BITFLIP

Aim:

To design and develop a cipher technique for encrypting plain text to obtain cipher text and decrypting cipher text to obtain original plain text.

Objective:

Develop a UI which allows to encrypt data by generating a random key and also decrypts the encrypted message using the same key.

Input Specimen:

* Input for encryption: Any Plain text to be encrypted
* Input for decryption: Cipher text and 8 bit key used in encryption process

Experimental Setup:

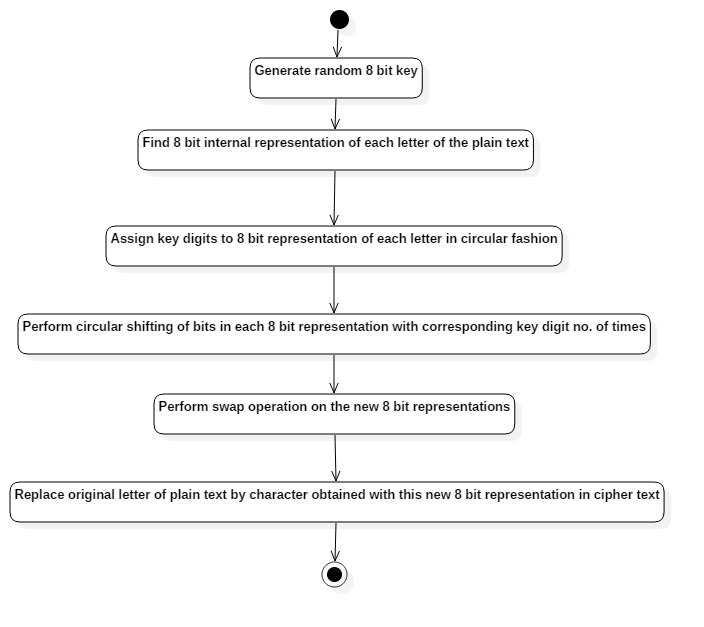
* Encryption Steps:

1. A random 8-bit key is generated which each key represents a value
2. Find 8-bit internal representation of each letter of the plain text
3. Assign the key digits to the 8-bit internal representation of each letter of the plain text computed in step ii. in circular fashion
4. Perform circular shifting of bits in each 8-bit representation with corresponding key digit number of times
5. Perform the Swap operation on the bits representation in Step iv
6. Character obtained from this new 8 bit representation will be used to replace/encrypt the plain text

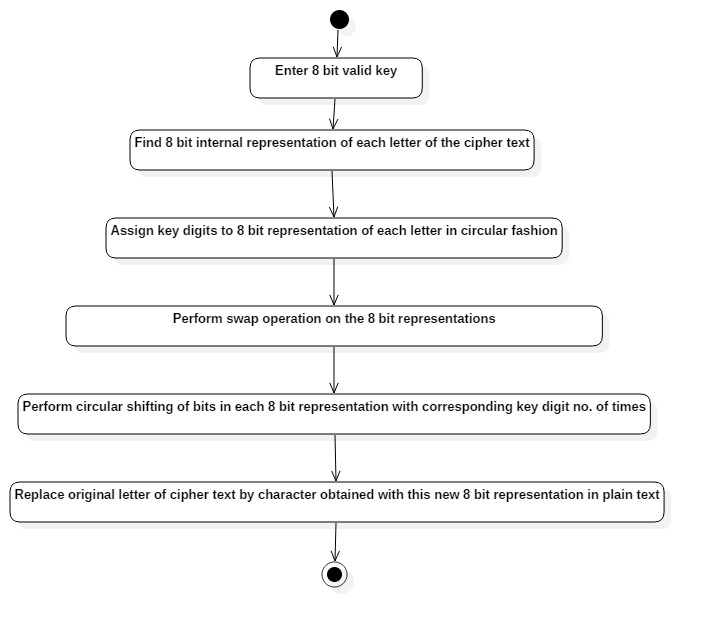
* Decryption Steps:

1. Use the 8-bit key generated in encryption process
2. Find 8-bit internal representation of each letter of the cipher text
3. Assign the key digits to the 8-bit internal representation of each letter of the plain text computed in step ii. in circular fashion
4. Perform the Swap operation on the bits representation
5. Perform circular shifting of bits in each new 8-bit representation with corresponding key digit number of times
6. Character obtained from this new 8 bit representation will be used to replace/decrypt the cipher text

Diagram:



Encryption Process



Decryption Process

Observation:

* Input size is directly proportional to time taken for completion of the process
* Parallelism approach helps in reducing time.
* Key generation randomness and manipulation of bits using Swap and circular shift increases randomness in security of the process

Conclusion:

* BitFlip cipher was designed and implemented using Java with aim at manipulation of the data at bit level to increase data security
* Main two operations used in this cipher technique are “SWAP” operation and “Circular Shift” operation
* Random key generation important feature as it adds into randomness as how data gets manipulated and transformed.