LIST OF TERMS

Terms	**Definition**
Pre-encryption	Encrypting a word w using $E_{k''}$ to produce X (or X_i) before further processing
Splitting	Dividing the pre-encrypted word X into two parts: L (left) and R (right)
Pseudorandom Generator (G)	Function generating a pseudorandom string S (or S_i) of length $n-m$, with a secret seed
Key Derivation via $f_{k'}$	Process of computing key k (or k_i) from the left part L (or L_i) of the pre-encrypted word
Ciphertext Block Formation	Constructing ciphertext C_i by XORing X_i with the tuple $T_i = \langle S_i, F_{k_i}(S_i) \rangle$
Search Process	Pre-encrypting a search word w, splitting it into L and R, computing $k = f_{k'}(L)$, and sending $\langle X, k \rangle$ to the server for matching
Partial Decryption (Server Side)	Server process of splitting each ciphertext block C_i and verifying the tuple to detect a valid match
Decryption (User Side)	Process where the user regenerates S_i, computes L_i and R_i, recovers X_i, and finally decrypts it to obtain w_i