ENCRYPTA: Chaos and Cryptography – A Software Based on the Logistic Map

Buniac, Felipe

I have developed a cryptography program, ENCRYPTA. My theoretical reference was Chaos Theory, particularly Logistic Maps – complex, dynamic systems that are rigorously deterministic and sensitive to initial conditions, that by modulating a supplementary recurring property makes it non-predictable over time. To write the software, I chose MATLAB, because it is a high-level, easy-to-learn, descriptive language and ease to manipulates data. I initially developed the first function, responsible for calculating and plotting the Logistic Map; next, one which calculates the value of Xn and which would from that value be associated with the interval wherein it is found in the Map. After that, I developed another function that would calculate the number of iterations before reaching the desired interval, followed by the function that associates the interval with the desired character. To complete the program, I synthesized all of the above functions, which coded and decoded only a single character, and, to use any number of characters, I created a vector that stores characters. The model underwent effectiveness and cryptanalysis tests to stress its security. I sent the same message hundreds of times to make sure that no noise would alter its content. Different key and message size configurations were used. The results confirmed the effectiveness and security previewed. ENCRYPTA marketable version will be offered as a plug-in. Furthermore, the distinction that will make it the best option is that in addition to being based in a nonlinear dynamic system, it includes point-to-point cryptography. Meaning data can circulate freely without risks.

Awards Won: