HAK Algorithm

Symmetric Cryptographic Technique

Harsh Baheti (20BCP065)

Aniket Gupta (20BCP049)

Kunal Gupta (20BCP068)

Introduction

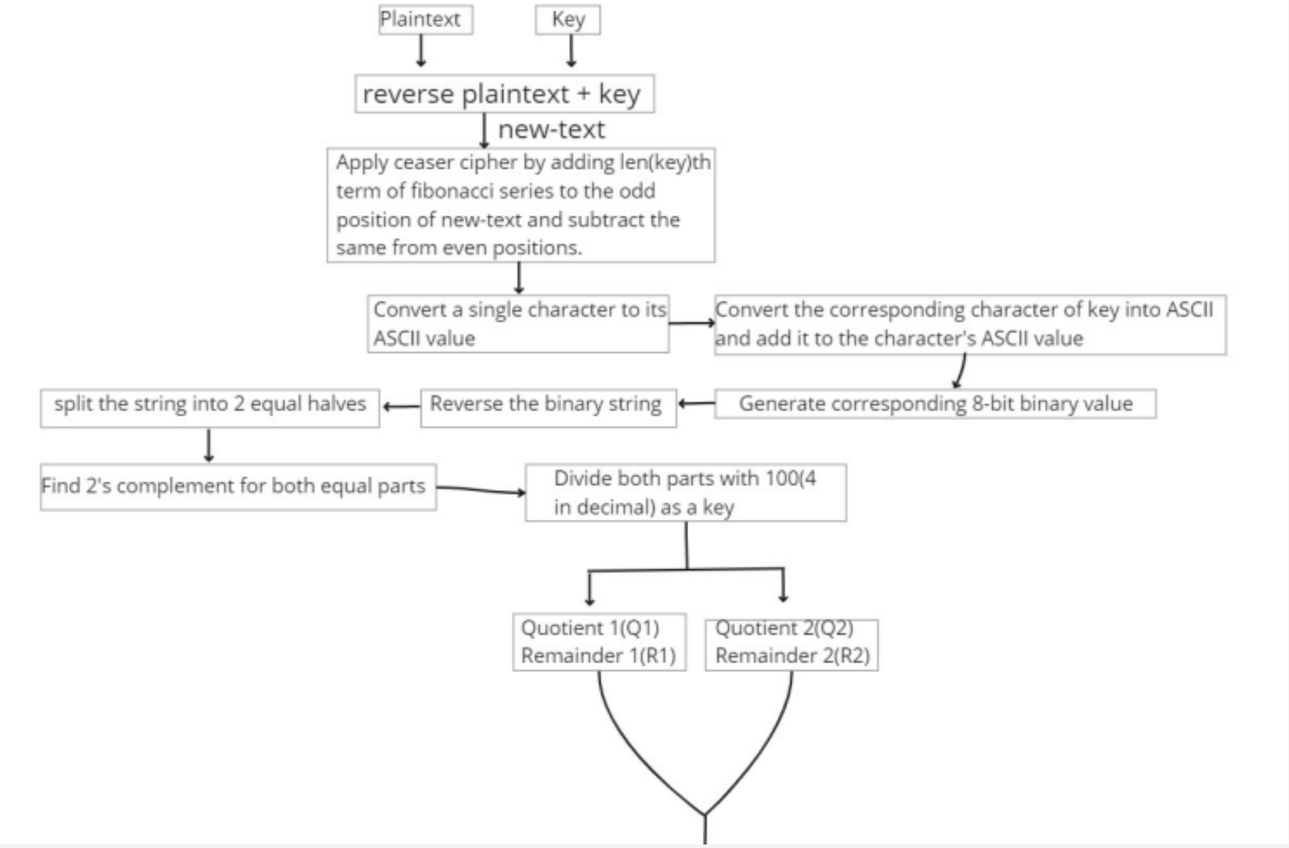
Encryption is one the most effective approach to achieve data security and privacy. The Encryption techniques hide the original content of a data in such a way that the original information is recovered only through using a key known as decryption process. The objective of the encryption is to secure or protect data from unauthorized access in term of viewing or modifying the data. Encryption can be implemented occurs by using some substitute technique, shifting technique, or mathematical operations. Several symmetric key base algorithms have been developed in the past year. In forward technique an efficient reliable symmetric key based algorithm to encrypt and decrypt the text data has proposed.

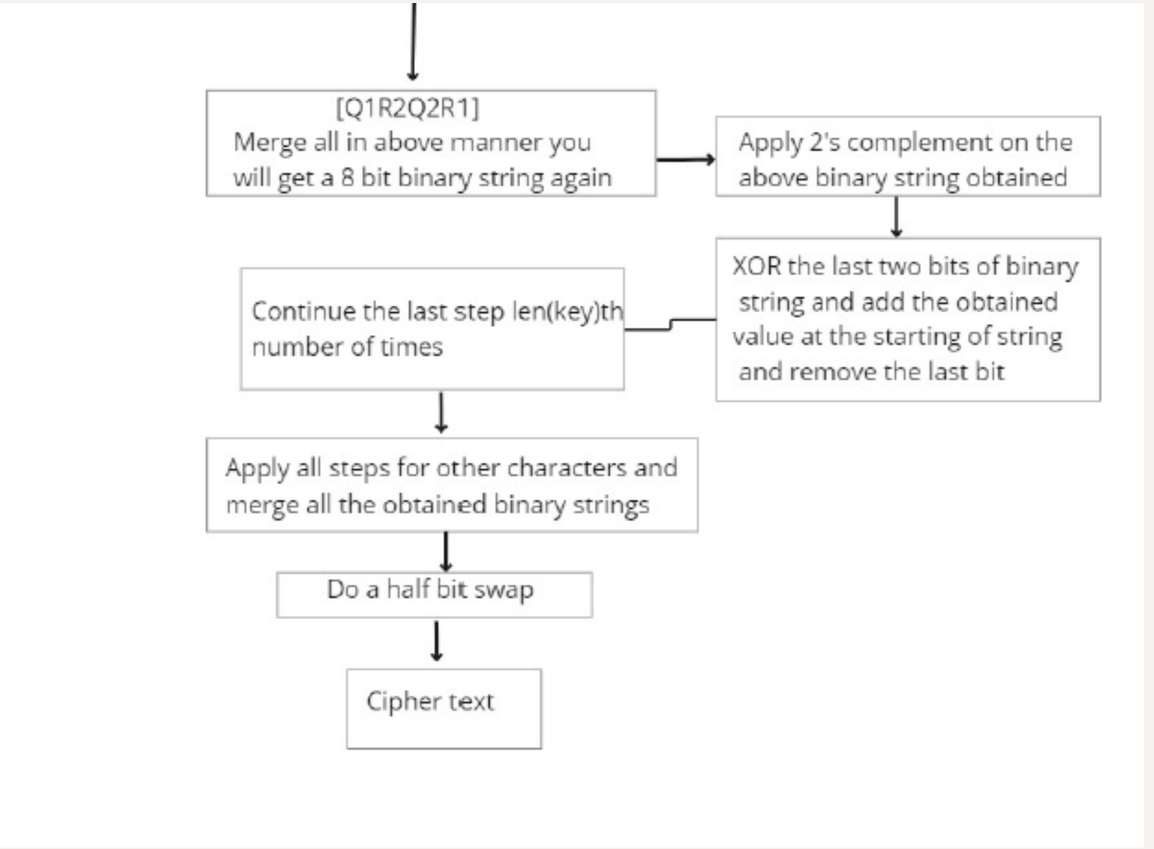
Purpose

The proposed method is used for **message** communication. Large message can be send securely using this encryption technique. The proposed approach is based on number of characters in message and simple calculation and operations are performed to minimize the execution time. In proposed work input will be a string of characters giving a string of binary numbers as output .

The Main Purpose is to built "A Secure and Fast Approach for Encryption and Decryption of Message Communication".

Proposed Work




[Q1R2Q2R1]
Merge all in above manner you will get a 8 bit binary string again
Apply 2's complement on the above binary string obtained
XOR the last two bits of binary string and add the obtained value at the starting of string and remove the last bit
Continue the last step len(key)th number of times
Apply all steps for other characters and merge all the obtained binary strings
Do a half bit swap
Cipher text

Example..

Plain text : plaintext (lowercase) Key : key

reverse Plaintext : txetnialp

newtext : txetnialpkey

- add and subtract len(key)th fibbonacci element alternatively

text : vvgrpgcjrigw

- Take first letter's ASCII value and add with key's corresponding letter's ASCII value

value : 118(v)+107(k)=225=11100001(in binary)

Reverse Binary : 10000111

- Dividing Binary in two parts

e1 : 1000 e2 : 0111

- 2's compliment of individual part

e'1 : 1000 e'2 : 1001

- Divide both the elements with 100 (Find Corresponding Quotient and Remainder)

Q1=10 Q2=10

R1=00 R2=01

- Now Merge in the manner (Q1R2Q2R1)

Merge(m) : 10011000

- Apply 2's compliment

m' : 01101000

- XOR last 2 bits add it to first and remove the last bit
- continue this step for len(key) times(here 3)

xor1 : 00110100

xor2 : 00011010

xor3 : 10001101

- Continue all the above steps for the remaining letters and combine all the corresponding binary strings
- Lastly , apply half bit swap and you will get the cipher text

References

- https://www.researchgate.net/profile/Ekta-Agrawal-2/publication/320149845_A_Secure_and_Fast_Approach_for_Encryption_and_Decryption_of_Message_Communication/links/59d111d30f7e9b4fd7fa2172/A-Secure-and-Fast-Approach-for-Encryption-and-Decryption-of-Message-Communication.pdf

- https://www.ijarcsse.com/docs/p

- https://www.ijert.org/cryptographic-algorithm-for-enhancing-data-security-a-theoretical-approach

Thank You ..

We're ready to answer your questions.