Chapter -1

Introduction

1.1 Research Objective

The main objective of this research is to study various cryptography algorithms, comparison and its analysis statistically, a model would be suggested for Cryptography for data Encryption and Decryption.

I would like to suggest a model for cryptography which provides security for any kind of data like Text, Image, Audio, Video etc. An algorithm based on model will be compared with RSA algorithm, ELGAMAL algorithm and DSA algorithm.

This model will work with character data, image data and audio data, it will be compared with various operating systems for performance measurement and then statistical analysis will show the result of comparison.

The aim of this research work is to suggest a model for all kind of encryption and decryption for more security in less amount of time.

1.2 Statement of the title

ANALYSIS AND DESIGN OF CRYPTOGRAPHIC ALGORITHMS

1.3 The research Area and problem definition

Cryptography algorithm working with two resources encryption and decryption, with this reference we can check different aspect like Time (Minute, Second) and cipher key language in different machines.

In cryptography, the security of most systems necessarily relies upon computational problems that are conjectured to be intractable, i.e., infeasible to solve with any realistic amount of computational resources. Over the past three decades, the most useful candidate hard problems have come from an area of mathematics called number theory. For instance, a commonly made conjecture is that it is infeasible to
compute the prime factors of huge random integers. However, the relatively high computational cost, and largely sequential nature, of operating on such enormous numbers inherently limits the efficiency and applicability of numbertheoretic cryptography. Even more worrisome is that quantum algorithms, which work in a model of computation that exploits quantum mechanics to dramatically speed up certain kinds of computations, can efficiently solve all the number-theoretic problems commonly used in cryptography! Therefore, the future development of a practical, large-scale quantum computer would be devastating to the security of today’s cryptographic systems. Alternative foundations are therefore sorely needed.

There are many security algorithm available, algorithm require more power to compute the result and the ones which require less computational power are easy to crack. To overcome the drawbacks of existing system, an algorithm is developed keeping in mind the high security and less computational power.

1.4 Relevance of research

I have study many algorithm related cryptography and design new algorithm that can be used for Data Encryption and decryption for all type of security applications.

In today’s world security of information is a fundamental necessity not only for military and diplomatic messages but also for private communication. Today’s era of communication has increased the importance of financial data exchange, image processing, biometrics and e-commerce transactions which in turn has made data security an important issue. Cryptography is defended as the science concerned with communications in security form. The goal of cryptography is the construction of schemes, which can maintain desired security, even after malicious attempts have been made. Cryptography consists of cryptography and cryptanalysis. The former involves the study and application of various techniques through which information may be rendered unintelligible to all breaking cryptosystems and recovering the secret information.

Recently, there has been a shift of focus in cryptography. Today’s cryptography not only provides confidentiality, authentication, data integrity and non repudiation, but has also the added task of providing security in menacing environments. Cryptology
is a strange field of science. As opposed works against a powerful, malicious adversary, often referred to as the eaves-dropper. The adversary attacking the system will try to manipulate the environment into conducive states and try to break the system by adopting strategies which the designer may have not envisioned. For the attacker it suffices to show a single successful weakness of the cryptosystem. A secured cryptosystem has to withstand all such types of attacks. This tussle between the cryptographer and the cryptanalysis has continued for ages.

1.5 Details of Remaining Chapters

The researcher has distributed the entire work into five different chapters. The chapter summary for the remaining chapter i.e. from chapter-2 to chapter-5 is as follow

Chapter 1 Introduction

This chapter contains introduction of cryptography, algorithm research problem, objective etc.

Chapter 2 Introduction of Cryptography

This chapter contains introduction of cryptography, it contains definition of cryptography algorithm, its needs and other basic detail.

Chapter 3 Analysis of Algorithms

This chapter describes the basic Private Key Algorithms. It also focuses on the different techniques for extracting, storing, comparing different features of Cryptography algorithms (DSA, RSA and ELGAMAL). The researcher has also discussed the different Algorithms processing tools to manage varies tasks of Algorithms. Comparison of various algorithms was carried out on the bit length criteria for 512 bits, 1024 bits and 2048 bits. Each of this bit length data were analyzed Character wise, Line wise & Paragraph wise. Variance analysis was performed for this data. Correlation between algorithms was
established and correlation coefficients are calculated. After obtaining results a variance table and a correlation coefficient table are constructed.

**Chapter – 4 Design, Model & of Public Key Algorithm**

The chapter is concerned with an experimental prototype of the model already proposed in the chapter-3. The researcher has developed the different components of the model. The data was taken by the algorithm for its experiential validation. Strength and complexity of the algorithm is tested by testing it for avalanche effect and performing security analysis. The final result of the PK algorithm for the input data is mentioned and special features of this algorithm are listed out.

**Chapter – 5 Summary and Future work**

All the chapters which are previously mentioned are well summarized in Chapter 5. The details of all the chapters individually are mentioned. The entire development process of the new PK algorithm which is developed with the help of DSA, RSA and ELGAMAL algorithm is summarized in this chapter. As a conclusion, the need of this algorithm, its efficiency compared to the already existing algorithm and details about the current trends and future trends in the field of data security is mentioned. the scope of expansion of the already developed PK algorithm. The future of technology is approaching with a rapid rate and therefore the adaptability of current technologies with future ones is absolutely vital. This chapter specifies what specific work can be done on this algorithm for future work.