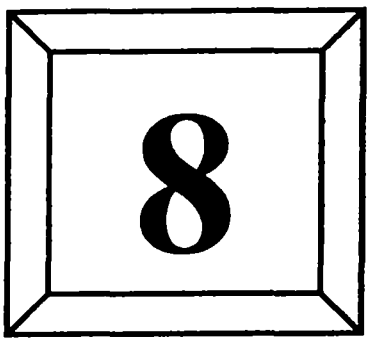

Formation of Secret Key

Contents

8.1 Introduction

Formation of the key is the most important activity in a secret key system, because even if the encryption policy is publicized, it is the secrecy of the key that helps in enhancing the security. Moreover, there should exist a tactful strategy in forming the key format, so that even applying the brute force attack the key cannot be estimated. The proper key management does not necessarily emphasize on constructing a key space as much lengthy as possible, but it deals with some factors like unambiguousness, proper invalidation, easiness in access, etc., the detailed discussion on which is made in section 9.5.4.1 [12, 23, 43].

In section 8.2, proposals are presented on key structures of different proposed techniques. Section 8.3 draws a conclusion on this issue.

8.2 Proposed Key Structures

This section provides the proposal of the key structure for each of the techniques proposed.

Schematically there exist some similarities between the RPSP and the RPPO schemes, since for both these schemes cycles are generated. Accordingly, in section 1.5.7 in chapter 1, these two techniques have been categorized as "Block Cipher with Repeated Block-to-Block Conversion". Section 8.2.1 presents a combined proposal for the format of the secret key for both the RPSP and the RPPO techniques, where instead of specifying the fixed length of the key, a superficial structure has been proposed, and depending on the exact encryption policy the length may differ.

The TE technique is one, which schematically different from all the remaining proposed techniques. In section 1.5.7 in chapter 1, this technique has been categorized as "Block Cipher with Option-based Block-to-Block Conversion". Section 8.2.2 provides the structure of the 180-bit key for the TE technique, which is to be constructed on the basis of some fixed assumptions on different issues.

The RSBP technique, categorized as "Block Cipher with Non-Contiguous Bit-Allocation" in section 1.5.7 in chapter 1, is the only one among all the proposed techniques, in which there exists the possibility of the alteration in size. Therefore in the

proposed structure of the key there should exist the size of the original file to ensure the correct decryption. This has been presented in section 8.2.3.

For the remaining two proposed techniques, the RPMS and the RSBM, section 8.2.4 provides the proposed key structure, which is common to both. Although in section 1.5.7 in chapter 1, these two techniques have been categorized respectively as "Block Cipher with Direct Block-to-Block Conversion" and "Block Cipher with Non-Contiguous Bit-Allocation".

8.2.1 Proposed Key Structure for RPSP and RPPO Techniques

Decomposing the source file into blocks of fixed size is less secured as it requires less number of iterations to form the cycle for the entire stream of bits. Another equally important reason of not choosing blocks with fixed size is the simplicity of the key. Because in such a case, the key, which may be sent to the receiver through some secret channel, will consist of only two numbers: one, the fixed block size, and the other, number of iterations used during the encryption. If variable block size is chosen, the key will be too complicated to be guessed and for each these varying sizes if the number of iterations to form the cycle is known, then only the number of such iterations to be performed during the process of encryption is to be written in the key. Figure 8.2.1.1 presents only the proposed structure of a key applicable to both the RPSP and the RPPO techniques [49, 52].

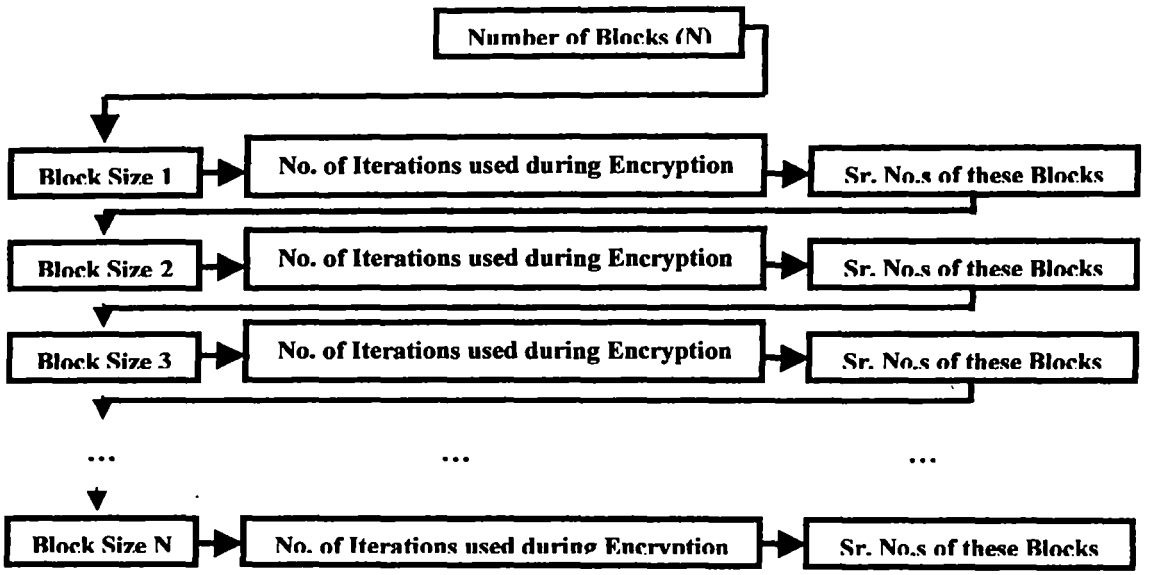

Figure 8.2.1.1
One Suggested Key Format for RPSP and RPPO Techniques

It is suggested that the key can be sent as a linear linked list, where each of the nodes stores the values stored inside a box, shown in figure 8.2.1.1. The number of nodes in the linked list depends on the number of blocks. If there exists N number of blocks, the number of nodes is (3N + 1).

8.2.2 Proposed Key Structure for TE Technique

On the basis of a fixed encryption policy, which is applicable only to very tiny files, the structure of the secret key is formed here. The policy is as follows:

- The maximum number of characters allowed in the message is 60.
- The maximum length of a block is 32 bits.
- The maximum number of blocks is 20.

Since the block length cannot exceed 32 bits, the maximum number of bits required to represent the exact length of a block is 6. Since a total of four options are available to choose the encrypted block, maximum 3 bits are required to identify a choice. Therefore a total of 9 bits are required for one block. so that, 20 being the maximum number of blocks, altogether 180 bits are required for the entire message to be

encrypted. Figure 8.2.2.1 shows the proposed format of the 180-bit secret key. With the change in the policy, the format can be changed [48, 49].

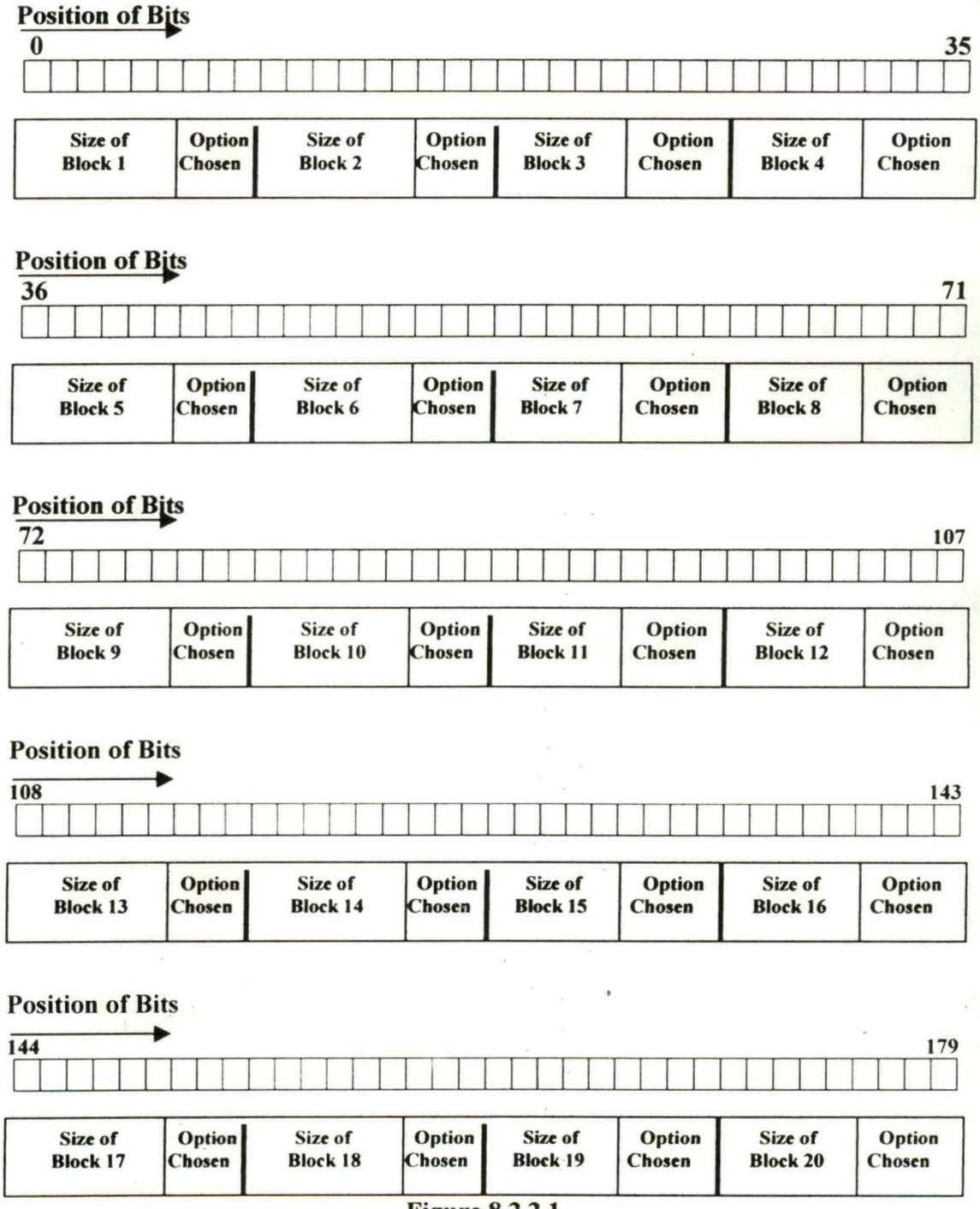

Figure 8.2.2.1
Format of 180-Bit Secret Key for TE Encryption Technique

8.2.3 Proposed Key Structure for RSBP Technique

Here the structure of the key has been proposed with an assumption on the encryption policy.

The entire stream of bits of the source file is decomposed into a total of 12 segments. Out of these, on the first 11 segments, the encryption policy is applied using the RSBP technique. The final segment is remained as it is. Each segment is assigned a unique rank value. So, rank values start with 1 for the first segment, starting from the beginning of the file, and the final segment on which the encryption policy is to be applied is with the rank value of 11. In each segment, blocks are constructed of the unique size, but the maximum number of blocks in one segment cannot exceed a limiting value [50, 54].

The relationship among the rank value of a segment (R), the unique block size in the segment (S), and the maximum number of blocks in the segment (N) is established by the following topology:

For the segment of the rank R, there can exist a maximum of $N = 2^{14-R}$ blocks, each of the unique size of $S = 2^{14-R}$ bits, R starting from 1 and moving till 11.

For different values of R, following segments are generated:

Segment with R = 1 formed with the first maximum 8192 blocks, each of size 8192 bits;
Segment with R = 2 formed with the next maximum 4096 blocks, each of size 4096 bits;
Segment with R = 3 formed with the next maximum 2048 blocks, each of size 2048 bits;
Segment with R = 4 formed with the next maximum 1024 blocks, each of size 1024 bits;
Segment with R = 5 formed with the next maximum 512 blocks, each of size 512 bits;
Segment with R = 6 formed with the next maximum 256 blocks, each of size 256 bits;
Segment with R = 7 formed with the next maximum 128 blocks, each of size 128 bits;
Segment with R = 8 formed with the next maximum 64 blocks, each of size 64 bits;
Segment with R = 9 formed with the next maximum 32 blocks, each of size 32 bits;
Segment with R = 10 formed with the next maximum 16 blocks, each of size 16 bits;
Segment with R = 11 formed with the next maximum 8 blocks, each of size 8 bits.

Since the total number of segments, the maximum number of blocks in a certain segment, and the size of blocks for a certain segment are fixed, a static structure of the key can be formed.

In the structure of the secret key, a total of 12 segments should exist, the first 11 of which are corresponding to the exact numbers of blocks in the respective segments of bits, and the final segment in the key stores the original file size. With this proposed format, the first 11 segments in the key require respectively 14, 13, 12, 11, 10, 9, 8, 7, 6, 5, and 4 bits. The final segment requires 24 bits to accommodate the source size, since, As per the calculation, with this key structure, a file of size 11.18 MB can be encrypted, and to store this size in the key, 24 bits are required. Therefore the total size of the proposed key is 123 bits.

Figure 8.2.3.1 exhibits the structure of this proposed format of key. Here each segment is shown through a pillar, and the number of bits in a segment equals to the height of the pillar. The left-most pillar stands for the first segment from the MSB position, and so on. The pillars are made of two colors. There are eleven blue pillars and one black pillar.

Each blue pillar stands for storing the number of blocks in a segment. For example, the left-most blue pillar is made of height 14, which indicates that this segment in the key is of length 14 bits, and hence it can provide information on exactly there are how many 8192-bit blocks in the segment with R=1, since it is fixed that maximum 8192 blocks can be present in this segment, and to present 8192 in modulo-2 notation, 14 bits are required.

The only black pillar is used in the final segment of the key to store the source file size. The height for this pillar is taken as 24, so that 24 bits are allocated for the source file size.

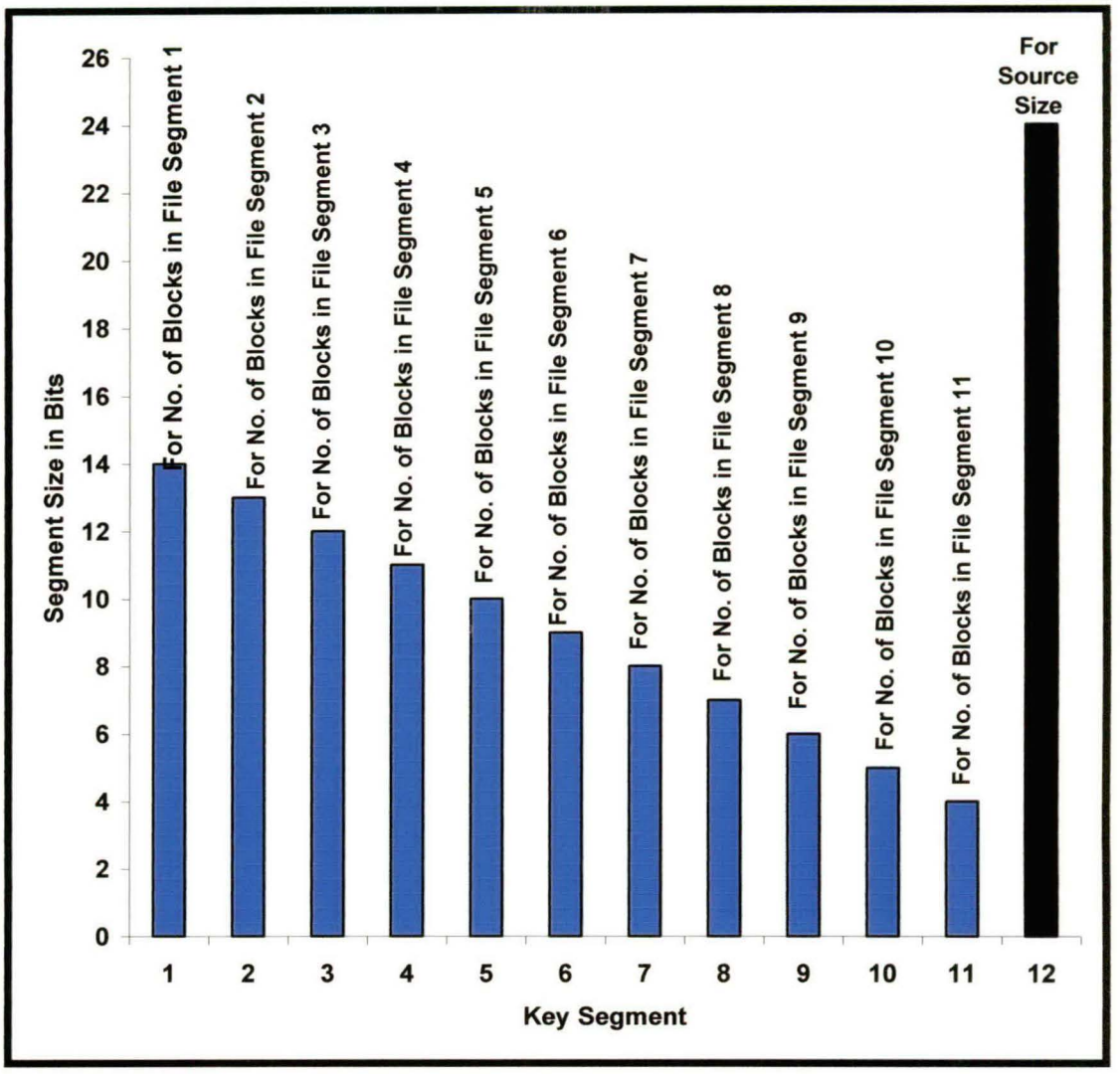

Figure 8.2.3.1
123-bit Key Format with 12 Segments for RSBP Technique

8.2.4 Proposed Key Structure for RPMS and RSBM Techniques

Here in the RPMS and the RSBM techniques, unlike the RPSP and the RPPO, there exist no formation of cycle; unlike the TE technique, there exist no option regarding the encryption; and unlike the RSBP technique, there exist no alteration in file size. In that respect, the structure of the key for the techniques of RPMS and RSBM should be consisting of the minimal information, only with sizes of different blocks to be constructed. Here this structure has been proposed only by removing the last segment from the key, shown in figure 8.2.3.1, corresponding to the RSBP encryption technique.

But in an attempt to produce a reasonably long key space, a little alteration is made in the structures of different file segments [50, 51].

For the segment of the rank R, there can exist a maximum of $N = 2^{15-R}$ blocks, each of the unique size of $S = 2^{15-R}$ bits, R starting from 1 and moving till 11.

For different values of R, following segments are generated:

Segment with R=1 formed with the first maximum 16384 blocks, each of size 16384 bits;
Segment with R=2 formed with the first maximum 8192 blocks, each of size 8192 bits;
Segment with R=3 formed with the next maximum 4096 blocks, each of size 4096 bits;
Segment with R=4 formed with the next maximum 2048 blocks, each of size 2048 bits;
Segment with R=5 formed with the next maximum 1024 blocks, each of size 1024 bits;
Segment with R=6 formed with the next maximum 512 blocks, each of size 512 bits;
Segment with R=7 formed with the next maximum 256 blocks, each of size 256 bits;
Segment with R=8 formed with the next maximum 128 blocks, each of size 128 bits;
Segment with R=9 formed with the next maximum 64 blocks, each of size 64 bits;
Segment with R=10 formed with the next maximum 32 blocks, each of size 32 bits;
Segment with R=11 formed with the next maximum 16 blocks, each of size 16 bits;

With such a structure, the key space becomes of 110 bits long and a file of the maximum size of around 44.74 MB can be encrypted using either of the RPMS and the RSBM techniques.

Figure 8.2.4.1 presents this structure. This figure to a large extend matches with figure 8.2.3.1. But here since the source file size is not needed to be stored, there does not exist any pillar for that purpose.

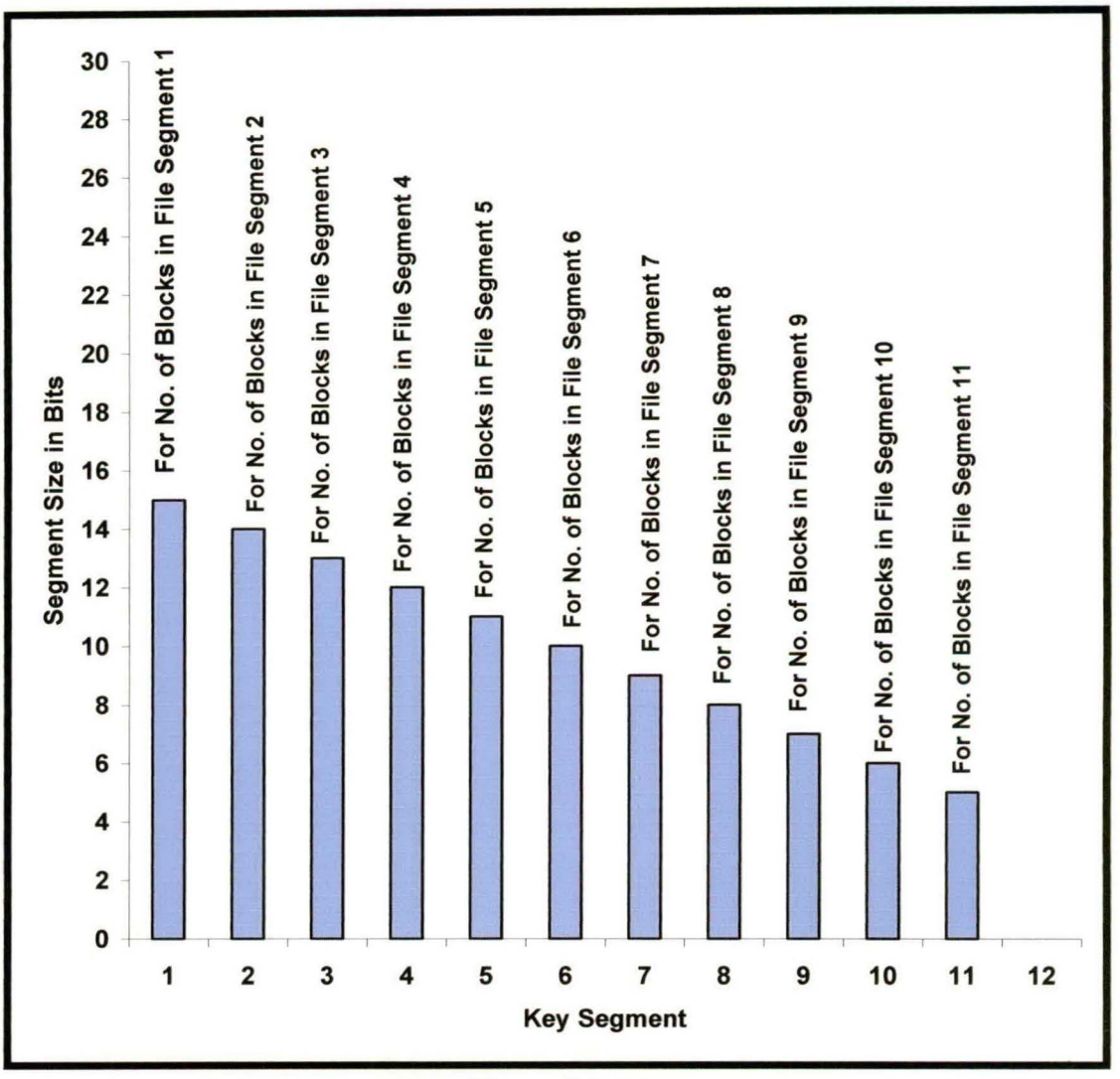

Figure 8.2.4.1
110-bit Key Format with 11 Segments for RPMS and RSBM Technique

8.3 Conclusion

Table 8.3.1 summarizes proposed key structures for different proposed techniques.

Table 8.3.1
Proposed Key Structures for Different Proposed Techniques

Proposed Techniques	Proposed Key Structure
RPSP	**No fixed length is proposed, the use of linked list is suggested**
TE	**180-bit key is proposed on the basis of a pre-fixed set of rules**
RPPO	**No fixed length is proposed, the use of linked list is suggested**
RPMS	**110-bit key is proposed that can encrypt files of upto 44.74 MB size**
RSBP	**123-bit key is proposed that can encrypt files of upto 11.18 MB size**
RSBM	**110-bit key is proposed that can encrypt files of upto 44.74 MB size**

A long key space enhances the security, but that does not necessarily mean that the key is to be constructed of excessively long size, because this, in turn, may be regarded as an overhead. Making a proper balance between these two issues, all the structures have been presented. But with the availability of more flexibility mainly in the issue of "blocks formation", much longer key spaces can be constructed for different proposed techniques [12, 23, 37, 41].