A straightforward technique for encrypting messages using non-min-entropy keys, such as passwords, is honey encryption (HE).As long as the password is entered correctly, an encrypted database can be obtained by an application or user, allowing them to access the data in its original, readable format while maintaining encryption.If the password key is not entered correctly, the data will remain encrypted and invisible, To obtain data, hackers who pilfer databases containing user login credentials only need to guess one correct password [2].Sweetheart In general, the process of encryption consists of two steps: distribution transforming encoding (DTE) for the input data and symmetric encryption (SE) for the .encrypted data