KEY GENERATION METHOD

Aim: The Idea was to create a dynamic key generation method which depends on the contents of input files. This method of key generation ensures that the generated key is unique every time according to the input files. In this way, the encryption key can not be traced by others.

Problem Definition: Using multiple input files uploaded by user, perform some operations individually on each file and use the intermediate results to perform some other operations on them collectively. This would result in complexly generated key, depending upon the files taken as input. Decryption of files which were encrypted using this unique key would be very complicated and difficult.

Inputs: Multiple files with textual contents.

Steps:

1. Take all the input files selected by the user
2. Process each and every file to find out frequencies of all the words present in it
3. Find the maximum occurring word of every file (intermediate result)
4. Append all the words obtained as intermediate result from all the files
5. Apply double transformation encryption on it using a secret key
6. The resultant encrypted word is the unique key generated by this method and could be used to encrypt and decrypt text later

Observations:

- Keys generated for every user are unique
- Image files create problems
- Decryption of files is very complicated, difficult and exhausting

Results: A dynamic key generation method which is secure and involves very complicated steps has been created. This method is difficult to crack and therefore, it is very useful to encrypt text files.