Matematica Haosului în Criptografie

Realizată de Chisilev Andrei și Coșulea Bianca-Iuliana.

Introducere în Criptografie și Haos

Criptografia protejează informațiile sensibile în era digitală.

Necesită generatoare de numere pseudorandom robuste.

Teoria haosului oferă un cadru intrigant pentru secvențe aleatorii.

Sistemele haotice sunt deterministe, dar imprevizibile.

Rolul Criptografiei

Protejarea datelor sensibile și a comunicațiilor.

Importanța Imprevizibilității

Chei criptografice și valori aleatorii esențiale.

Haosul în Criptografie

Generarea de secvențe aparent aleatorii.

Fundamentele Teoriei Haosului

Sistemele haotice sunt deterministe, dar par aleatorii.

Sunt guvernate de legi matematice precise.

Diferă de sistemele cu adevărat aleatorii.

Sistem Aleatoriu

Rezultate fundamental imprevizibile.

Exemple: aruncarea zarurilor, fenomene cuantice.

Sistem Haotic

Comportament complex, aparent aleatoriu.

Sensibilitate ridicată la condițiile inițiale.

Proprietăți Cheie ale Sistemelor Haotice

Determinism

Reguli matematice fixe, fără aleatoriu inerent.

Sensibilitate la Condiții Inițiale

Mici schimbări duc la traiectorii diferite (efectul fluturelui).

Neliniaritate

Ecuații neliniare generează dinamică imprevizibilă.

Aparent Aleatoriu

Traiectoriile par aleatorii, greu de anticipat.

Exemple de Sisteme Haotice

Harta Logistică și Sistemul Lorenz sunt exemple clasice.

Ele demonstrează complexitatea și sensibilitatea haosului.

Acestea sunt relevante pentru aplicații criptografice.

Harta Logistică

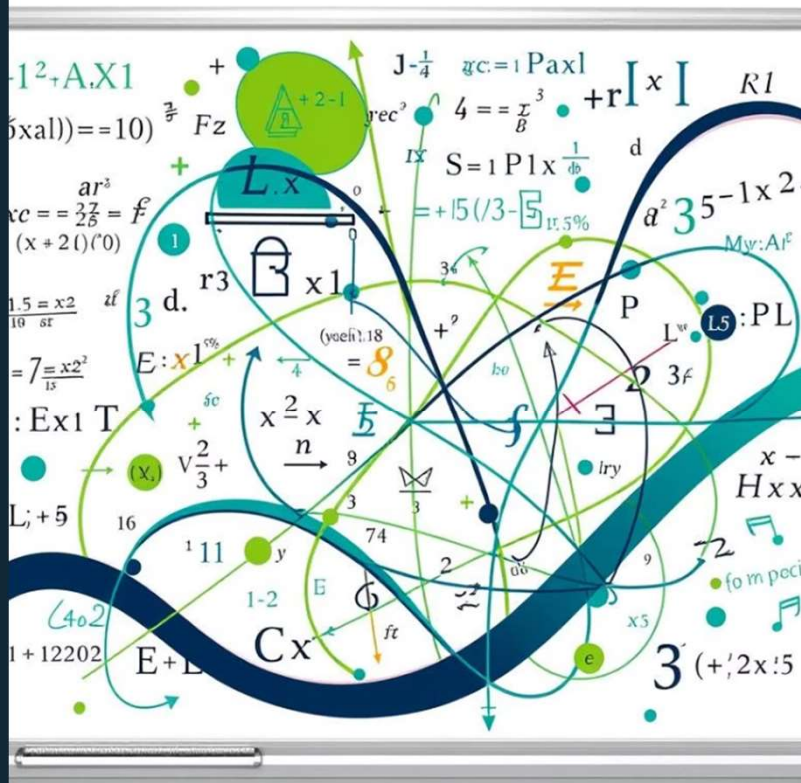
Model matematic simplu pentru creșterea populației.

Intră în regim haotic pentru anumite valori.

Sistemul Lorenz

Ecuații diferențiale pentru convecția termică.

Faimos pentru atractorul său haotic.



Harta Logistică și Secvențele Haotice

Harta logistică generează comportament haotic.

Formula sa este $x_{n+1} = r \cdot x_n \cdot (1 - x_n)$.

Este utilă pentru generarea de secvențe criptografice.

Chei Criptografice

Parametrul r și x_0 pot servi ca cheie secretă.

Generare Biți

Valorile x_n pot fi convertite în biți pseudorandom.

Permutare Date

Secvențele haotice pot permuta elemente de date.

Generatoare Pseudorandom și Haos

PRNG-urile sunt esențiale în criptografie.

CSPRNG-urile sunt special concepute pentru securitate.

Haosul oferă o alternativă intrigantă pentru PRNG-uri.

1

PRNG

Algoritm determinist, produce secvențe aparent aleatorii.

Poate deveni previzibil dacă algoritmul sau seed-ul sunt cunoscute.

2

CSPRNG

Rezistă atacurilor predictive, nu permite reconstrucția.

Folosește algoritmi sofisticați și surse de entropie.

Avantaje și Riscuri ale Haosului în Criptografie

Implementarea haosului este simplă și rapidă.

Oferă entropie aparentă ridicată și comportament complex.

Riscurile includ compromiterea prin parametri cunoscuți.

Avantaje

Implementare simplă și rapidă.

Entropie aparentă ridicată.

Comportament neliniar și complex.

Riscuri

Compromitere dacă parametrii inițiali sunt cunoscuți.

Majoritatea sistemelor haotice sunt reversibile.

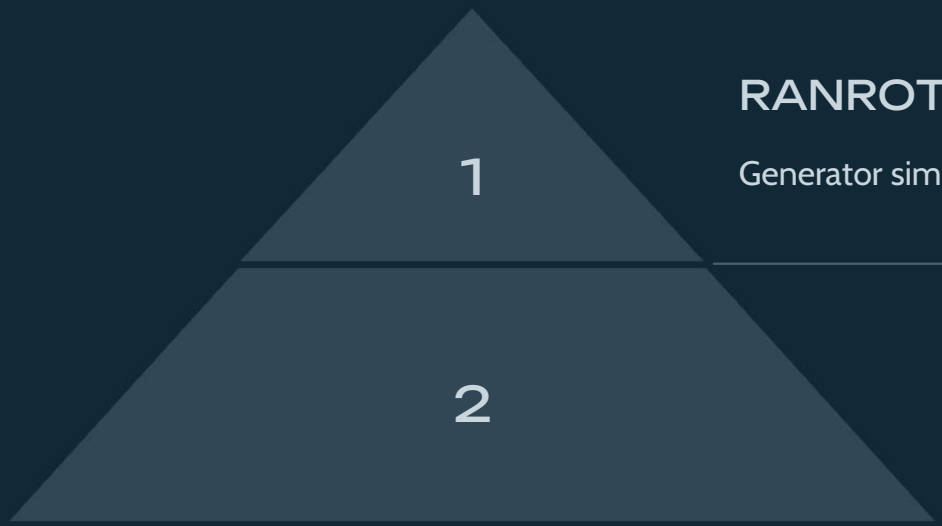
Nu toate hărțile haotice sunt sigure criptografic.

Funcțiile RANROT – Agner Fog

RANROT este o familie de generatoare pseudorandom.

Sunt rapide și simple, ideale pentru aplicații non-criptografice.

Agner Fog a propus două versiuni principale.



RANROT Tip A

Generator simplu și rapid, combina rotații de biți și adunări.

RANROT Tip B

Versiune mai complexă, folosește un buffer circular și rotații multiple.

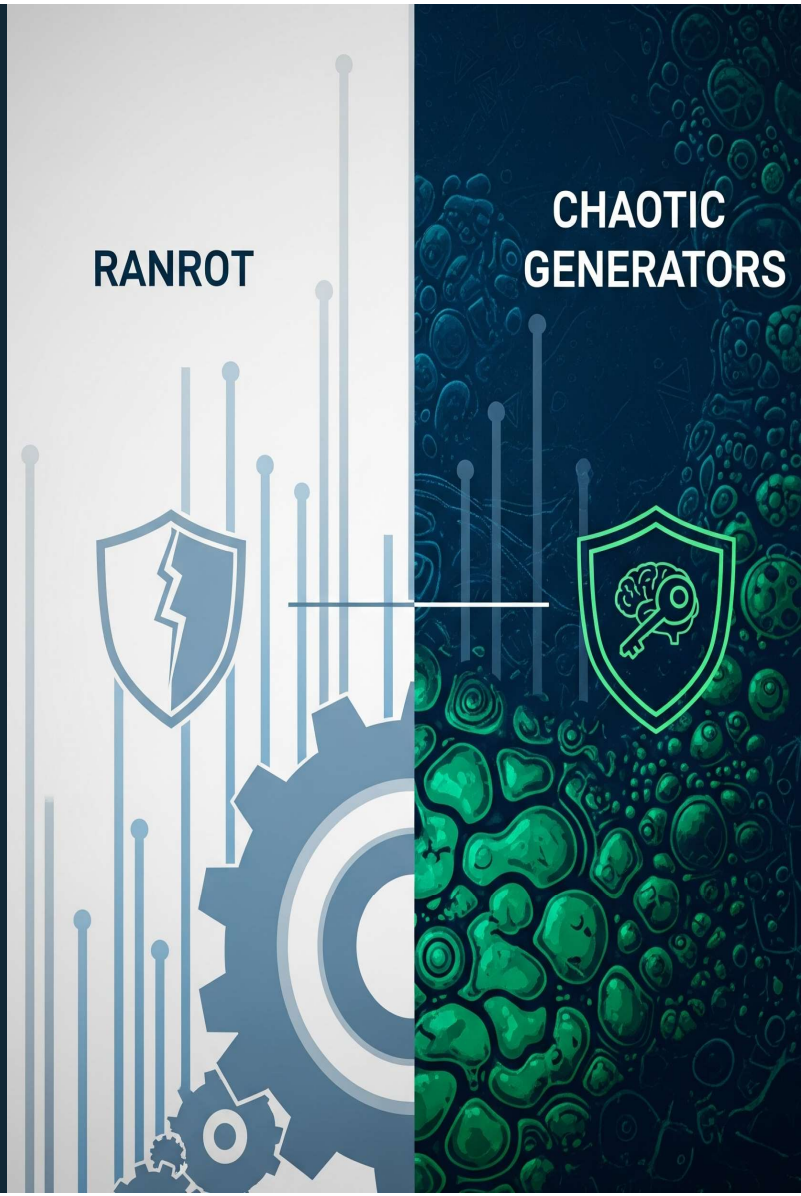
Comparație RANROT cu Generatoarele Haotice

Ambele sunt deterministe și par imprevizibile.

RANROT este eficient și ușor de implementat.

Nu este considerat un CSPRNG din cauza limitărilor criptografice.

Caracteristică	RANROT	Generatoare Haotice
Determinism	Da	Da
Eficiență	Ridicată	Bun
Complexitate Implementare	Scăzută	Medie
Securitate Criptografică	Limitată (nu CSPRNG)	Potențială (depinde de implementare)



Criptografia bazată pe haos: Aplicații practice

Pentru a ilustra modul în care conceptele teoretice din matematica haosului pot fi aplicate în criptografie, au fost realizate două experimente practice. Acestea demonstrează utilizarea generatorilor pseudo-aleatori haotici pentru criptarea textului și a imaginilor digitale.

Experimente practice de criptare

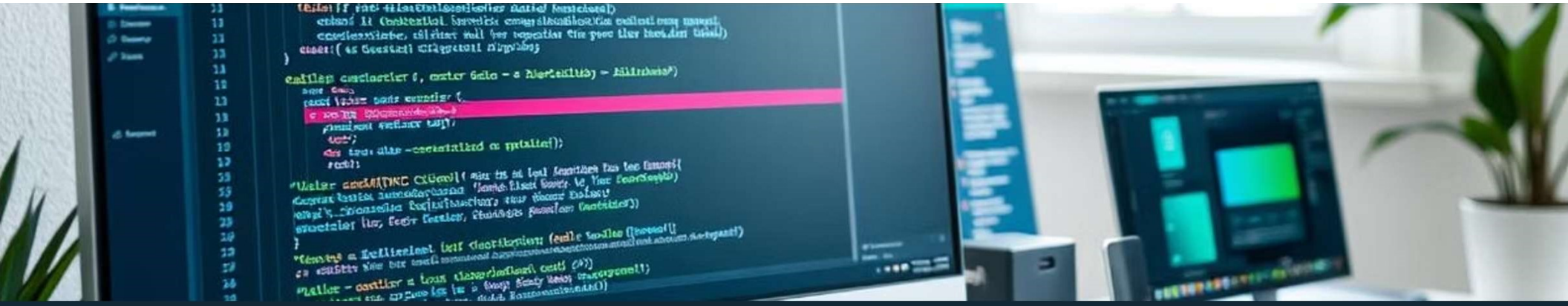
Am realizat două experimente practice pentru a ilustra aplicarea conceptelor de matematică a haosului în criptografie. Acestea demonstrează utilizarea generatoarelor pseudo-aleatoare haotice pentru criptarea textului și a imaginilor digitale.

Criptarea textului

Textul este convertit într-o secvență de octeți folosind codificarea UTF-8, apoi criptat cu o mască generată haotic.

Criptarea imaginilor

Imaginile digitale sunt transformate într-un flux de octeți, reprezentând datele pixelilor, și criptate similar cu textul.



Detalii de implementare

Implementarea practică a fost dezvoltată în Python, cu o interfață de utilizator creată cu Streamlit. Logica criptografică de bază este modularizată pentru claritate și eficiență.

Limbaj de programare

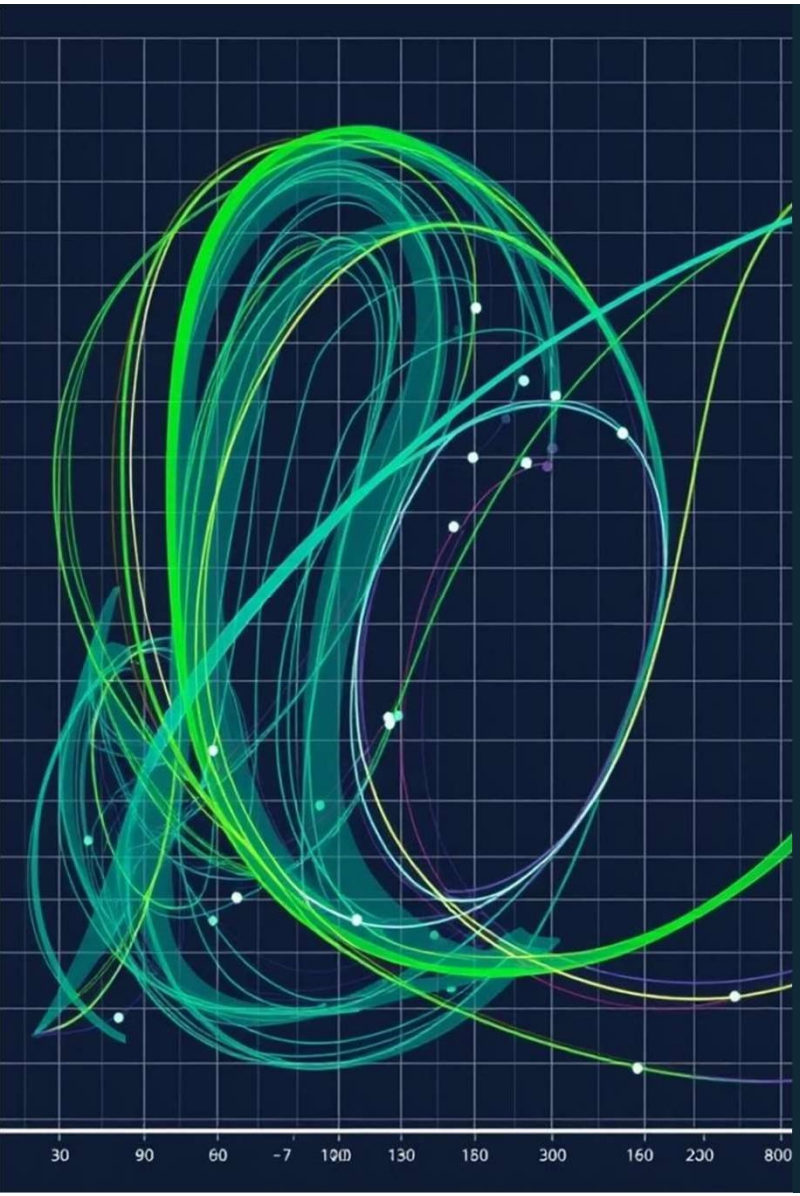
Python a fost ales pentru flexibilitatea și bogăția bibliotecilor sale, facilitând dezvoltarea rapidă.

Interfață utilizator

Streamlit a permis crearea unei interfețe intuitive, organizată pe pagini separate pentru criptarea imaginilor și a textului.

Modularitate

Logica criptografică este structurată modular, asigurând o mai bună mentenabilitate și scalabilitate a codului.



Generarea cheii haotice: Harta Logistică

O secvență de octeți pseudo-aleatoare este generată folosind ecuația hărții logistice. Comportamentul sistemului este guvernat de parametrul de control r și de o condiție inițială x_0, care împreună formează cheia secretă.

Ecuația hărții logistice

$$x_{n+1} = r \cdot x_n \cdot (1 - x_n)$$

Parametri cheie

r (în regim haotic, 3.57-4.0) și x_0 (între 0 și 1) servesc drept cheie secretă.

Faza tranzitorie

O serie inițială de iterații este efectuată și rezultatul său este eliminat pentru a asigura stabilitatea generatorului.

Generarea cheii pseudo-aleatoare: RANROT-B

Generatorul RANROT-B se bazează pe o stare internă menținută într-un buffer circular. Această stare este populată inițial pe baza unei semințe întregi furnizate de utilizator, care servește drept cheie secretă.

Buffer circular

Starea internă este menținută într-un buffer circular, asigurând o gestionare eficientă a memoriei.

Semințăsecretă

O semințăîntreagă furnizată de utilizator inițializează starea, folosind un Generator Congruențial Liniar (LCG).

Valori pseudo-aleatoare

Noi valori sunt produse prin combinarea a două valori decalate din buffer printr-un proces aditiv.

Gestionarea datelor și criptarea XOR

Pentru criptare, datele de intrare (text sau imagine) sunt convertite într-un flux de octeți. Masca generată (de la Harta Logistică sau RANROT-B) este adaptată la lungimea exactă a datelor. Criptarea se realizează prin aplicarea unei operații XOR bit cu bit.

Masca adaptată

Masca generată se potrivește exact cu lungimea datelor.

Conversia datelor

Textul în UTF-8, imaginile în flux de octeți.

Operația XOR

Criptarea se face prin XOR între date și mască.

Procesul de decriptare

Decriptarea se realizează prin aplicarea aceleiași operații XOR, utilizând exact aceeași mască pseudo-aleatoare folosită pentru criptare. Reversibilitatea inerentă a operației XOR asigură recuperarea fidelă a datelor originale.

1

Regenerarea măștii

Masca trebuie regenerată cu parametrii cheie originali (r și x_0 pentru Harta Logistică, sau semința pentru RANROT-B).

2

Aplicarea XOR

Aceeași operație XOR este aplicată datelor criptate.

3

Recuperarea datelor

Textul sau imaginea originală este recuperată fidel datorită reversibilității XOR.

Rezultate și sensibilitate la cheie

Exemplele practice demonstrează că o modificare minimă a parametrilor cheie duce la o decriptare complet eronată, evidențiind sensibilitatea sistemului.

1

Text original

"Hello, chaos and encryption!"

2

Text criptat

Sm9K7pAvK078mHUTz13XqISPILrzhnJ+QOaTKQ== (Base64)

3

Text decriptat

"Hello, chaos and encryption!" (cu aceiași parametri)

4

Sensibilitate

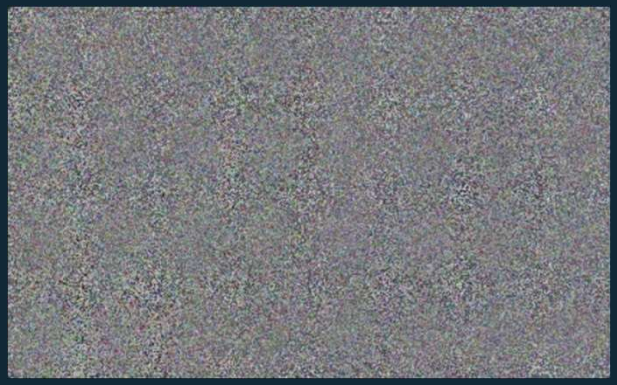
Modificarea minimă a r sau x_0 (Logistic Map) sau a seminței (RANROT) duce la date ilizibile.

Criptarea imaginilor: Demonstrație vizuală

Criptarea unei imagini .png cu Harta Logistică sau RANROT-B transformă imaginea într-un zgomot aleatoriu. Decriptarea cu exact aceleași chei restabilește imaginea originală, demonstrând eficacitatea metodei.

Imagine originală

O imagine .png clară și lizibilă, gata de criptare.



Imagine criptată

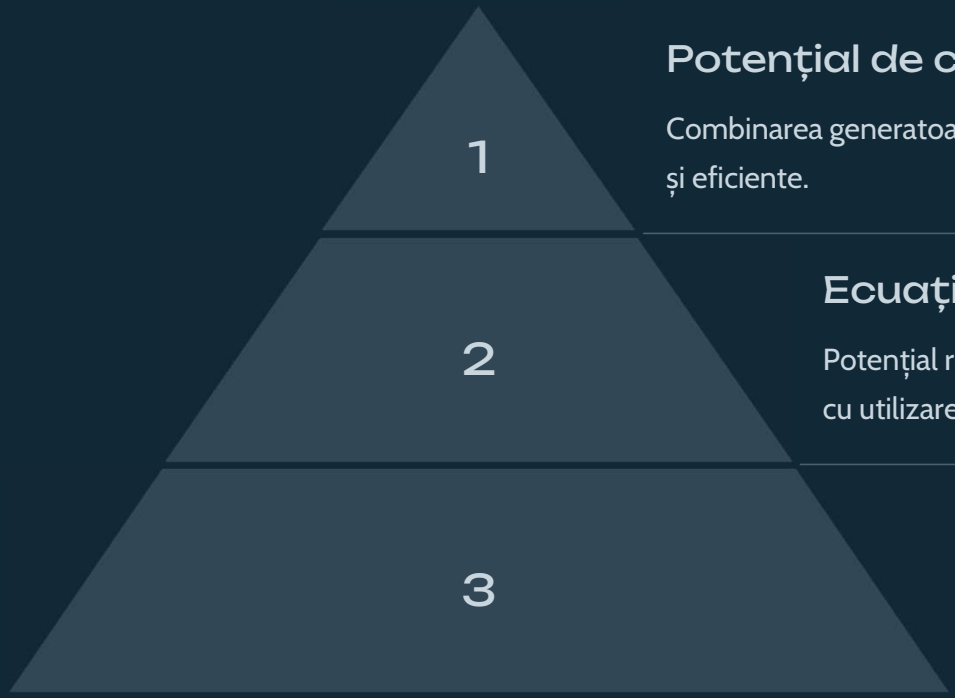
După criptare, imaginea apare ca un zgomot aleatoriu, complet nerecognoscibilă.

Imagine decriptată

Cu aceleași chei, imaginea este decriptată și este identică cu originalul.

Concluzii și potențial de cercetare

Matematica haosului oferă un cadru puternic pentru criptografie, valorificând proprietăți precum sensibilitatea la condițiile inițiale și aleatorietatea aparentă. Există un potențial considerabil de cercetare în combinarea generatoarelor haotice cu metode criptografice bine stabilite.



Potențial de cercetare

Combinarea generatoarelor haotice cu metode criptografice consacrate pentru sisteme sigure și eficiente.

Ecuația logistică

Potențial real pentru generarea de secvențe pseudo-aleatoare utile în criptografie, cu utilizare precaută.

Funcțiile RANROT

Metodă eficientă și rapidă pentru generarea de numere pseudo-aleatoare, dar cu limitări de securitate criptografică.