ijecs open access www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 3 Issue 9 September, 2014 Page No. 8092-8096

A Review of Various Encryption Techniques

Harshraj N. Shinde[1], Aniruddha S. Raut[2], Shubham R. Vidhale[3], Rohit V. Sawant[4], Vijay A. Kotkar[5]

[1]Student (UG), Department of Computer Engineering,
A.I.S.S.M.S College of Engineering, Pune, Maharashtra, India
meharshraj@gmail.com

[2]Student (UG), Department of Computer Engineering,
A.I.S.S.M.S College of Engineering, Pune, Maharashtra, India
aniruddharaut007@gmail.com

[3]Student (UG), Department of Computer Engineering,
A.I.S.S.M.S College of Engineering, Pune, Maharashtra, India
srvidhale@gmail.com

[4]Student (UG), Department of Computer Engineering,
A.I.S.S.M.S College of Engineering, Pune, Maharashtra, India
rohitsawant3030@yahoo.co.in

[5]Assistant Professor, Department of Computer Engineering,
A.I.S.S.M.S College of Engineering, Pune, Maharashtra, India
vijaykotkar26@gmail.com

Abstract*: In today's world secure transmission of important or personal data is of big concern. The encryption of the data plays important factor of security while sending the information of data. Encryption of data means converting plain text to cipher text. There are many encryption techniques available, but the big question that arises is which one is good one or which one is suitable as per requirements. In this paper we do analysis of various encryption techniques viz. AES, BLOWFISH, DES, 3DES, RC4, RC6, RSA, UMARAM and UR5.*

Keywords: Encryption, Decryption, UR5, AES, Blowfish.

1. Introduction

Internet has changed our lives drastically. Now internet is the core of our life, be it banking, shopping, socializing etc. everything is through internet now-a-days. As there were burglars, thieves or dacoits earlier to loot us, now we have hackers who track down our movements online find out our personal information and then attack us virtually. Therefore, the need of secure transferring of information or data is essential. Over the decade many techniques have been developed to encrypt the data which is to be sent over unsecure channel. New algorithms come by now and then, which are better than their predecessors in certain ways. As we all know every coin has two side's likewise strong encryption techniques might also have a down side such as computational time taken or any other. In this paper we study some popularly used techniques and try to find out their strength and weaknesses.

The paper is organized as follows. Section I gives an introduction and basic terminologies which might be required. Section II gives a brief about all the algorithms which are surveyed. Section III is the discussion part where pros and cons are discussed about the surveyed algorithms and then we conclude.

1.1 Basic Terminologies:

A. Cryptography

It is the practice and study of encryption techniques for securing the data.

B. Plain text

A text which makes sense in its own context or text which is created by user to be sent over network to receiver is known as plain text. For example, "Hello Sam, How are you?" is a plain text.

C. Cipher Text

The text which has no association with the plain text whatsoever or may look meaningless to others is called Cipher text. Cipher text is non-readable message which is to be sent to receiver from an unsecured channel. For example, "How are you, Mr. Sanjay?" is encrypted in such a way that if seen will look something like this, "hnchj56gvju^$#&GF".

D. Encryption

The process of converting the plain text to cipher text is known as Encryption. Encryption requires a key and an algorithm to implement. The process of encryption is done at sender side.

E. Decryption

The process of converting the received cipher text to plain text is known as decryption. Decryption is reverse process of encryption hence it is important to know how the encryption was done to decrypt the text.

F. Key

A Key is a numeric or alpha numeric text or may be a special symbol. The key is used at the time of encryption of text to cipher text and at the time of decryption of text to plain text. Hence, key plays an important role in encryption and decryption that's why it is important to carefully select the key as conversion directly depends on it. For example, if a person uses a key of 3i.e.:- the letter is shifted by 3 places in alphabetically forward order then encryption of the plain Text "INDIA" will produce Cipher Text "KPFKC".

G. Symmetric Key

In symmetric key algorithm only one key is used to convert plain text. Same key is used by sender and receiver for encrypting and decrypting respectively. If weak key is used then it gets easy to crack the cipher code.

H. Asymmetric Key

In asymmetric key algorithm two keys are used to convert the plain text to cipher text i.e. public key and private key. Public key is known to everyone publicly and private key is with receiver which is not shared with public. Public key is used to encrypt the data and private is used to decrypt the data. There is some mathematical relation between the public and private key.

2. ENCRYPTION TECHNIQUES

A. Advanced Encryption Standard (AES):

The AES encryption algorithm is a block cipher that uses an encryption key and a several rounds of encryption. A block cipher is an encryption algorithm that works on a single block of data at a time. In the case of standard AES encryption the block is 128 bits, or 16 bytes, in length. The term "rounds" refers to the way in which the encryption algorithm mixes the data re-encrypting it ten to fourteen times depending on the length of the key. There are several operations in AES algorithm which repeat with each round. The operations are as follows: ADD ROUND KEY, BYTE SUB, SHIFT ROW, and MIX COLUMN is enhances the security of algorithm [1]. Though High End hardware is required and hard implement because of complexity. Requires more processing power than DES, 3DES, BLOWFISH. Brute force attack is the only effective attack known against this algorithm [2]. AES is better for live video streaming transmission compared to RC4 and XOR. AES can be implemented more comfortably in high and low level language as compared to DES [3].

B. Data Encryption Standard (DES):

The DES is a block cipher algorithm which uses 56-bit (with 8-bit additional parity bits) key to encipher the plain text. The key looks like 64-bits, but 1 bit in each octet is used for odd parity so actual key is of 56-bits only [2]. DES uses series of substitutions and permutation on each block of plain text which is of 64-bit in size, which is then EX-OR with input. Above process is repeated 16 times with different sub-keys, Sub-keys are the keys formed by taking different order of the key bits each time. Because of 16 rounds the DES algorithm becomes more secure [4]. Decryption is done in a reverse way as that of encryption by using the same key used at the sender's end, since it is symmetric algorithm. Completely specified and easy to understand. Very high throughput rates can be achieved i.e. up to 100Mbits/sec can be implemented on economical hardware. DES is said to be had known key problems. In DES, the key consist of 56 bits which gives space of 2^{56}=7.2058 X 10^{16} elements. In an exhaustive search known plain-text attack, the attacker will obtain the solution after 2^{55} trials on an average. Key used in DES itself can sometimes make work easy for attacker. In situation like when all sub-keys are same then at the end of 16-rounds we will get plain text only instead of cipher text [5]. There are many attacks which can exploit the weaknesses of DES, which makes this algorithm insecure [2].

C. Triple Data Encryption Standard (3DES):

Triple DES is developed to overcome the drawbacks of conventional DES algorithm, drawbacks like Key space size, Weak key etc. Triple DES uses same algorithm of DES but change here is that here it is used three times. In 3DES, algorithm uses two or three keys depending on the size of key which we required, that is two keys gives us key size of 112 bits and three key gives us size of 168 bits [4].

3DES with two keys:

When we use two keys in DES, suppose k1, k2 then we have to take one of the key two times in encryption process. First we will encipher plain text using key k1 then we will decrypt the previously cipher text using key k2 and finally we will encipher the prior result with key k1 [4]. Algorithm is same as that of DES. Here we use two keys each of 56-bit hence we get total key size of 112 bits. This algorithm can be used as normal DES by giving k1=k2.Then the process will be like first encrypt the plain text with key k1 then decrypt the cipher text using k2 which is actually k1, hence now we'll get plain text again and now we will encrypt the plain text using key k1 [6].

3DES with three keys:

In this algorithm we use three keys which gives us key size of 168 bits which will increase the secure level of algorithm. It is different from two key-3DES, because here we do not use the first key at last again instead we use third key (k3) for last encryption. It is more secure than conventional DES because it has keys of size 112,168 bits corresponding to number of keys used in algorithm. Exhaustive search cannot crack the key because key space of 3DES is 2^{112}. As 3DES uses 3 keys hence straight forwardly we can say it takes 3 times the computational time than that of DES [6].

D. Blowfish:

Bruce Schneider designed Blowfish in 1993 as a fast alternative to existing encryption algorithms. Blowfish is a symmetric encryption algorithm, means that it uses the same secret key (private key) to both Encrypt and decrypt

messages or data. Blowfish is also called as block cipher, means that it divides a message up into fixed length blocks during encryption and decryption. The block length for Blowfish is 64 bits. Messages which are not multiple of eight bytes in size must be padded. It takes a variable-length key from 32 bits to 448 bits. Blowfish consists of two parts: Data encryption and key-expansion [7]. Blowfish came into existence in order to allow anyone to use encryption free of patents and copyrights. No attack is known to be successful against it. Blowfish has remained in the public domain to this day [8]. Blowfish has 16 rounds. Blowfish Algorithm is a Feistel Network, a simple encryption function is iterated 16 times. All operations are XORs and additions on 32-bit words. The only additional operations are four indexed array data lookups per round [9]. Due to the speed of the algorithm is more the throughput is also more. The power consumption is also less. Added functionality of key expansion makes it hard to crack. It suffers from weak keys problem. BLOWFISH is better than AES, DES, 3DES in terms of throughput and processing time [8]. BLOWFISH encrypts audio files at less speed. It also encrypts image most efficiently on windows xp, vista and 7 in comparison with AES [10].

E. Rivest, Shamir and Adleman (RSA):

RSA algorithm is Public Key cryptography also called as asymmetric key cryptography. Two keys are generated in RSA, one key is used for encryption and other key is used to decrypt message. No other key can decrypt the message. Even if it is efficient algorithm it is vulnerable to attackers. RSA algorithm consist of three phases. In phase one key generation is carried out which is to be used as key to encrypt and decrypt data. In second phase encryption of data, where actual process of conversion of plaintext to cipher text is being carried out and in third phase decryption is done, where encrypted text is converted in to plain text at other side [11].

RSA algorithm is relatively simple and easy to understand and implement. Key agreement and key exchange problem that is generated in secret key cryptography is solved by RSA. As a public key is used for encryption and is known by everyone with the help of public key the hacker can use brute force method to find private key which is used to decrypt message. As RSA is based on arithmetic modulo large numbers, it can be slow. Especially, when RSA decrypts the cipher text and generates the signatures, more computation time and capacity is required [11]. RSA is affected by Avalanche effect. Encryption time taken by RSA is much higher than that of AES and DES. Also memory usage of RSA is high compared to AES and DES. Output byte is less in RSA as compared to AES and DES [10].

F. Rivest Cipher 4 (RC4):

RC4 is a stream cipher, symmetric key algorithm. The same algorithm is used for both encryption and decryption as the data stream is simply XORed with the generated key sequence. The key stream is completely independent of the plaintext used. It uses a variable length key from 1 to 256 bit to initialize a 256-bit state table. The state table is used for subsequent generation of pseudo-random bits and then to generate a pseudo-random stream which is XORed with the plaintext to give the cipher text. Used for secured communications as in the encryption of traffic to and from secure web sites using the SSL protocol [12].

G. Rivest Cipher 6 (RC6):

RC6 proper has a block size of 128 bits and supports key sizes of 128, 192 and 256 bits. RC6 is very similar to RC5 in structure, using data-dependent rotations, and modular addition and XOR operations; in fact, RC6 could be viewed as interweaving two parallel RC5 encryption processes. However, RC6 does use an extra multiplication operation not present in RC5 in order to make the rotation dependent on every bit in a word, and not just the least significant few bits [3].

H. UMARAM:

The UMARAM was designed by Ramesh G and R. Umarani in the year 2010. This algorithm uses a key size of 512-bits to encrypt a plaintext of 512-bits during the 16-rounds. In this Algorithm, a series of transformations have been used depending on S-BOX, different shift processes, XOR-Gate, and AND-Gate. The S-Box is used to map the input code to another code at the output. It is a matrix of 16 X 16 X 16. The S-Box consists of 16-slides, and each slide having 2-D of 16 x16. The numbers from 0 to 255 are arranged in random positions in each slide. Avoids fixed key exchange between sender and receiver [13].

I. UR5:

This algorithm was designed by G. Ramesh and Dr. R. Umarani. It is a block encryption algorithm. In this Algorithm, a series of transformations will be used viz: - S-BOX, XOR Gate, and AND Gate. The UR5 algorithm encrypts a plaintext of size 64-bits by a key size of 64-bits. It uses eight rounds for encryption or decryption process [14]. It is more efficient and useable for the Wireless Local Area Network because it avoids the using of the same key with other packets within a message i.e.:- same key is not used to encrypt other blocks within the packet and key is not directly exchanged between sender and receiver, hence hackers can be avoided plus the algorithm is simple to implement [15].

3. DISCUSSION

Thambiraja et al showed that AES consumes highest processing power among DES, 3DES, BLOWFISH. AES is better than RC4 for smaller packets also it is better for live video streaming transmission compared to RC4 and XOR. Time taken by RSA is much higher than that of AES and DES. Memory usage of RSA is high compared to AES, DES. Output byte in RSA is less as compared to AES and

DES.RC4 is fast and energy efficient than AES for larger packets. Time for encryption and decryption almost remains constant for RC4 if key size is increased and less time is required to encrypt as compared to AES, DES, and 3DES [10].

Thakur et al showed that AES can be implemented more comfortably in high and low level language as compared to DES. Blowfish has better performance when packet size is changing as compared to AES, DES, 3DES, RC2, and RC6 [2].

Ramesh et al showed that UMARAM runs slower than DES and 3DES for Text data.UR5 is more efficient compared to UMARAM, RC6, DES, 3DES and also encrypts image most efficiently [15].

4. CONCLUSION

Every technique is unique in its own way. Each could be used as per the requirements of the applications. But in general or overall we could say that UR5 algorithm is better technique as key is not exchanged between the users and key update's itself. So even if some gets there hand on encrypted data which is being transmitted by unsecure channel, that person will have no idea about the key, sequence of data etc. Hence, it is quite difficult to crack the technique and as of now no leak or crack is available publicly.

References

[1] Mr. Shelke R.B., Mrs. Patil A.P. and Dr. (Mrs) Patil S.B., "VLSI Based Implementation of Single Round AES Algorithm", IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) ISSN: 2278-2834, ISBN: 2278-8735, PP: 63-67.

[2] Jawahar Thakur and Nagesh Kumar, "DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis", International Journal of Emerging Technology and Advanced Engineering, Volume 1, Issue 2, December 2011, ISSN 2250-2459.

[3] Milind Mathur and Ayush Kesarwani, "COMPARISON BETWEEN DES, 3DES, RC2, RC6, BLOWFISH AND AES", Proceedings of National Conference on New Horizons in IT - NCNHIT 2013.

[4] Sombir Singh, Sunil K. Maakar and Dr. Sudesh Kumar, "Enhancing the Security of DES Algorithm Using Transposition Cryptography Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, PP: 464-465, June 2013, Volume 3, Issue 6.

[5] PoojaRathore, Jaikarn Singh, Mukesh Tiwari and Sanjay Rathore. "Optimized DES Algorithm Using X-nor Operand Upto 4 Round on Spartan3", International Journal of Computational Engineering Research (ijceronline.com), ISSN 2250-3005(online), PP: 193-198, December 2012, Volume 2, Issue 8.

[6] Mandeep Singh and Narula Simarpreet Singh, "Implementation of Triple Data Encryption Standard using Verilog", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN:2277 128X, PP:667-670, January 2014, Volume 4, Issue 1.

[7] Ms. Neha Khatri Valmik and Prof. V. K Kshirsagar, "Blowfish Algorithm", IOSR Journal of Computer Engineering (IOSR-JCE), Volume 16, Issue 2, Ver. X (Mar-Apr. 2014), PP: 80-83, www.iosrjournals.org, e-ISSN:2278-0661, ISSN:2278-8727.

[8] Pratap Chnadra Mandal, "Superiority of Blowfish Algorithm", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 9, September 2012 ISSN:2277 128X.

[9] Tanjyot Aurora and Parul Arora, "Blowfish Algorithm", International Journal of Computer Science and Communication Engineering IJCSCE Special issue on "Recent Advances in Engineering & Technology" NCRAET-2013 ISSN: 2319-7080.

[10] 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 2012 ISSN: 2277 128X.

[11] Rajan. S. Jamgekar and Geeta Shantanu Joshi, "File Encryption and Decryption Using Secure RSA", International Journal of Emerging Science and Engineering (IJESE), Volume-1, Issue-4, February 2013 ISSN: 2319–6378.

[12] Allam Mousa and Ahmad Hamad, "Evaluation of the RC4 Algorithm for Data Encryption", Nablus, Palestine.

[13] G. Ramesh and Prof. Dr. R. Umarani, "UMARAM: A NOVEL FAST ENCRYPTION ALGORITHM FOR DATA SECURITY IN LOCAL AREA NETWORK", ICCCCT'10.

[14] G. Ramesh and R. Umarani, "A Comparative Study of Six Most Common Symmetric Encryption Algorithms across Different Platforms", International Journal of Computer Applications (0975 – 8887) Volume 46– No.13, May 2012.

[15] G. Ramesh and Prof. Dr. R. Umarani, " UR5:A Novel Symmetrical Encryption Algorithm With Fast Flexible and High Security Based On Key Updation", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 4, April 2012 ISSN: 2277 128X.

Author Profile

Harshraj N. Shinde pursuing Bachelor's degree from Savitribai Phule Pune University in A.I.S.S.M.S College of Engineering, Pune, Maharashtra, India.

Aniruddha S. Raut pursuing Bachelor's degree from Savitribai Phule Pune University in A.I.S.S.M.S College of Engineering, Pune, Maharashtra, India.

Shubham R. Vidhale pursuing Bachelor's degree from Savitribai Phule Pune University in A.I.S.S.M.S College of Engineering, Pune, Maharashtra, India.

Rohit V. Sawant pursuing Bachelor's degree from Savitribai Phule Pune University in A.I.S.S.M.S College of Engineering, Pune, Maharashtra, India.

Vijay A. Kotkar, Assistant Professor, completed Master's Degree in 2013 from North Maharashtra University Jalgaon, Maharashtra India. 10 papers have been published and presented in various National and International Conferences as of now, working in the area of Image Processing and Pattern Recognition.