PERFORMANCE OF VARIOUS ALGORITHMS USED IN CRYPTOGRAPHY

Chhaya Nayak*

Abstract:

Performance of cryptosystems is a very important process in measuring the performance of Cryptosystems. Communication is the basic process of exchanging information. The effectiveness of computer communication is mainly based on the security aspects. Security of information transmitted over the network is becoming tougher in spite of the availability of many cryptographic algorithms. This paper provides the various factors affecting the performance of Encryption algorithms .This paper also focuses on the factors which affects the security of the information transmitted over the networks. Since our main concern here is the performance of these algorithms under different settings, the presented comparison takes into consideration the behavior and the performance of the algorithm when different data loads are used. The security of algorithms and performance of a given algorithm depends on variety of parameters such as key size, block size, diffusion and confusion properties. This paper presents the analytical results of the cipher which were analyzed quantitatively based on the above mentioned parameters.

Key words: Cryptography, Encryption, Decryption, cipher, cryptanalysis, Key, security.

*** SIA, indore.**

1. Introduction

Many encryption algorithms are widely available and used in information security [8, 9, 10] to enhance the security of the information that has been transmitted through the internet. In spite of adopting large block size, wide key length, complex substitution and other key aspects in designing the ciphers an, ,the security of the information and network security is still a challenge. Thus it is necessary to develop the ciphers suitable for the security requirements of the particular applications. In [1][2][3][4] [5], it has been indicated that the security of algorithms and performance of a given algorithm depends on variety of parameters such as key size, block size, diffusion and confusion properties. This paper presents the analytical results of the cipher which were analyzed quantitatively based on the above mentioned parameters. This paper also suggests some factors which could be essentially considered while designing ciphers, so that the efficiency of the ciphers that are being designed can be considerably effective. Section 2 discusses description of various cryptography Algorithms. Section 3 discusses about the role of key in designing cryptographic algorithms. Section 4 gives details about the two desirable properties of cryptosystems i.e., confusion and diffusion. Section 5 gives details about performance factors that affect the performance of ciphers.

Section 6 gives conclusion drawn from the above discussions. Section 7 gives references.

2. Description of various cryptography Algorithms

Brief definitions of most common encryption techniques are given as follow:

DES: DES (Data Encryption Standard) was the first encryption standard to be recommended by NIST. DES is (64 bits key size with 64 bits block size). Since that time, many attacks and methods recorded the weaknesses of DES, which made it an insecure block cipher [1],

3DES: 3DES (Triple DES) is an enhancement of DES; it is 64 bit block size with 192 bits key size. In this standard the encryption method is similar to the one in the original DES but applied 3 times to increase the encryption level and the average safe time. It is a known fact that 3DES is slower than other block cipher methods.

Blowfish: Blowfish is block cipher 64-bit which can be used as a replacement for the DES algorithm. It takes a variable length key, ranging from 32 bits to 448 bits; default 128 bits. Blowfish: Blowfish is unpatented, license-free, and is available free for all uses. Blowfish has variants of 14 rounds or less. Blowfish is successor to Twofish [5].

IDEA: International Data Encryption Algorithm (IDEA)A block cipher with block size 64 bits and 128-bit key IDEA very effective in achieving diffusion.

RC5: Suitable for hardware and software. Adaptable to processors of different word lengths. variable number of rounds, variable-length key.

3. Role of key in designing cryptographic algorithms.

Key size is a very important parameter which affects the security of the cipher. Larger key size means greater security but reduced encryption and decryption operation speed. Many ciphers employs separate key generation algorithm which works in parallel with the associated encryption and decryption algorithm. Randomness of the keys generated can be increased by efficient techniques using rational number generation to increase confusion property [4] [5].Some ciphers also made use of genetic algorithm concepts. Throughput and processing time mainly decides the efficiency of the algorithms. [4][5][6].

4. Desirable properties of cryptosystems

Cryptographic systems are categorized by two properties mainly confusion and diffusion Confusion property makes the cryptanalysis very difficult and thus makes the algorithm stronger. Many ciphers available made use of modulus operation, Exclusive-or operations, discreet logarithms, exponentiation, prime number arithmetic ,shift operation etc to hide the statistical relationship between plaintext and cipher text [6].The confusion property is based on s-box design techniques.[2][6]. Diffusion property can be incorporated by performing the

operations for n number of rounds where n is an integer and an integral multiple of 2. The role of S-Box is a very important aspect in the designing of the ciphers.

The following table depicts S-Box design parameters of DES and Blowfish Algorithms [6].

Table 1: S – Box design parameters

Size of the S-Box	DES	BLOWFISH
	6x4 S-Boxes	8 8x32 S- Boxes

5. Design factors and Performances comparisons of Ciphers

Coding and simulation of ciphers is also play a very important role in the design and development of ciphers for security applications. VHDL can be made use to simulate any complex ciphers. FPGA implementations are the efficient means for producing the chip level implementations of the ciphers [5]

Following table shows the typical design parameter values and performance of various ciphers. [6]

Table 2: Typical design parameters

Algorithm	Clock Cycles per round	Number of rounds		Number of clock cycles per byte Encrypted
DES	18	16		45
Blowfish	9	16		18
RC5	12	16		23
IDEA	50	8		50
Triple-DES	18	48		108

6. Conclusion

This paper presents a performance evaluation of selected symmetric encryption algorithms. The selected algorithms are DES, 3DES, RC5, Blowfish and IDEA. Fixing the performance metric to evaluate the performance of cryptosystems is a very important process in measuring the performance of Cryptosystems. Security of information in transit is a very important task in secured communication. Many Ciphers are available which have been developed by using arithmetic and logical operations. The two important desirable properties of the cryptosystems are its speed and security. Speed refers to the time taken by the algorithm to convert a given plaintext to cipher text. The Key plays a very important role in encryption and decryption operations. The Security of the algorithm is based on the key size. The increase in the key size reduces the speed of the algorithm but in turn increases the security. Thus the aim of the designer is to design efficient cryptosystems with acceptable speed and appreciable security strength with large key length. Implementation procedures also play a major role in cryptosystems design.

7. References

- A Block Cipher Having a Key on One side of the Plaintext Matrix and its Inverse on the otherSide-Dr.V.U.KI.Sastry, Prof.D.S.R.Murthy, Dr.S.Durga Bhavani
- A Modified Hill cipher Involving Interweaving and iteration,V.Umakanta Sastry, N.Ravishankar and S.Durga Bhavani,Director, SCSI, Dean (R&D), Srreenidhi Institute of Science and Technology, Hyderabad, India,CSE Department, SNIST, Hyderabad, India,International Journal of Network Security
- A Performance Analysis of Encryption Algorithms' Text length size on Web Browsers-Syed Zulkarnain Syed Idrus, syed Alwee Aljunid, Salina Mohd Asi, Suhizaz sudin and Badlishah Ahmad, school of Computer and ,communication Engineering, University Malasia Perlis, Perlis, Malaysia
- Evaluating The Performance of, Symmetric Encryption Algorithms-Diaa Salama abd Elminaam, Hatem Mohamed Abdul Kader, and Mohiy Mohamed Hadhoud, higher Technological Institute 10th of Ramadan city, Egypt, Faculty of Computers and Information Minufiya University, Egypt.
- Efficient FPGA Realization of S-Box using Reduced Residue of Prime Numbers-Muhammad H.Rais and Syed M.Qasim,King Saud University, College of Engineering, department of Electrical Engineering , Riyadh, Saudi Arabia, Vol.II, No.1,pp-11-16,July 2010.
- Cryptography and Network Security, Principles and Practices-William Stallings Third Edition
- Performance Evaluation of Symmetric Cryptography Algorithms- Gurjeevan Singh, Ashwani Kumar Singla, K.S. Sandha , IJECT Vol. 2, Issue 3, Sept. 2011
- Applied Cryptography-Bruce Schneider Second Edition.
- Introduction to modern cryptography , Bruce Schnier second Edition