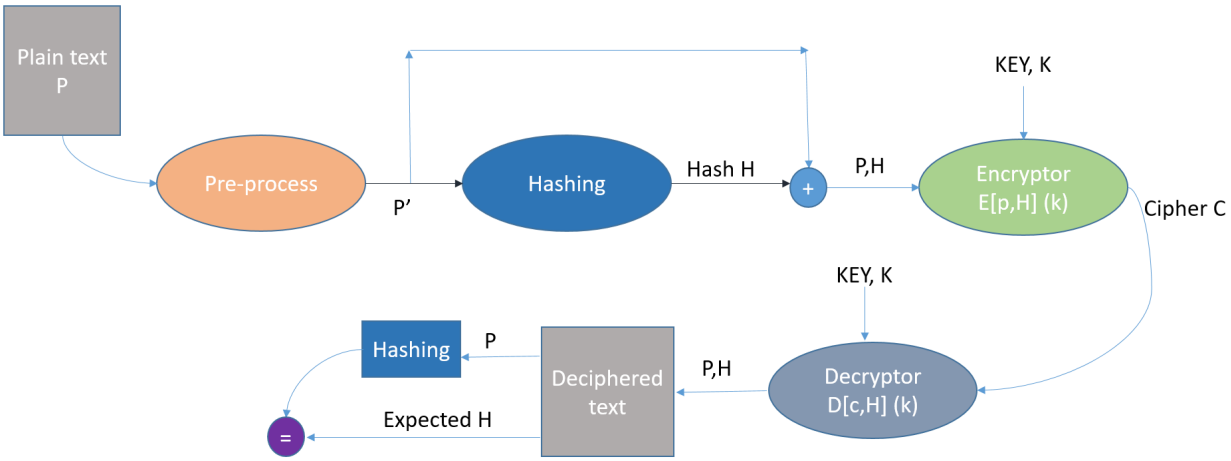
NS ASSIGNMENT 1



Description of system

Project #2: Encryption and Decryption using transposition algorithm

1. Preprocess:
    a. Cleans the plaintext to contain only characters (a-z).
    b. Pads the string accordingly leaving space for the hash code.
    c. This padding ensures that we have enough characters to not leave any row empty while encryption.

2. HashFunction(String Input)
    a. Suppose Input = s1 s2 s3 … sn
    b. Fills a matrix of 8 (in our case) columns with the Input.
    c. Initialize hash code with a's.
    d. Take character-wise xor by each row and rotate left after each operation.

3. Encryptor
    a. Performs encryption through transposition.
    b. Populate plaintext as a matrix
    c. Permute columns as guided by the key.
    d. Read column by column to obtain the ciphertext.

4. Decryptor
    a. Performs decryption through transposition.
    b. Populate ciphertext as a matrix along 'key length' columns.
    c. Permute columns as guided by the key.
    d. Read row by row to obtain the plaintext.

Hritik Goel (2018148) and Dushyant Pancha(2018033)

5. PropertyCheck (π)
    a. Plaintext that we encrypt = plaintext + 8-character hashcode.
    b. If the last 8 characters = hash(remaining characters), satisfies π.

6. BruteForce
    a. Iterate over all possible permutations for key size 2 to 9.
    b. We create a list of candidate keys through bruteforce over 1 sample.
    c. Next, we tried candidate keys on the rest 4 samples.
    d. Correct key satisfies all the samples.

Sample Input and Output

```
Randomly Generated Key: [8, 9, 6, 4, 1, 5, 7, 2, 3]
Sample-1-----------------------------------------
plainText: i am hritik goel studying at IIITD
processedText: iamhritikgoelstudyingatiiitd
hashvalue: zvdebpcj
hashedText: iamhritikgoelstudyingatiiitdzvdebpcj
cipherText: rsteidickytjhladitibmegvtuipigidaonz
decipherText: iamhritikgoelstudyingatiiitdzvdebpcj
--------------------------------------------------

Sample-2-----------------------------------------
plainText: This is our NS assignment one
processedText: thisisournsassignmentonekwdr
hashvalue: gaoesysi
hashedText: thisisournsassignmentonekwdrgaoesysi
cipherText: isneunwsrmdissoosiesiataogkytnerhsng
decipherText: thisisournsassignmentonekwdrgaoesysi
--------------------------------------------------

Sample-3-----------------------------------------
plainText: my partner is Dushyant panchal
processedText: mypartnerisdushyantpanchalpq
hashvalue: fkhpowoh
hashedText: mypartnerisdushyantpanchalpqfkhpowoh
cipherText: rscpealornphaunhthhopdaknyawmitqyspf
decipherText: mypartnerisdushyantpanchalpqfkhpowoh
--------------------------------------------------

Sample-4-----------------------------------------
```

```
plainText: we have been assigned project two
processedText: wehavebeenassignedprojecttwo
hashvalue: qbrjlfco
hashedText: wehavebeenassignedprojecttwoqbrjlfco
cipherText: viejeetcedwoasjregclhsobbntfwnpoearq
decipherText: wehavebeenassignedprojecttwoqbrjlfco
-------------------------------------------------

Sample-5-----------------------------------------
plainText: Project involves transposition cipher system with brute
force attack
processedText:
projectinvolvestranspositionciphersystemwithbruteforceattackszvx
hashvalue: lydyaidf
hashedText:
projectinvolvestranspositionciphersystemwithbruteforceattackszvxlydya
idf
cipherText:
eeshwfcyirishczdnaoybevfjvopmeadcsieiokaolpiettytttrtrsipvnnsraxrosct
utl
decipherText:
projectinvolvestranspositionciphersystemwithbruteforceattackszvxlydya
idf
-------------------------------------------------


Launching brute force ...
Starting key searchh from length 1 to 9
Woooo! Found key :  (8, 9, 6, 4, 1, 5, 7, 2, 3)
```