A cryptographic algorithm and a set of cryptographic keys are the basic elements of a security system. The degree of protection depends on several factors which include the strength of the cryptosystem, its implementation in hardware or software [GUE and NOR 1997] and the possible keys that are used for encryption. The general assumption is that the opponent knows the cryptosystem that is under use. This approach assures the level of security which is dependent on the secrecy of the key only. Thus an essential factor in the design of a cryptographic system is focused on the length of the key, whose size places an upper bound.

Security analysis identifies several attack models, which include Cipher text-only attack, Chosen plain text attack, Known plain text attack and Chosen cipher text attack. At the same time, the solution of any cryptogram in general involves four basic steps viz. determination of the language used, determination of the general system used, reconstruction of specific keys, reconstruction of the plain text.

The complex properties of natural languages play an important role in the formation of message text. Shannon addressed the redundancy of a language as its uncertainty. Every language is associated with certain amount of redundancy. Large amount of redundancy directs cryptanalyst towards simple mechanisms of decipherment.
Elimination of spurious keys, while determining correct one demands for the knowledge from the statistical behaviour of the message text. Unicity distance, proposed by Shannon is a measure to quantify the strength. This parameter is a resultant of message and key equivocation behaviour. The concept of perfect secrecy can be achieved by providing an independent key for every message unit, which is found to be computationally difficult task in the real world scenario. Either a single key in a short duration or multiple keys are allocated for various session dependent messages. Under this pretext unicity distance is a measure between the non linearity of message and linear characteristics of the key. The strength of the crypto system based on unicity distance is compared in this work for four different languages, English, Telugu, Kannada, Hindi.

A generic model for encipherment and decipherment with emphasis on Indian languages is proposed. The proposed model is evaluated on a corpus size of 10,00,000, 32,00,000, 17,00,000 and 9,00,000 with languages English, Telugu, Kannada and Hindi respectively.

The conditional and unconditional probability distributions of language units on unigrams, bigrams and trigrams is computed while building apriori knowledge. Test samples of varying size from 6000 to 1,10,000 are used for evaluation purpose in the decipherment approach. Retrieval efficiency is considered as a measure equivalent to
unicity distance while concluding the strength of the algorithm versus language complexity. Conditional probability distribution is observed to play an important role while improving the performance of cipher text only attack algorithms.

In addition to algorithm and Key complexities, language is proved to be a parameter of interest in determining the strength of the algorithm. Entropy of Indic scripts is found to be relatively greater than English, where as redundancy is smaller. In other words for an equal key size, an algorithm possess relatively lesser strength for English message text, than that of Indic scripts.