research Journal of Computer Science Engineering & Information Technology
website:- www.compitjournal.org
Estd. 2010

Critical Analysis of Various Cryptographic Algorithms

[1]PARIVESH KASTURIA and [2]KAMINI MAHESWAR

[1]NITTTR Bhopal (India)
[2]UIT, Barkatullah University, Bhopal (India)
Email of Corresponding Author :- pkasturia@nitttrbpl.ac.in
http://dx.doi.org/10.22147/jucit/080102

Acceptance Date 9th Feb., 2017, Online Publication Date 26th Feb. 2017

Abstract

Now a day mostly people are doing their daily routine digitally, because current era is based on information and communication technology. But security is one of the most important and challenging issues in this technological world. As per the literature analysis there is a demand for a encryption which should be strong and efficient. Cryptography is a private secure communication in the public world. Cryptography is a technique of protecting secure information from hacking and cracking by unauthorized individuals and converting it into unintelligible form. It provides authentication, identification to user data, confidentiality and also provides security and privacy to the data stored. It is an emerging technology in the area of network security. There is a broad range of cryptographic algorithms that are used for securing networks and presently continuous researches on the new cryptographic algorithms are going on for evolving more advanced techniques for secures communication. The main objective of this paper is to study the basic terms used in cryptography, its purpose and to compare the encryption techniques used in cryptography.

Key words : Cryptography, Encryption, Decryption, Symmetric key, Asymmetric key.

Introductionto Cryptography

Cryptography is a standard way of securing the electronic documents. Cryptography is a powerful tool used to protect the information in computer systems. It is used to ensure that the information is confidentially transmitted and would not be altered. Cryptography enables the user to transmit confidential information across any insecure network so that it cannot be used by an intruder. It allows users to carry over the confidence found in the physical world to the electronic world. It enables the users to do business electronically without bothering of hackers. The high growth in the networking technology leads a common culture for interchanging of the data very drastically. Hence while communication it is very important to protect the information and thus the message is encrypted so that intruder cannot read the message. For this many encryption techniques are existing which are used to avoid the information theft. Network security is highly based on cryptography. There are various cryptography techniques under the symmetric and asymmetric cryptosystem. The perfect selection of specific encryption scheme play important role to exchange the information and to enhance security objectives. In symmetric-key cryptography, the same key is used by both parties. The sender uses this key and an encryption algorithm to encrypt data; the receiver uses the same key and the corresponding decryption algorithm to decrypt the data. In asymmetric or public-key

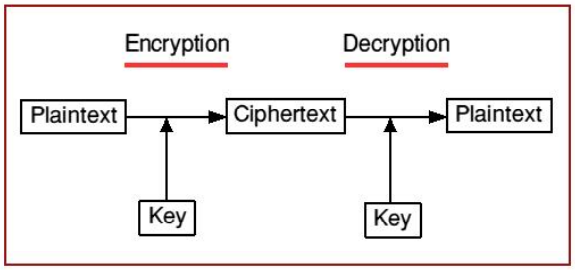
cryptography, there are two keys: a private key and a public key are used. The private key is kept by the receiver and public key is announced to the public.Applications of cryptography include ATM cards, computer passwords, and electronic commerce[3,8,9].

Terms Used In Cryptography :

1. ***Plain Text:*** The original text or message used in communication in called as Plain text. In cryptography the actual message that has to be send to the other end is given a special name as Plain Text. Example: Rita sends "Hello" to Bob. Here "Hello" is Plain text or Original message.
2. ***Cipher Text:*** In Cryptography the plain text is transformed into non readable message. The message that cannot be understood by anyone or meaningless message is called Cipher Text Example: "Hello" message is converted in "-&tt%". This meaningless message is Cipher Text.
3. ***Encryption:*** Encryption is a process of converting Plain text into Cipher text. Cryptography uses the encryption technique to send confidential messages through an insecure channel. Encryption process is done using encryption algorithm. An encryption algorithm means the technique that has been used in encryption. Encryption takes place at the sender side.
4. ***Decryption:*** Decryption process is the reverse of Encryption process. It is a process of converting Cipher Text into Plain Text. Cryptography uses the decryption technique at the receiver side to obtain the original message from non readable message (Cipher Text). Decryption process is done using decryption algorithm. A Decryption algorithm means the technique that has been used in Decryption. Generally the encryption and decryption algorithm are same.
5. ***Key:*** A Key is a numeric or alpha numeric text or may be a special symbol. In encryption process it takes place on Plain text and in decryption process it takes place on cipher text. In Cryptography the selection of key is very important since the security of encryption algorithm depends directly on it.

General Process of Encryption :

Cryptography is the process that involves encryption and decryption of text using various mechanisms or algorithms. A cryptographic algorithm is a mathematical function that can be used in the process of encryption and decryption. Encryption is the process of converting the plain text into an unreadable form called a cipher text. This unreadable form (cipher text) cannot be easily understood by an intruder and sent across the insecure media. Decryption is the process of converting this unreadable form (cipher text) back into its original form (plain text), so that it can be easily understood by the intended recipient[5,9].



General Process

Objectives of Cryptography :

Cryptography provides a number of security goals to ensure the privacy of data, non alteration of data and so on. Due to the great security advantages of cryptography it is widely used today. The various goals of cryptography are:

1. ***Confidentiality:*** Information in computer is transmitted and has to be accessed only by the authorized party and not by anyone else. It ensures that nobody can read the text except the proposed receiver.
2. ***Authentication:*** The process of providing one's identity is called authentication. The sender and receiver can confirm each other's identity and the origin/destination of the information to check whether the information is arriving from an authorized person or a false identity.
3. ***Integrity:*** It is a property that gives assurance that the message that is received has not been changed by any unauthorized individuals or in an accidental manner from the original text. Only the authorized party is allowed to modify the transmitted information. No one in between the sender and receiver are allowed to alter the given message.
4. ***Non Repudiation:*** A mechanism that proves that sender has really sent that message. Ensures that neither the sender, nor the receiver of message should be able to deny the transmission.
5. ***Key Exchange:*** The method by which crypto keys are shared between sender and receiver.

Types of Cryptography :

The two main types of cryptography are:

1. ***Symmetric key cryptography or Secret key cryptography:*** Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share the same key. In symmetric-key cryptography, the same key is used by both parties. The sender uses this key and an encryption algorithm to encrypt data; the receiver uses the same key and the corresponding decryption

algorithm to decrypt the data. Symmetric key ciphers are implemented as either block cipher or stream cipher. Some commonly used symmetric cryptography techniques are Data Encryption Standard (DES) and the Advanced Encryption Standard (AES)[2].

A significant disadvantage of symmetric ciphers is the key management necessary to use them securely.

2. ***Asymmetric key cryptography or Public key cryptography:*** Asymmetric key cryptography, where different keys are used for encryption and decryption. In asymmetric or public-key cryptography, there are two keys: a private key and a public key are used. The private key is kept by the receiver and public key is announced to the public[10].

Some commonly used asymmetric cryptography techniques are RSA (Rivest Shamir and Adleman), Diffie-Hellman.

Commonly Used Cryptography :

- ***DES (Data Encryption Standard) :***

Data encryption standard (DES) is a symmetric key algorithm which was found by IBM in the year 1977. This algorithm uses a key size of 64 bits and a block size of 64 bits. This algorithm is a block cipher and it uses feistel network to transfer messages. It takes about 16 rounds to convert messages and its network security can be broken by brute force attack. Benefit of this algorithm is that DES has been around a long time, even now no real weakness has been found, the most efficient attack is still found to be brute force attack. It is actually fast in hardware and relatively fast in software. Drawback of the algorithm is as technology is improving there is a possibility to break the encrypted code in DES and as we use private key for cryptography if it is lost we cannot get the readable data at the receiving end[7].

- ***Triple DES (3DES) :***

Triple-DES is also proposed by IBM in 1978 as a substitute to DES. Triple DES was developed from DES, uses a 64-bit key consisting of 56 effective key bits and 8 parity bits. In 3DES, DES encryption is applied three times to the plaintext. The plaintext is encrypted with key A, decrypted with key B, and encrypted again with key C. 3DES is a block encryption algorithm[7].

- ***AES (Advanced Encryption Standard) :***

AES (Advanced Encryption Standard) is developed by Vincent Rijmen, Joan Daeman in 2001. In December 2001, the National Institute of Standards (NIST) approved the AES as Federal Information Processing Standards Publication (FIPS PUB) 197, which specifies application of the Rijndael algorithm to all sensitive classified data. The Advanced Encryption Standard (AES) is a symmetric block cipher used by the U.S. government to protect classified information and is implemented in software and hardware throughout the world for sensitive data encryption. AES is actually, three block ciphers, AES-128, AES-192 and AES-256. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128 bits, 192 bits and 256 bits, respectively. In Advanced encryption standard there are 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys[7].

- ***IDEA (International Data Encryption Algorithm):***

IDEA (International Data Encryption algorithm) is a block encryption algorithm designed by Xuejia Lai and James Massey in 1996 It is based on the concept of substitution permutation structure that uses block cipher of 64 bit plain text and is controlled by 128 bit key. The algorithm used for encryption and decryption is the same. The plaintext of 64 bits is divided into four parts (each of 16 bits). These four parts became the input for first round which consists of mixing operations from different algebraic groups[4].

- ***Blowfish :***

Blowfish was developed by BruceSchneier in 1993 as an alternative to the existing encryption algorithms. It is a symmetric key block cipher which uses 64 bit block size and a variable key length from 32 bits to 448 bits. It has 16 or less rounds. It is the fastest block ciphers developed till date. No attack is known to be successful against Blowfish;however it suffers from weak key problems. Moreoverspace requirement for Blowfish is also very less; it canexecute in less than 5KB memory[13].

- ***Twofish :***

Twofish is also a symmetric block cipher having fiestel structure. It is also developed and explained by Bruce Schneier in 1998. Twofish also uses block ciphering like Blowfish. It is efficient for software that runs in smaller processor (smart cards) and embedding in hardware. It allows implementers to customize encryption speed, key setup time, and code size to balance performance. Twofish is license-free, un-patented and freely available for use. In twofish encryption it uses key sizes of 128, 192 and 256 bits. It uses the block size of 128 bits and there are 16 rounds of encryption in this encryption algorithm[1].

- ***Threefish :***

Threefish is a symmetric key block cipher designed by Bruce Schneier, Niels Ferguson, Stefan Lucks, Doug Whiting, Mihirbellare, Jesse Walker. It was first

published in year 2008. Threefish block cipher is directly related to Blowfish and Twofish. Threefish algorithm is tweakable block cipher. Tweakable block cipher take three inputs, a key, a tweak and block of message. A unique tweak value is used to encrypt every block of message. The tweak value is 128 bits for all block sizes. Threefish encryption uses three types of keys 256 bits, 512 bits or 1024 bits. In Threefish, the key size is equal to the block size. It means it uses three block sizes i.e. 256, 512 or 1024 bits. It applies encryption in 72 rounds generally, but in case of 1024 bit block size its encryption rounds are 80 [13].

- ***RC2& RC5 :***

Ronald Rivest (RSA Labs),developed these algorithms. They are block encryption algorithms with variable block and key sizes. It is difficult to break if the attacker does not know the original sizes when attempting to decrypt captured data[6].

- ***RC4 :***

RC4 is recognized as the most commonly utilized stream cipher in the world of cryptography. RC4 is a variable key-size stream cipher with byte-oriented operations. RC4 has a use in both encryption and decryption while the data stream undergoes XOR together with a series of generated keys. It takes in keys of random lengths and this is known as a producer of pseudo arbitrary numbers.The output is then XORed together with the stream of data in order to generate a newly-encrypted data[11].

- ***RC6 :***

RC6 was developed by Ron Rivest, Matt Robshawin the year 1998. It is a symmetric key block cipher which uses 128 bits block size and a variable key length from 128 bits to 256 bits. It has 20 or less rounds[11].

- ***Diffie-Hellman :***

Diffie-Hellman was found by Whitfield Diffie and Martin Hellman in the year 1976. This algorithm doesn't have specified key size because it uses key exchange management and has a block size of 64bits. It is a symmetric key cipher and uses common network to transfer messages. It takes nearly 14 round to convert a message and its security is broken by eaves dropping. Benefits of this algorithm is that security factors with respect to the fact that solving the discrete algorithm is very challenging, and that the shared key is never itself transmitted over the channel. Drawback of it is the lack of authentication[12].

- ***Rsa :***

Rivest-Shamir-Adleman(RSA) is asymmetric algorithm developed by Ron Rivest, Adi Shamir and Leonard Adleman in the year 1977. This algorithm uses a key size greater than 1024bits and its block size depend on the key size that is being used. Block size depends on key size. It is a block cipher and common networks are used to transfer messages. It takes 1 round to convert one message and its security is broken by timing attack. Benefit of this algorithm is that it uses public key to transfer messages and also provides security to digital signatures that cannot be repudiated. Drawback of the algorithm is that even though the public key is safe its speed is comparatively low[14].

Analysis Done

Algorithm	Key Size(s)	Security	Block Size	Number of Rounds	Algorithm Type	Scalable	Throughput	Security Attacks
DES	64 (56 usable)	Insecure	64 bits	16	Symmetric	Yes	Very High	Exclusive Key search, Linear cryptanalysis, Differential analysis, Brute force attack
TRIPLE DES	112/168 bits	Moderately Secure	64 bits	48	Symmetric	Yes	High	Related Key attack
AES	128, 192, 256 bits	Secure	128, 192 or 256 bits	10 for 128 12 for 192 14 for 256	Symmetric	Yes	High	Key recovery attack, Side channel attack, Chosen plain attack
IDEA	128 bits	Very Secure	64 bits	8	Symmetric	Yes	High	Meet in the middle attack
BLOWFISH	Variable key length i.e. 32-448 bits	Secure	64 bits	16	Symmetric	Yes	High	Reflection attack, No attack is found to be successful against blowfish
TWOFISH	128, 192, 256	Secure	128 bits	16	Symmetric	Yes	High	Brute force attack
THREEFISH	256, 512 or 1024 bits	Secure	256, 512 or 1024 bits	For 256, 512 key =72 For 1024 key = 80	Symmetric	Yes	High	Boomerang attack
RC2	8 to 128 bits; 64 bits by	Vulnerable	64 bits	16	Symmetric	Yes	Low	Linear attack, Differential attack
RC4	Variable key length i.e. 40-2048	Moderately Secure	40-2048 bits	256	Symmetric	Yes	High	Klein's attack, Royal Holloway attack, No more attack
RC5	0 to 2040 bits key size (128 suggested)	Vulnerable	34 , 64, 128 (64 suggested)	1 to 255 (64 suggested)	Symmetric	Yes	High	Differential attack
RC6	128, 192, 256	Vulnerable	128 bits	20	Symmetric	Yes	High	Differential attack, Brute force attack
Diffie-Hellman	Uses key exchange management	Secure	64 bits	14	Asymmetric	Yes	Low	Man in Middle attack, Eaves dropping
RSA	1024 bits and above	Secure	Depends on key size	1	Asymmetric	No	Low	Brute force attack, Timing attack

Conclusion

Encryption algorithm keeps very important contribution in communication security. This paper, analyzed various encryption algorithms on different parameters. In this work the performance of widely used encryption techniques like AES, DES and RSA algorithmsetc is analysed. All the techniques are having pros and cons and are useful for real-time encryption. Each technique is unique in its own way, which might be suitable for specific applications. The present study provides better understanding and working of these algorithms. It is observed that each algorithm has its own benefits according to different parameters and the strength of the each encryption algorithm depends upon the key management, type of cryptography, number of keys, number of bits used in a key. In future, comparative or performance analysiscan be made by taking different parameters to outline thestrengths and weaknesses of various algorithms. Throughthe understanding of shortcomings of these algorithms,some new encryption algorithms can be proposed bymaking amendments in the existing algorithms.Encryption algorithms are more secure and fast to work with and in future, there is wide scope of improvement.

References

1. Pushpendra Verma, Dr. Jayant Shekhar, Preety and Amit Asthana, "Survey Paper: A Survey for Performance Analysis Various Cryptography Techniques Digital Contents", published in International Journal of Computer Science and Mobile Computing, IJCSMC, Vol. 4, Issue. 1, January, pg. 522 – 531 (2015).
2. M. Kumar and E. G. Dharma, "A comparative analysis of symmetric key encryption algorithm", IJARCET, vol. *3*, no. 2, (2014).
3. K.B. PriyaIyer, R. Anusha and R. ShakthiPriya, "Survey Paper: Comparative Study on Various Cryptographic Techniques", published in International Conference on Communication, Computing and Information Technology (ICCCMIT-2014).
4. A. Kakkar and M. L Singh, "Comparison of Various Encryption Algorithms and Techniques for Secured Data Communication in Multinode Network", Published in International Journal of engg, and technology (IJET), vol. *2*, no. 1, (2012).
5. M. Abutaha, M. Farajallah, R. Tahboub and M. Odeh, "Survey Paper: Cryptography Is the Science of Information Security", published in International Journal of Computer Science and Security (IJCSS), Vol. *5*, no. 3, (2011).
6. R. L. Rivest, "The RC5 Encryption Algorithm", MIT laboratory for C.S, Cambridge.
7. J. V. Shanta, "Evaluating the performance of Symmetric Key Algorithms: AES (Advanced Encryption Standard) and DES (Data Encryption Standard) in IJCEM International Journal of Computational Engineering & Management", vol. *15*, no. 4, pp.43-49 (2012).
8. AtulKahate, "Cryptography and Network Security", Tata McGraw-Hill publishing company, New Delhi, (2008).
9. G. C. Kessler, "An Overview of Cryptography", http://www.garykessler.net/library/crypto.html, (2006).
10. Ritu Tripathi, Sanjay Agrawal, "Comparative Study of Symmetric and Asymmetric Cryptography Techniques", International Journal of Advance Foundation and Research in Computer (IJAFRC), volume 1, issue 6, June, ISSN 2348 – 4853 (2014).
11. E. Thambiraja, G. Ramesh and Dr. R. Umarani," A Survey on Various Most Common Encryption Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, volume 2, Issue 7, July, ISSN: 2277 128X (2012).
12. Vekariya Meghna, "Survey Paper: Comparative Analysis of Cryptographic Algorithms and Advanced Cryptographic Algorithms, published in International Journal of Computer Engineering and Science, August- (2014).
13. J. W. Cornwell, "Blowfish Survey", Department of Computer Science, Columbus State University, Columbus.
14. Shashi Mehrotra Seth and Rajan Mishra," Comparative Analysis Of Encryption Algorithms For Data Communication", IJCST Vol. 2, Issue 2, June pp.192-192 (2011).