PERFORMANCE ANALYSIS OF SINGLE KEY BLOCK CIPHERS

DR. MINIRANI S, ANAGHA SHASTRI

Abstract: In the world which has gone wireless today, the need for security of information becomes extremely important. In this paper a study and analysis of existing symmetric key cryptographic techniques is done. Also a performance analysis of the selected symmetric key encryption techniques is carried out.

Keywords: cryptography, decryption, encryption, AES, Blowfish, DES, TDES.

Introduction to cryptography: Cryptography is the science of devising methods that allow the information to be sent in a secure form in such a way that the only person able to retrieve this information is the intended recipient. Encryption is based on algorithms that scramble information into non-discernable form. Decryption is the process of restoring the scrambled information to its original form. A collection of algorithms and associated procedures for hiding and revealing information constitutes a cryptosystem. Cryptanalysis is the process of analysing a cryptosystem, either to verify its integrity or to break it for ulterior motives. The process of attacking a cryptosystem is called cracking or hacking.

The job of a cryptanalyst is to find the weaknesses in the cryptosystem. Some cryptosystems are rated in terms of years and the price of the computing equipment it would take to break them. In the last few decades cryptographic algorithms, by being mathematical in nature, have become sufficiently advanced so that they can only be handled by computers. Cryptography although essential for military and diplomatic communications has many commercial uses and applications: from protecting company's confidential information to protecting a telephone call, to allowing someone to order a product on the internet without the fear of their transaction details to be intercepted and used against them. Cryptography is all about increasing the level of privacy of individuals and groups.

Cryptography provides certain security advantages to ensure the privacy and non alteration of data. Various goals of cryptography includes confidentiality, authentication, integrity, non repudiation and access control to the information exchanged over networks. Confidentiality provides the privacy for messages and stored data by hiding information using encryption techniques. Authentication provides two service. First, it identifies the origin of the message. Second, it verifies the identity of a user logging into a system and continues to verify their identity in case someone tries to break into the system. Message integrity provides assurance to all parties that the message remains unchanged from the time it was created to the time it was opened by the recipient. Non-repudiation can provide a way of proving that the message came from someone even if they are trying to deny it.

Overview of encryption techniques: The various cryptographic techniques used for encryption and decryption are AES, DES, IDEA, Blowfish and RSA. These techniques differ in the key size, block size and execution time. It must be assumed that any eavesdropper has access to all communications between the sender and the recipient. A method of encryption is only secure if even with this complete access, the eavesdropper is still unable to recover the original message being sent which is the plaintext from the encrypted message which is the ciphertext. A key is a value that causes a cryptographic algorithm to run in a specific manner and produce a specific ciphertext as an output. The key size is usually measured in bits. The bigger the key size the more secure will be the algorithm.

The technique which uses just one key for encryption and decryption is called symmetric cryptography or secret key cryptography. The problem with this technique is that the key has to be kept confidential. Also the key must be changed from time to time to ensure secrecy of transmission. This means that the secret key has to be communicated to the recipient. To get around the problem of communicating the key, the concept of public key cryptography was developed by Diffie and Hellman. This technique is called asymmetric encryption in which there are two keys, one held privately and the other one made public; what one key can lock, the other key can unlock.

The actual mathematical function used to encrypt and encrypt messages is called a cryptographic algorithm or cipher. Algorithms that use a key system allow all details of the algorithm to be widely available. This is because all of the security lies in the key. With a key based algorithm the plaintext is encrypted and decrypted by the algorithm which uses a certain key, and the resulting ciphertext is dependent on the key and not the algorithm.

Symmetric Cryptography: Symmetric algorithms have one key that is used both to encrypt and decrypt the message and hence also called single key algorithms. These algorithm are fast and efficient, especially if large volumes of data need to be processed. Symmetric cryptography provides a means

of satisfying the requirement of message content security, because content cannot be read without the secret key. There remains a risk of exposure, because neither party can be sure that te other party has not exposed the secret key to a third party whether accidently or intentionally. It also addresses the integrity and authentication requirements. The technique doses not adequately address the non-repudiation requirement, as both parties have the same secret key. There are two type of symmetric algorithms, block ciphers and stream ciphers. Block ciphers usually operate on groups of bits called blocks. Each block is processed a multiple number of times. In each round the key is applied in a unique manner. The more the number of iterations, the longer is the encryption process, but results in a more secure ciphertext. Stream ciphers operate on plaintext one bit at a time. Plaintext is streamed s raw bit through the encryption algorithm. While block cipher will produce the same ciphertext from the plaintext using the same key, a stream cipher will not. The ciphertext produced by a stream cipher will vary under the same conditions.

The next section discusses four symmetric encryption techniques i.e. DES, 3DES, AES, Blowfish.

Data Encryption Standard (DES): Designed in 1973, DES which was the first encryption standard recommended by National Institute of Standards and Technology as the most efficient method for encryption of data. It is a block cipher which encrypts 64 bit plaintext at a time and uses a key of 56 bits to customise the transformation so that the decryption can be performed by the party who know the key used for encryption. In DES, there are 16 stages of processing with an initial and final permutation termed as IP and FP. At first IP is performed on the 64-bit plain text which produces two halves of the permuted message, left plain text and right plain text. These two undergoes 16 rounds of encryption process and in the end are rejoined and a final permutation is performed on the combined block.

The advantages of DES are that it has proved resistant to all forms of cryptanalysis and so it has been used in many commercial and financial applications. Since its key size is too small its entire 56 bit key space can be searched in less than 22 hours and was recognised as less secure because of the advancement in the processing speed of the computers.

Triple DES (TDES): This is an enhancement of data encryption standard with a 64-bit block size and 192 bits key size. Here the encryption method is similar to DES but applied three times on each block to increase the level of encryption and average safe time. The most common method used for this is the minus Encrypt-Decrypt-Encrypt method in which each iteration of TDES will use this to encrypt a block using a 56-bit key, then decrypt the block using a different 56-bit key and at the end a 56-bit key to encrypt the data again which makes it slower than the other block cipher methods. TDES is still approved by US government systems, but largely replaced by the advanced encryption standards. The major advantage of TDES is that it is easy to implement in both hardware and software.

Encryption Techniques	DES	TDES	AES	BF
Average Time-Machine 1	134	383	228	108
Average Time-Machine 2	14	42	21	11

Advanced encryption systems (AES): Developed by two Belgian cryptographers, Joan and Vincent Rijmen, was approved by US government for the encryption of sensitive but unclassified data. This is a symmetric key algorithm in which the number of internal rounds of the cipher is a function of the key length. AES uses Rijndael block cipher which has shown resistance to the cryptographic attacks to an extent. Here the key and block length can be 128, 192 or 256 bits and uses 9, 11and 13 processing rounds respectively with an extra round of encryption performed at the end. Each processing round involves four steps - a non-linear substitution step where each byte is replaced with another, a simple permutation where each row is shifted cyclically a certain number of steps, a mixing operation which combines four bytes in each column and an add round key which combines each byte using bitwise XOR. AES encryption is fast and flexible and has been in securing information of smart cards and online transactions. One of the disadvantages is that AES in Galois Counter Mode is challenging to implement in software.

Blowfish: Developed by Bruce Schneier, blowfish is a block cipher which takes variable key length ranging from 32 bits to 448 bits which allows a trade-off between speed and security. Blowfish is fast compared to other block ciphers as its encryption rate on 32-bit microprocessors is 18 clock cycles per byte and can run in less than 5K of memory. It is one of the best conventional encryption algorithms whose security is unchallenged and which is unpatented, licence-free and is available for all users.

Comparative study of symmetric key encryption techniques: The study was carried out for the symmetric key algorithms discussed above: DES, TDES, AES and Blowfish. Their performance was analysed encrypting various input files with different contents and sizes which was conducted on two different machines. The results obtained are presented in Table1 and Fig. 1.

Table 1 : Average performance time for the algorithms

Conclusion: The results clearly show the superiority of Blowfish algorithm in term of average time of performance of algorithms. Also DES has a better performance than AES and TDES. It should also been noted that TDES needs around three times more time than DES to process the same amount of data thus making it the least efficient among the studied algorithms.

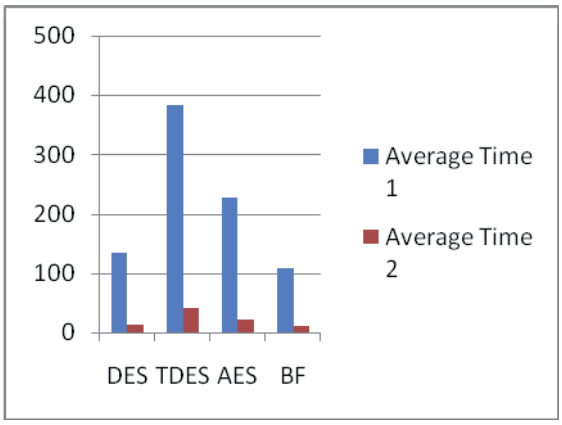

Fig. 1 : Comparison of performance of the algorithms

References:

1. Dr.A.Praveenprakash, Kanimozhiraman, A Study of Problems Faced By Old Age People Using Fuzzy; Mathematical Sciences international Research Journal ISSN 2278 – 8697 Vol 3 Issue 2 (2014), Pg 731-733
2. A William Stallings, "Network Security Essentials", Pearson Education, 2004.
3. C. Jaya Subba Reddy, K. Hemavathi, P. Gurivi Reddy, Some Results on Reverse Derivations in Prime Rings; Mathematical Sciences international Research Journal ISSN 2278 – 8697 Vol 3 Issue 2 (2014), Pg 734-735
4. Atul Kahate, "Cryptography and Network Security", Tata McGraw Hill, 2008.
5. Vaddiparthi Yogeswara, Biswajit Rath, Ch.Ramasanyasi Rao, FS-Sets And Infinite Distributive Laws; Mathematical Sciences International Research Journal : ISSN 2278-8697Volume 4 Issue 2 (2015), Pg 251-256
6. Abdel-Karim Al Tamimi, "Performance Analysis of data Encryption Algorithms", http://www.cse.wustl.edu/~jain/cse567-06/ftp/encryption_perf/
7. Harjinder Singh, Jatinder Kaur., Coefficient inequality for A Subclass of Regular P-Valent Functions; Mathematical Sciences international Research Journal ISSN 2278 – 8697 Vol 4 Issue 1 (2015), Pg 262-264
8. Vikrant M. Adiki, Shubhanand S. Hatkar, "A survey on cryptographic techniques", Int. J. of Computer Science and Software Engineering, Vol. 6, Issue 6, June 2016.
9. C. Jayasekaran, S. Robinson Chellathurai, M. Jaslin Melbha , Mean Square Sum Labeling Of Some Cycle Related Graphs; Mathematical Sciences International Research Journal : ISSN 2278-8697Volume 4 Issue 2 (2015), Pg 257-262
10. Mitali, Vijaya Kumar, Arvind Sharma, " A survey on various cryptographic techniques", Int. J. of Emerging Trends & Tech. in Computer Science, Vol. 3, Issue 4, August 2014.
11. Chander Bhan Mehta, Susheel Kumar, Stability of Two Superposed Porous Elastico-Viscous; Mathematical Sciences International Research Journal ISSN 2278 – 8697 Vol 3 Issue 1 (2014), Pg 238-240
12. Pratap Chandra Mandal, "Superiority of Blowfish Algorithm", Int. J. of Advance Research in Computer Science and Software Engineering, Vol. 2, Issue 9, Sept. 2012.

Dr. Minirani S, Anagha Shastri
Don Bosco Institute of Technology, Kurla, Mumbai.