LINEAR ALGEBRA PROJECT

CHAOTIC DYNAMICS ANALYSIS AND ITS APPLICATION IN CRYPTOGRAPHY

Presented by Aryan, Saswat and Tushitaa

PROJECT OVERVIEW

- In this project we will explore how chaos analysis of logistic map equation can be utilized to create an efficient PRNG and in turn a secure encryption algorithms.
- We will discuss the basics of encryption, the logistic map equation, and their integration in encryption algorithms.
- Let's dive into the fascinating world of harnessing chaos for secure communication!

METHODOLOGY

1st

Research and Understand the Logistic Map Equation

2nd

Chaos Analysis of The logistic map

3rd

Development of PRNG

4th

Integrating PRNG into Cryptographic model

The Logistic Map Equation

- The logistic map equation is a classic example of a chaotic dynamical system.
- It is given by the equation:

$$X_{n+1} = r * X_n * (1 - X_n),$$

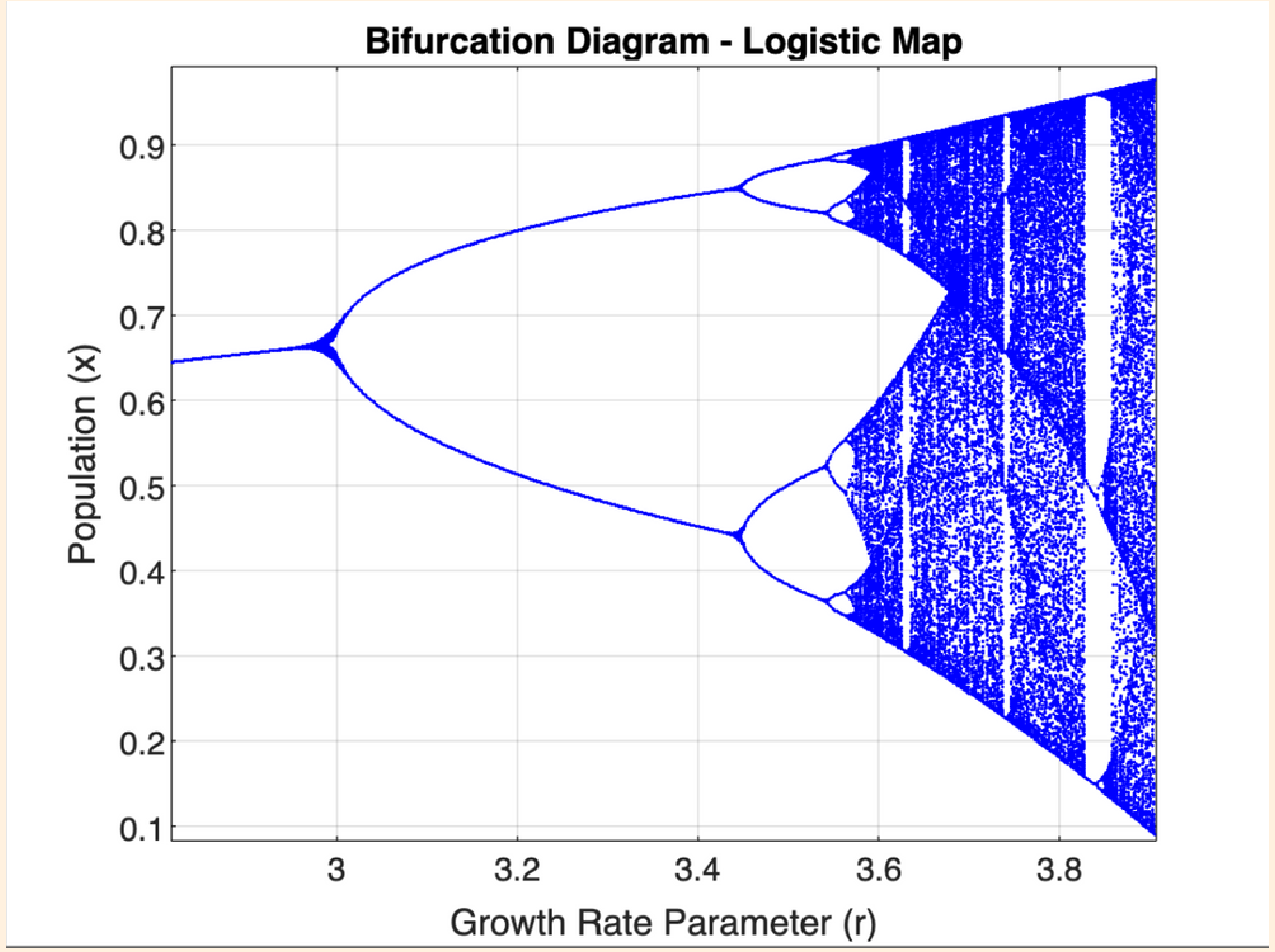
where Xn represents the population at time n, and r is a parameter representing the growth rate.

- The logistic map equation exhibits a wide range of complex behaviors, including periodicity, bifurcations, and chaotic dynamics

Chaos Analysis of the logistic map

- Lets say we chose r=2 and initial value of x as 0.5. After doing some iterations we will see that on further iterations x is not growing but stable at a constant value.
- What if r is >3, then after some iterations x is oscillating its value between two values.
- As we go on to increase x is oscillating between 4, 8, 16 and after some time its total chaos.
- This is what represented in the bifurcation diagram for different values of r and the trajectory of x.

Bifurcation Diagram Plot



Chaos Analysis of the logistic map

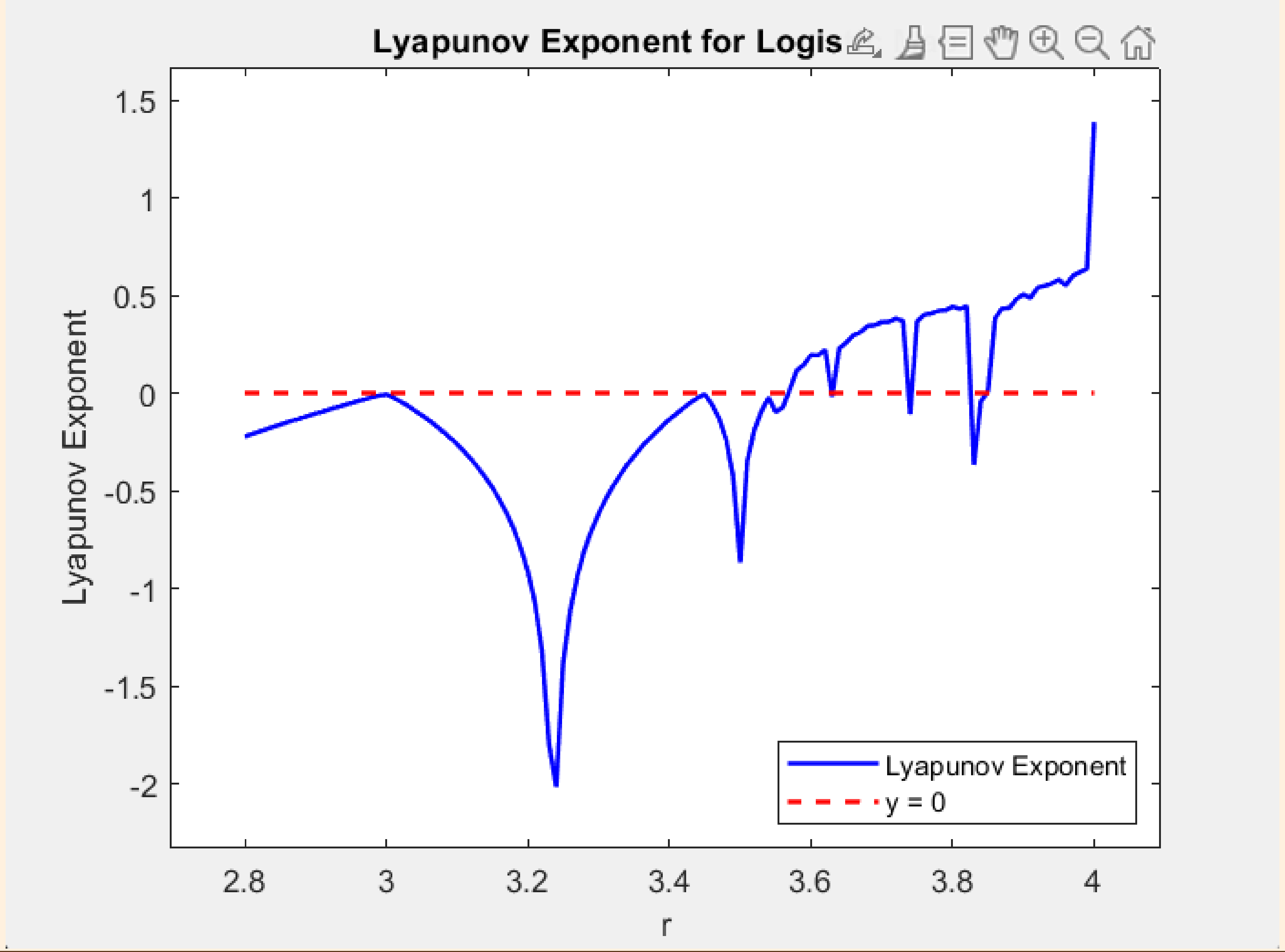
- Chaos theory studies the behavior of complex and unpredictable systems.
- So how do we find where the system is chaotic or where it is not. There is a way to do this using Lyapunov exponent which is numerically calculated as:- (where f(x) is the logistic map equation.)

$$\lambda_L = \mathrm{Lim}_{n \to \infty} \frac{1}{n} \sum_{i=1}^{n} \ln \left| f'(x_i) \right|$$

Chaos Analysis of the logistic map

- Another way to calculate lyapunov exponent using linear algebra techniques is by Finding the jacobian matrix (partial derivatives of logistic map at a particular r).
- Using Singular value Decomposition to find the sigma matrix. The largest eigenvalue is obtained with help of this singular matrix which represents the approximate lyapunov exponent at that instant.
- If lyapunov exponent is positive the system is chaotic, if it is 0 at some point it means bifurcation is happening at that instant. If it is negative the system is not chaotic

Chaos Analysis of the logistic map



Development of PRNG

- After we know that when the system is chaotic which is for $r>4$ we have developed a PRNG function which takes x_n as input value and generates random value on the trajectory of x_n for $r=4.1$.
- For every call this function updates a variable named self which is used to move forward in trajectory after every function call.

Encryption Algorithms

- We have developed a simple cryptographic model which uses basic block ciphers and apply them randomly in any order while encrypting and decrypts using the reverse order.
- Each of the algorithm has been improved while implementing individually.
- We have only used our developed PRNG function wherever required in individual ciphers and main encryption file.

Encryption Algorithms

We used 3 Algorithms ;

- Shift Cipher
- Vignere Cipher
- Substitution Cipher

Let's wrap it up
and see a small Demo

CONCLUSION

The integration of the logistic map equation in encryption algorithms provides a novel approach to enhance security in communication systems.

By harnessing chaos and the unpredictability of chaotic systems, logistic map encryption offers robust protection against cryptographic attacks.

Embracing chaos theory opens up new avenues for innovation in the field of cryptography.

A WARM THANK YOU TO ALL OF YOU!

PLEASE FEEL FREE TO ASK ANY QUESTIONS