AN ANALYSIS OF THE DESIGN FACTORS AFFECTING THE PERFORMANCE OF CRYPTOSYSTEMS

S.G.Srikantaswamy

Research Scholar,
National Institute of Engineering, Mysore,
sg_srikantaswamy@yahoo.com

Prof. H.D.Phaneendra

Research Guide and Professor,
National Institute of Engineering, Mysore,
hdphanee@yahoo.com

Abstract

Communication is the basic process of exchanging information. The effectiveness of computer communication is mainly based on the security aspects. The internet made the communication more flexible and resourceful. Then securing the data that has been transmitted over the channel turned in to a different shape. Security of information transmitted over the network is becoming tougher in spite of the availability of many cryptographic algorithms. This paper aims at providing the zoom on 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.

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

1. Introduction

Many ciphers have been developed so far in the field of communication 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 about the role of key in designing cryptographic algorithms. Section 3 gives details about the two desirable properties of cryptosystems i.e, confusion and diffusion. Section 4 gives implementation details. Section 5 give details about performance factors that affects the performance of ciphers.
Section 6 gives conclusion drawn from the above discussions. section 7 gives references.

2. Key size parameters

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].

3. Confusion and diffusion

Confusion property makes the cryptanalysis very difficult and thus makes the algorithm more strong. 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

4. Implementation Issues 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].

5. Design factors and Performances comparisons of Ciphers

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

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 is 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

[1] 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

[2] 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

[3] 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 ,ommunication Engineering, University Malasia Perlis, Perlis, Malaysia

[4] 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.

[5] 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.

[6] Cryptography and Nertwork Security, Principles and Practices-William Stallings Third Edition

[7] Applied Cryptography-Bruce Schneier Second Edition.

[8] Introduction to Modern Cryptography,- jonathan Katz, Yehuda Lindell.