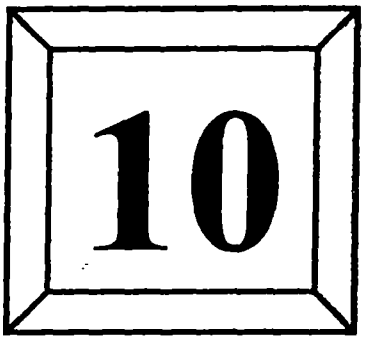

A Conclusive Discussion

Contents **Pages**

10.1	**Introduction**	**303**
10.2	**A Comparison of Different Implementations**	**303**
10.3	**A Conclusion on Proposed Implementation**	**310**

10.1 Introduction

During the entire activity of developing the proposed encryption techniques, different techniques have been implemented in different ways. With comparing these implementations, it is not possible to compare the efficiencies of the techniques. Yet from the implementation point of view, performing this task of comparison has an effective significance. Section 10.2 attempts to perform this task.

Apart from the real implementation, for each proposed technique, a model implementation is also proposed in the respective chapter and in chapter 8. One conclusion on this issue is drawn in section 10.3.

10.2 A Comparison among Different Implementations

The policies adopted for the implementation of different techniques have been pointed out in the respective chapters. In this section, the comparison is done on the basis of the encryption time, the decryption time, and the chi square value. Since while implementing different proposed techniques, the same set of sample files have been considered, for each technique, the average encryption/decryption time and the chi square value have been computed, and on the basis of these results, the comparison has been performed. This entire activity has already been summarized in table 7.5.1 in chapter 7.

Using table 7.5.1, figure 10.2.1, figure 10.2.2, and figure 10.2.3 present diagrammatic comparisons respectively for the encryption time, the decryption time, and the chi square value.

In figure 10.2.1, there exist six vertical pillars standing for six proposed techniques. On the basis of the average encryption times required during implementing the different techniques for all fifty sample files, heights of the pillars have been settled. The left-most pillar stands for the RPSP technique, for which the average encryption time is 8.75713800 seconds. Followed by this, along the left-to-right direction, the remaining pillars respectively stand for the techniques of TE, RPPO, RPMS, RSBP, and RSBM, with average encryption times being 0.86703290 seconds, 0.73186806 seconds, 0.23659592 seconds, 0.74673470 seconds, and 0.55959400 seconds.

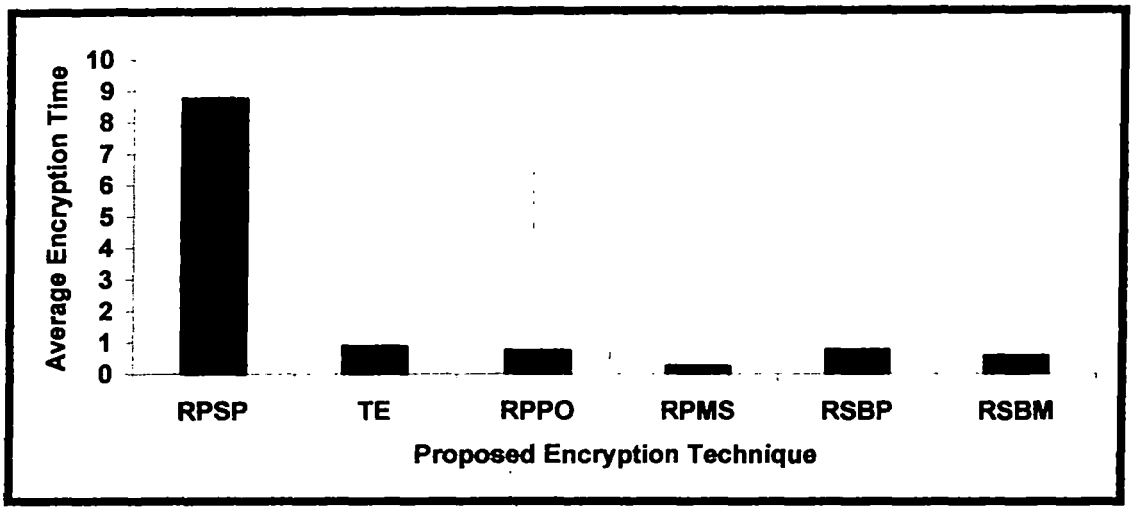

Figure 10.2.1
Comparison of Average Encryption Times for Different Proposed Techniques

In figure 10.2.2, there exist six vertical pillars standing for six proposed techniques. On the basis of the average decryption times required during implementing the different techniques for all fifty sample files, heights of the pillars have been settled. The left-most pillar stands for the RPSP technique, for which the average decryption time is 8.73955200 seconds. Followed by this, along the left-to-right direction, the remaining pillars respectively stand for the techniques of TE, RPPO, RPMS, RSBP, and RSBM, with average decryption times being 0.94175818 seconds, 7.03076904 seconds, 0.15137143 seconds, 0.11040816 seconds, and 0.09020000 seconds.

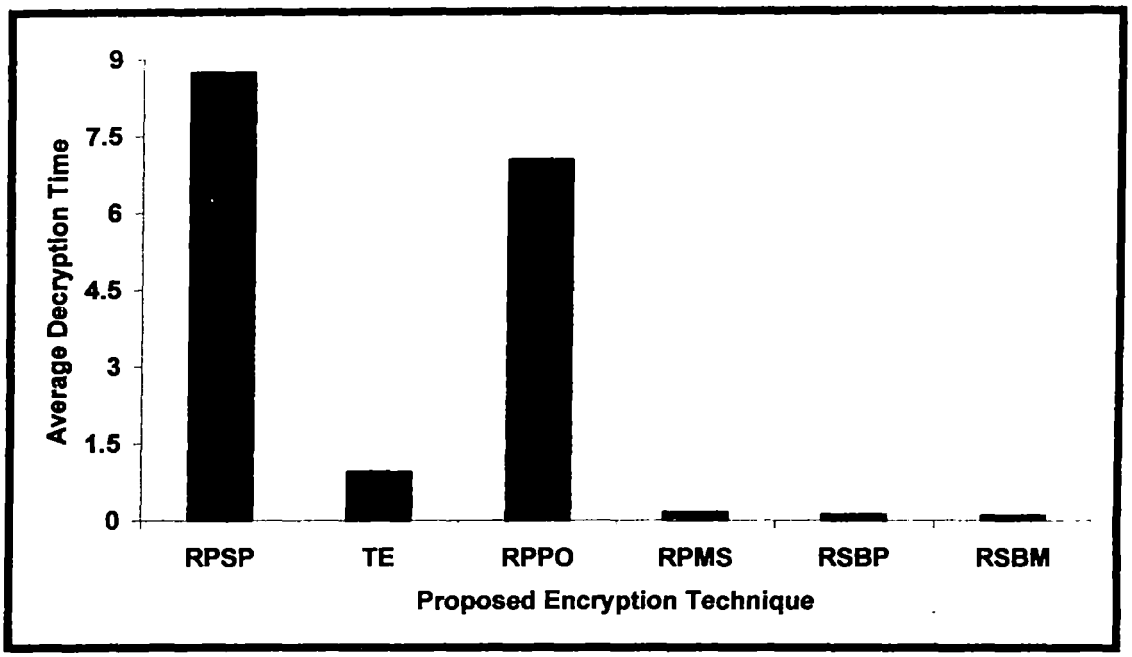

Figure 10.2.2
Comparison of Average Decryption Times for Different Proposed Techniques

In figure 10.2.3, there exist six vertical pillars standing for six proposed techniques. On the basis of the average Chi Square values obtained after implementing the different techniques for all fifty sample files, heights of the pillars have been settled. The left-most pillar stands for the RPSP technique, for which the average Chi Square value is 10701.70. Followed by this, along the left-to-right direction, the remaining pillars respectively stand for the techniques of TE, RPPO, RPMS, RSBP, and RSBM, with average values being 64188.04, 85350.94, 140196.94. 201990.76, and 40581.68.

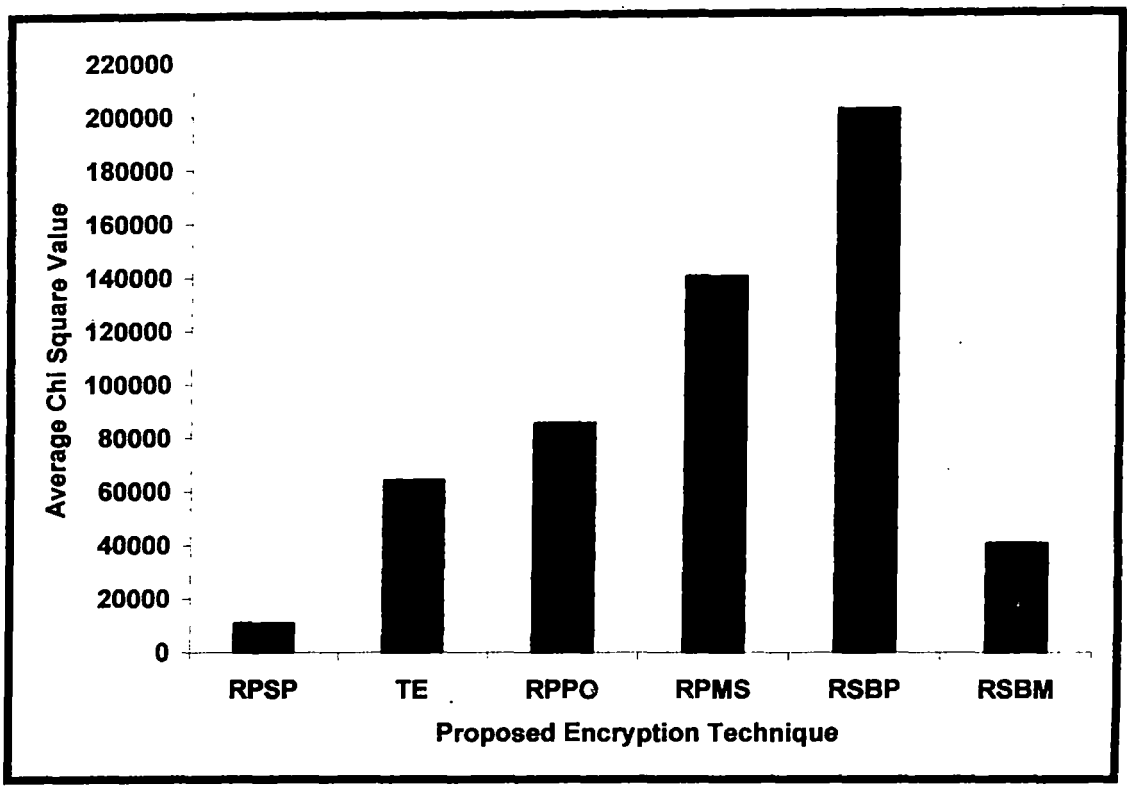

Figure 10.2.3
Comparison of Average Chi Square Values obtained for Different Proposed Techniques

To compare implementations of all proposed techniques with that of the RSA technique, the average chi square value has been computed for implementations of all .CPP sample source files, and the result is enlisted in table 10.2.1. Here the observed value for the existing RSA technique is 175993.4. The values that are most closely compatible with this value are 151357.8, which is obtained for the RPMS technique, and 133624.5, which is obtained for the RSBP technique. Values obtained for the other proposed techniques of RPSP (26511.1), TE (40427.4), RPPO (28902.4), and RSBM (31781.9) are good enough to conclude that files are heterogeneous in nature with only 1% uncertainty.

Table 10.2.1
Average Chi Square Value for Different Proposed Techniques and Existing RSA Technique implementing .CPP Files

	Proposed RPSP Technique	Proposed TE Technique	Proposed RPPO Technique	Proposed RPMS Technique	Proposed RSBP Technique	Proposed RSBM Technique	Existing RSA Technique
Average Chi Square Value	26511.1	40427.4	28902.4	151357.8	133624.5	31781.9	175993.4

The corresponding graphical relationship is shown in figure 10.2.4. Vertical pillars of color blue stand for results corresponding to different proposed techniques mentioned in the figure, whereas the black pillar is corresponding to the result for the RSA technique.

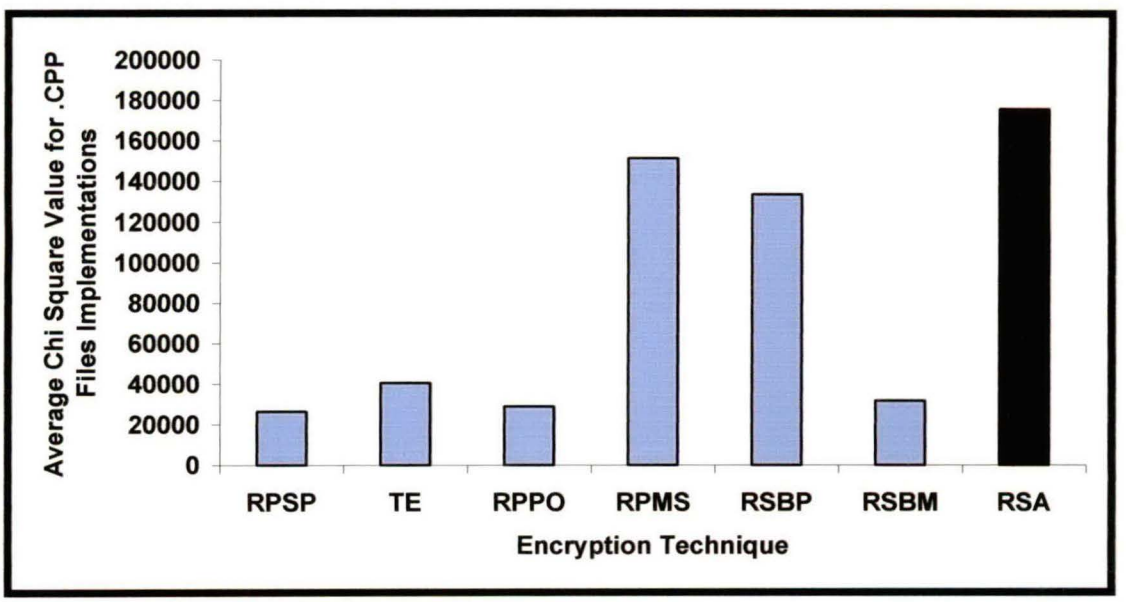

Figure 10.2.4
Graphical Relationship of Average Chi Square Value for Different Proposed Techniques and Existing RSA Technique implementing .CPP Files

Table 10.2.2 points out those instances where results in terms of the Chi Square values are observed to be better than the corresponding results using the existing RSA technique. It is observed that results for PROJECT.CPP, START.CPP, CHARTCOM.CPP, and MAINC.CPP are better at the implementation through the RPSP

and the RSBP techniques. In case of the encryption through the TE technique, the result is found better for MAINC.CPP. The same is true for the RPPO and the RSBM implementations also. By implementing the RPMS technique for PROJECT.CPP, START.CPP, and MAINC.CPP Chi Square results are observed to be better than those using RSA implementation.

Table 10.2.2
List of Files generating Better Result in Proposed Technique than Existing RSA Technique

Proposed Technique	Source File(s) with Better Results
RPSP	PROJECT.CPP START.CPP CHARTCOM.CPP MAINC.CPP
TE	MAINC.CPP
RPPO	MAINC.CPP
RPMS	PROJECT.CPP START.CPP MAINC.CPP
RSBP	PROJECT.CPP START.CPP CHARTCOM.CPP MAINC.CPP
RSBM	MAINC.CPP

As per table 10.2.2, the file for which the result of implementation in terms of the chi square value is observed better for all proposed techniques than the existing RSA technique is MAINC.CPP. Table 10.2.3 enlists chi square values obtained after encrypting MAINC.CPP using all proposed techniques and the RSA technique. The Chi Square value of 4964 is generated through the implementation of the RSA technique. whereas all the proposed techniques produce higher values. These higher values include 32724 (for the RPSP technique), 7916 (for the TE technique), 9920 (for RPPO technique), 22485 (for the RPMS technique), 24048 (for the RSBP technique), and 6245 (for RSBM technique).

Table 10.2.3
Comparison of Chi Square Values obtained encrypting MAINC.CPP using All Proposed Techniques and Existing RSA Technique

	Proposed RPSP Technique	Proposed TE Technique	Proposed RPPO Technique	Proposed RPMS Technique	Proposed RSBP Technique	Proposed RSBM Technique	Existing RSA Technique
Chi Square Value	32724	7916	9920	22485	24048	6245	4964

Graphically this comparison is shown in figure 10.2.5. Here also blue vertical pillars stand for results for MAINC.CPP after implementations through different proposed techniques mentioned in the figure, whereas the black pillar stands for the same after the implementation through the RSA technique.

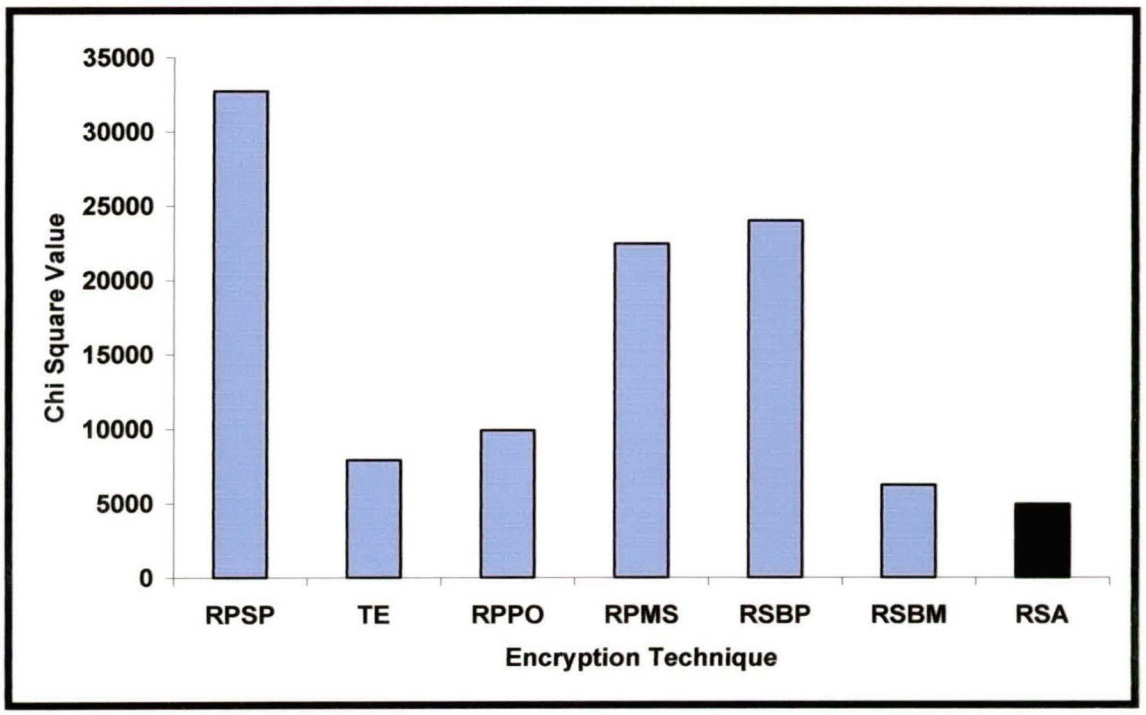

Figure 10.2.5
Graphical Comparison of Chi Square Values obtained encrypting MAINC.CPP using All Proposed Techniques and Existing RSA Technique

On the basis of the entire process of implementations and comparison, it is not a wise point to perform the final evaluation of different proposed schemes. All techniques being block ciphers, it is the issue of decomposition of the source stream of bits that also

plays a vital role in enhancing the security. Evaluation through the chi square value is only one accepted model for the purpose of evaluation. But the real strength lies in the proposed key structures, the concluding remark on which is made in section 10.3.

10.3 Conclusion on Different Model Implementations

On the basis of the entire activity of development and simple implementation of different proposed encryption policies, and comparison of these implementations with the well-accepted RSA system of encryption, the following steady conclusion can be drawn:

If each of the proposed encryption techniques is implemented independently following the protocol of the model implementation, presented in chapter 8; or if the proposed techniques are implemented in the cascaded manner following the protocol of the model implementation, presented in chapter 9, perfect, computationally secure cipher files can be generated; and on the basis of all possible kinds of factors normally used for evaluation, this can be proved to be well-compatible with the existing encryption systems.