ISSN: 2321-7782 (Online)
Volume 2, Issue 3, March 2014
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Paper / Case Study
Available online at: www.ijarcsms.com

A Survey on Cryptography Algorithms

Maulik P. Chaudhari[1]
Student of Master in Computer Science & Engineering
Gujarat Technological University
Ahmedabad – India

Sanjay R. Patel[2]
Student of Master in Computer Science & Engineering
Gujarat Technological University
Ahmedabad – India

Abstract: ***Information Security has been very important issue in data communication. Any loss or threat to information can prove to be great loss to the organization. Encryption technique plays a main role in information security systems. Information security area there are many cryptography algorithm is available and comparison has been made on the basis of these parameters: rounds block size, key size, and encryption / decryption time, CPU process time in the form of throughput and power consumption. These results show that blowfish is better than other algorithm. Blowfish is more secure and fast processing algorithm. But there is some problem in the existing Blowfish algorithm blowfish weak keys produces "bad" S-boxes, since Blowfish's S-boxes are key dependent. There is a chosen plaintext attack against a reduced-round variant of blowfish that is made easier by the use of weak key.***

Keywords: : Cryptography, AES, DES, 3DES, BLOWFISH, Fuzzy Value.

I. INTRODUCTION

1.1 Cryptography

Cryptography is the science that studies the mathematical techniques for keeping message secure and free from attacks [1]

Cryptography system can be classified into two parts first is Symmetric – key Cryptography and second is public – key cryptography.

1.1.1 Symmetric – key cryptography:

In symmetric key cryptography system sender and receiver share a single key which is used to encrypt and decrypt a message. It is also called secret key cryptography. The algorithms used for symmetric – key cryptography is called symmetric- key algorithms. There are two types of symmetric algorithms such as stream cipher and block cipher. Stream ciphers encrypt the bits of information one at a time and Block ciphers encrypt the information by breaking down into blocks. [1]

List of Symmetric Algorithms

1. Data Encryption Standard(DES)
2. Advanced Encryption Standard (AES)
3. Blowfish Encryption Algorithm
4. International Data Encryption Algorithm
5. Triple Data Encryption Standard etc.

1.1.2 Public- key cryptography:

In public key cryptography there is pair of keys one is secret key and other is public key. In which one is used for encrypting the plain text, and the other is used for decrypting the cipher text [1].

List of public – key algorithms

1. Diffie-Hellman
2. RSA
3. DSA etc.

The Goal of Cryptography is about concealing the content of the message. At the same time encrypted data package is itself evidence of the existence of valuable information. [3]

II. EXISTING SYSTEM

2.1 Cryptography

2.1.1 Symmetric Algorithms

AES is a symmetric-key block cipher published by National Institute of Standards and Technology (NIST) in December 2001.AES is a non-Feistel cipher that encrypts and decrypts a data block of 128 bits. It uses 10, 12, or 14 rounds. The key size which can be 128,192, or 256 bits, depends on the number of rounds. If both block length and key length are 128 bits, AES will perform 9 processing rounds. If the block and key are 192 bits, AES will perform 11 processing rounds. If the block and key are 256 bits, then it performs 13 processing rounds. Each processing rounds involves four steps:

1. Substitute bytes: Uses an S-box to perform a byte by byte substitution of the block.
2. Shift rows: A simple permutation.
3. Mix column: A substitution method where data in each column from the shift row is multiplied by the algorithm's matrix.
4. Add round key: The key for the processing round is XORed with the data [10][2].

DES was the first encryption standards to be published by NIST [6] (National Institute of Standards and Technology).It was designed by IBM based on their Lucifer Cipher. Initially,56 bits of the key are selected from the initial 64 by permuted choice(1).the remaining eight bits are either discarded or used as parity check bits. The 56 bits are then divided into two 28-bit halves; each half is thereafter treated separately. In successive rounds, both halves are rotated left by one or two bits and then 48 sub key bits are selected by permuted choice(2),24 bits from the left half and 24 from the right. The key schedule for decryption is similar; the sub keys are in reverse order compared to encryption [10][2][6].

In cryptography, TRIPLE DES [8] is the common name for Triple Data Encryption Algorithm block cipher, which applies the Data Encryption Standard cipher algorithm three times to each data block. The triple DES (3DES) algorithm was needed as a replacement for DES due to advances in key searching [6]. TDES uses three rounds message. This provides TDES as a strongest encryption algorithm since it is extremely hard to break 2^168 possible combinations. Another option is to use two different keys for the encryption algorithm. This reduces the memory requirement of keys in TDES. The disadvantage of this algorithm is that it is too time consuming [8]. The original DES cipher's key size of 56 bits was generally sufficient when that algorithm was designed, but the availability of increasing computational power made brute-force attacks feasible. Triple DES provides a relatively simple method of increasing the key size of DES to protect against such attacks. It takes three 64-bit keys, for an overall key length of 192 bits. In Triple DES the data is encrypted with the first key, decrypted with the second key, and finally encrypted with the third key. Triple DES runs three times slower than DES, but it much more secure. The procedure for decrypting is the same as the procedure for encryption, except it is executed in reverse. [10][2]

Blowfish is a symmetric block cipher that can be effectively used for encryption and safeguarding of data. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for securing data. Blowfish was designed in 1993 by Bruce

Schneider as a fast, free alternative to existing encryption algorithms. Blowfish algorithm is a Feistel Network, iterating a simple encryption function 16 times. The block size is 64 bits, and key can be any length up to 448 bits. It is significantly faster than most encryption algorithms when implemented on 32- bit microprocessors with large data caches. The algorithm consists of two parts: a key expansion part and a data-encryption part. Key expansion converts a key of at most 448 bits into several sub keys arrays totaling 4168 bytes. Blowfish is now considered to be insecure for many applications. So it becomes very important to augment this algorithm by adding new levels of security to make it applicable and can be depending on in any common Communication channel [9][5][7].

2.1.2 Asymmetric algorithm

RSA is most widely used public-key cryptosystem. It provides data confidentiality, key exchange and digital signature. The strength of RSA is factoring large numbers [10].. It is a block cipher. In RSA, the plaintext and cipher text are integers between 0 and n-1 for some n. The description of the RSA algorithm is as follows [4]. Plaintext is encrypted in blocks , with each block having a binary value less than some number n. [10]

Public key components:

n = product of two large primes, p and q

e = a random number relatively prime and less than (p-1)(q-1)

Primary key components:

D = e-1 mod ((p-1)(q-1)) , the multiplicative inverse of mod((p-1)(q-1))

Encryption:

C = Me mod n

Decryption:

M = Cd mod n

Digital Signature:

S = Mdmod n

M = Se mod n = Med mod n (to verify the signature)

The following requirements must be met for RSA to be satisfactory.

1. p and q , two large primes must remain secretive.
2. It is possible to find value of n, e, d such that, Med mod n for all M<n.
3. It is infeasible to determine d, given e and n.
4. It is easy to calculate Meand C for all values of M<n.

Other Asymmetric Key Algorithm

Other asymmetric key algorithms are used in conjunction with RSA. These other algorithms have their limitations. These algorithms are Diffie–Hellman [10]. Digital Signature Algorithm [2], ElGamal[10].and Elliptic Curve Cryptography[8]. The disadvantage of Diffie-Hellman (DH) algorithm is that it is not as versatile as RSA and key generation might be too computationally expensive for the mobile device. Digital Signature Algorithm (DSA) is not as versatile as RSA. Another problem is that the key varies from 512 to 1024 bits, so requiring a strong key size beyond 1024 bits is not possible. DSA is slower than RSA in terms of signature verification [10]. In ElGamal, the cipher text generated is twice the size as the plaintext;

therefore it is not suitable in an environment with high latency and low bandwidth. ECC provides equal security for a smaller key size, thereby reducing processing overhead [10]. So, ECC is more beneficial than RSA.

III. RESULTS

Table 1.Comparative execution time among DES, AES and BLOWF1SH [4]

INPUT SIZE(IN KB)	DES Execution in Time (In Sec)	AES Execution in Time (In Sec)	BLOWFISH Execution in Time (In Sec)
20,527	16.2	40.5	10.07
36,002	28.4	71.07	17.67
45,911	36.2	90.63	22.53
59,852	47.2	118.17	29.37
69,545	54.8	137.3	34.1
1,37,325	108.2	271.1	67.33
1,58,959	125.2	313.8	77.93
1,66,364	131	328.4	81.57
1,91,383	150	377.8	93.8

TABLE2. Comparative memory usage and Throughout among DES. AES and BLOWF1SH [4]

Algorithm	Memory Usage(In KB)	Throughout (In Byte/Sec)
DES	43.3	1268.765
AES	32.5	558.2886
Blowfish	25.2	2270.288

IV. CONCLUSION

In this Paper we conclude that the Blowfish algorithm is faster than other algorithm. It reduces the execution time and provides a better security and it consumes less memory usage compared to any other algorithm. To improve the performance parameter of the Blowfish Algorithm like change in key size to prevent from brust force attack, change the size of plain text and Possible to minimize the key size of blowfish and making round more complexes for improving performance.

Acknowledgement

With the cooperation of my guide, we are highly indebted to Asst. Prof. Neha Parmar, for her valuable guidance and supervision regarding our topic as well as for providing necessary information regarding review paper. We are very much thanks to Asst. Prof. Dinesh Vaghela for helping us in text preparation.

References

1. Komal Patel, Sumit Utareja, Hitesh Gupta, "Information Hiding using Least Significant Bit Steganography and Blowfish Algorithm", International Journal of Computer Applications (0975 – 8887) Volume 63– No.13, February 2013.
2. O P Verma, Ritu Agarwal, DhirajDafouti, ShobhaTyagi,"Peformance Analysis Of Data Encryption Algorithms",IEEE 2011
3. Mr .VikasTyagi, Mr.Atulkumar, Roshan Patel, Sachin Tyagi, Saurabh Singh Gangwar,"IMAGE STEGANOGRAPHY USING LEAST SIGNIFICANT BIT WITH CRYPTOGRAPHY"
4. A.Ramesh, Dr.A.Suruliandi "Performance Analysis of Encryption Algorithms for Information Security", International Conference on Circuits, Power and Computing Technologies 2013 IEEE
5. Irfan.Landge, Burhanuddin Contractor, Aamna Patel and Rozina Choudhary "Image encryption and decryption using blowfish algorithm", World Journal of Science and Technology 2012, 2(3):151-156 ISSN: 2231 – 2587
6. Gurjeevan Singh, Ashwani Kumar, K.S Sandha "A Study of New Trends in Blowfish Algorithm", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 Volume 1, Issues 2.
7. Asaf M.Ali Al-Neaimi, Rehab F. Hassan, "New Approach for Modifying Blowfish Algorithm by Using Multiple Keys", International Journal of Computer Science and Network Security (IJCSNS), VOL.11 No.3, March 2011
8. Monika Agrawal, Pradeep Mishra, "A Modified Approach for Symmetric Key Cryptography Based on Blowfish Algorithm", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-6, August 2012
9. PratapChnadraMandal,"Superiority of Blowfish Algorithm",International Journal of Advanced Research in Computer Science and Software Engineering(IJARCSSE)ISSN: 2277 128X,Volume 2, Issue 9, September 2012
10. W.Stallings, "Cryptography and Network Security 4th Ed," Prentice Hall, 2005.

AUTHOR(S) PROFILE

Maulik P. Chaudhari received the B.E. degree in Computer Engineering from Ahmedabad Institute Of Technology, Ahmedabad under Gujarat Technological University in 2012, Gujarat and pursuing Master of Engineering degrees in Computer Science & Engineering from Parul Institute Of Technology under Gujarat Technological University, Ahmedabad.

Sanjay R. Patel received the B.E. degree in Computer Engineering from Saffrony Institute Of Technology, Mehsana under North Gujarat University in 2010, Gujarat and pursuing Master of Engineering degrees in Computer Science & Engineering from Parul Institute Of Technology under Gujarat Technological University, Ahmedabad.