Improve Security Algorithm Cryptography Vigenere

Cipher Using Chaos Functions

Introducere :

Scopul proiectului este îmbunătățirea algoritmului Vigenere Cipher folosind funcția chaos (Logistic map). Pentru a obține o cheie care are o securitate puternica, cand se aplica formula de "logistic map" o sa genereze numere aleatoare care se vor baza pe doua constante din formula "r" și "K0" , astfel spargerea criptarii va deveni foarte complexă fata de un Vigenere Cipher normal care folosește o cheie simpla, atunci aceeași cheie se va repeta de mai multe ori , astfel poate fi sparta dacă folosim un dictionary in python cu usurinta. Prin logistic map vom transforma Vigenere Cipher într-o un stream cipher .

Functia logistic map :

$$x_{i+1} = r\, x_i\, (1 - x_i)$$

Algoritmul :

O sa generam un număr dublu fata de caracterele din text, pentru a fi siguri ca e suficient. Astfel facem modul de 100003 pe funcția logistic map, pentru a obține numere prime și fiecare număr sa fie de 5 cifre. După ce obțin valorile aleatoare, trebuie concatenate toate valorile generate ca un șir lung de numere.
În pasul doi vom grupa din acest șir doua cate doua numere de la începutul șirului pana la finalul acestuia. La pasul trei luăm din toate grupările cate un grup de 2 numere pentru fiecare caracter .

Criptarea :

Aplicam formula de criptare Vinegar Cipher clasic : yi = xi + ki (mod 26).
Adunam fiecare grup de 2 numere obtinut din funcția logistic map care reprezinta cheia cu valoarea caracterului din tabelul de plain text, aplicând modul de 26 după adunare, astfel rezultatul va fi un numar care reprezinta un caracter diferit de cel din text.

Decriptare :

Aplicam formula de decriptare Vinegar Cipher clasic : xi = yi - ki (mod 26).
Scadem fiecare grup de 2 numere (grup care reprezinta cheia din fiecare caracter) din textul criptat a carui valoare va fi obtinuta din tabelul de caractere . Rezultatul va fi, astfel, numarul care reprezinta caracterul plain text-ului si poate fi găsit în tabel de caractere.

Tabelul de caractere :

0 = a	1 = b	2 = c	3 = d	4 = e
5 = f	6 = g	7 = h	8 = i	9 = j
10 = k	11 = l	12 = m	13 = n	14 = o
15 = p	16 = q	17 = r	18 = s	19 = t
20 = u	21 = v	22 = w	23 = x	24 = y
25 = z				

Exemplu de valori generate de logistic map :

Daca k0 = 6 & r = 4;
k1 = 99880, k2 = 41920, k3 = 22080, k4 = 82720,
k5 = 37280, k6 = 55520, k7 = 40480, k8 = 40320, k9 = 51680,
k10 = 17120, k11 = 90880, k12 = 65920 etc

Comparatie intre Vigenere Cipher classic și chaos Vigenere Cipher :

*Vigenere Cipher classic :

- **Securitate slaba , folosește dar 26 de caractere pentru a crea o cheie .**
- **Foarte ușor de spart pentru ca nu folosește altceva decat literele alfabetului .**

***chaos Vigenere Cipher:**

- **Securitate foarte buna dacă va fi făcuta o modificare mica la valoarea inițială, va fi o schimbare mare la valorile funcției .**
- **Plain text-ul foarte greu de spart, dacă valoarile "K0" și "r" vor fi schimbate, toate valorile cheii vor fi modificate.**

Dezavantaje de chaos Vigenere Cipher :

Dezavantajul este ca ecuatiile logistic map din functia chaos trebuie sa stocheze cheia generata in procesul de criptare, procesul cheie de stocare fiind esential pentru a efectua procesul de decriptare.

Statistica fiecarui caracter din alfabet în cei doi algoritmi:

Chaos Vigenere Cipher :

A: 115,
B: 119,
C: 110,
D: 129,
E: 111,
F: 126,
G: 95,
H: 107,
I: 119,
K: 112,
L: 92,
M: 118,
N: 115,
O: 98,
P: 96,
Q: 103,
R: 116,
S: 129,
T: 102,
V: 109,
X: 100,
Y: 133,
Z: 116

R = 7 , K0 = 6;

Classic Vigenere Cipher :

A: 144,
B: 127,
C: 84,
D: 78,
E: 181,
F: 120,
G: 135,
H: 102,
I: 131,
K: 77,
L: 118,
M: 119,
N: 90,
O: 88,
P: 103,
Q: 102,
R: 174,
S: 100,
T: 112,
V: 152,
X: 119,
Y: 92,
Z: 102

Key = "RandomTextGeneratorisawebapplicationwhichprovidestruerandomtext"