Conference: Congreso Interdisciplinario de Energías Renovables - Mantenimiento Industrial - Mecatrónica e Informática

Booklets

RENIECYT - LATINDEX - Research Gate - DULCINEA - CLASE - Sudoc - HISPANA - SHERPA UNIVERSIA - E-Revistas - Google Scholar

DOI - REBID - Mendeley - DIALNET - ROAD - ORCID

Title: Algoritmo Criptográfico Con Semilla Caótica y Generador Congruencial Para Fortalecer La Seguridad De Los Datos Transmitidos De Forma Inalámbrica

Author: Angélica ELIZALDE CANALES

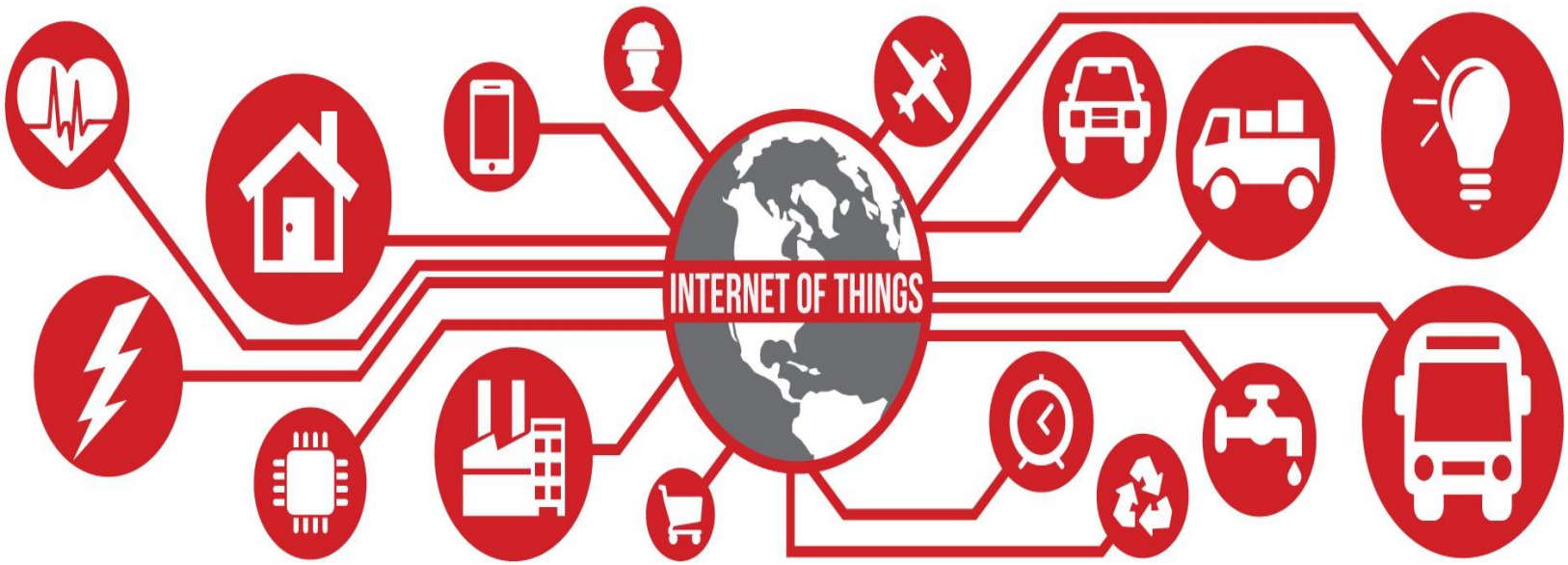
Editorial label ECORFAN: 607-8324
BCIERMIMI Control Number: 2017-02
BCIERMIMI Classification (2017): 270917-0201

Pages: *13*
Mail: *francisca.elizalde@upt.edu.mx*
RNA: 03-2010-032610115700-14

Contenido

- Introducción
- Problemática
- Resultados experimentales
- Conclusiones
- Referencias

IoT para el la industria energética



http%3A%2F%2Fmundoejecutivo.com.mx%2Fsites%2Fdefault%2Ffiles%2Finternet.png&imgrefurl

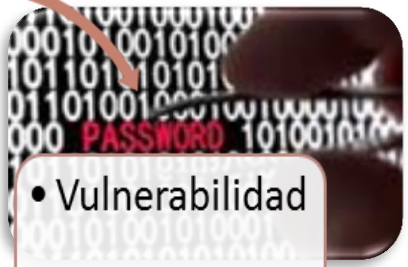
Problemática

• Amenaza

crea

Explota

• Ataque



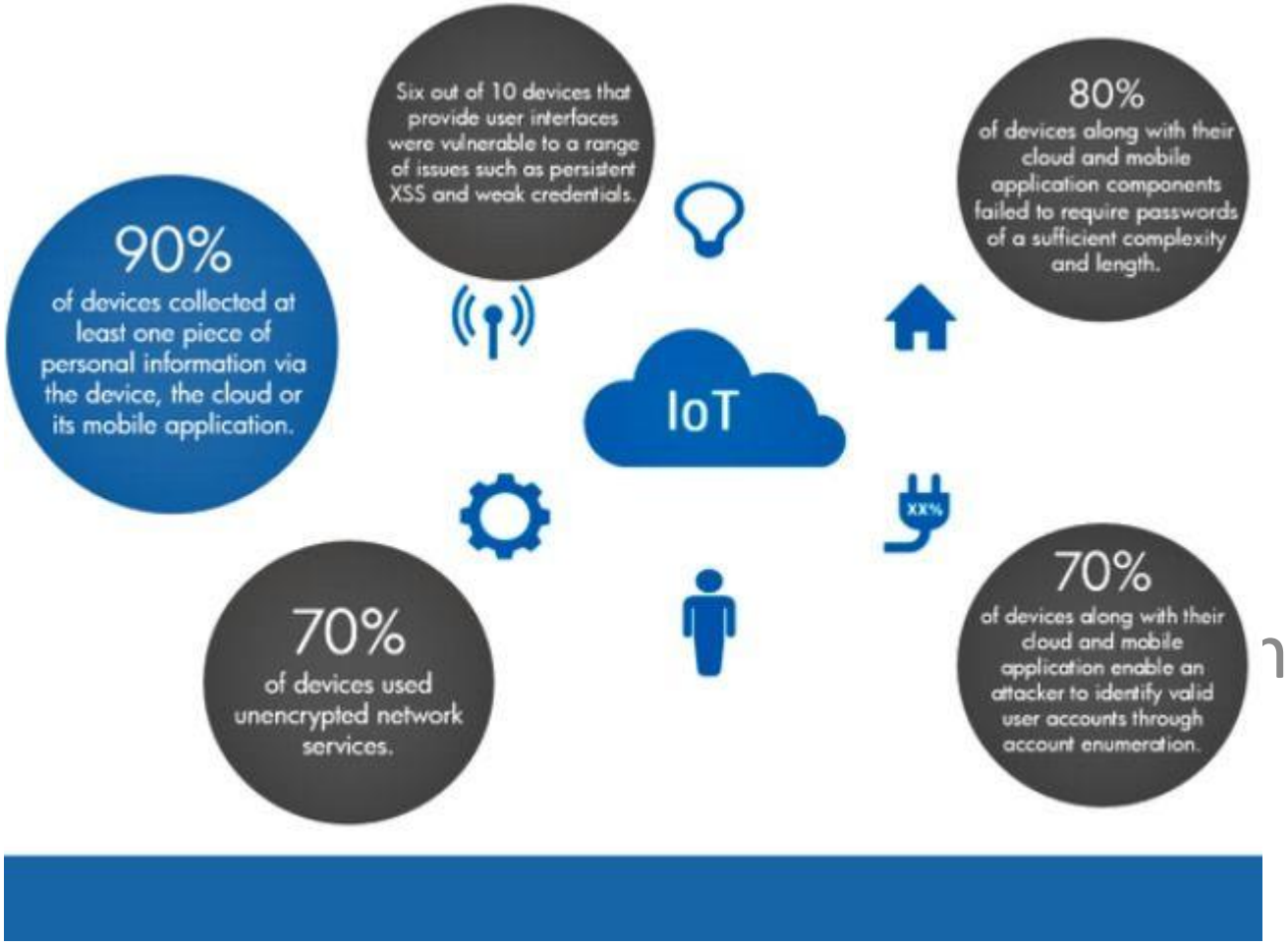
• Vulnerabilidad

Genera

Control preventivo

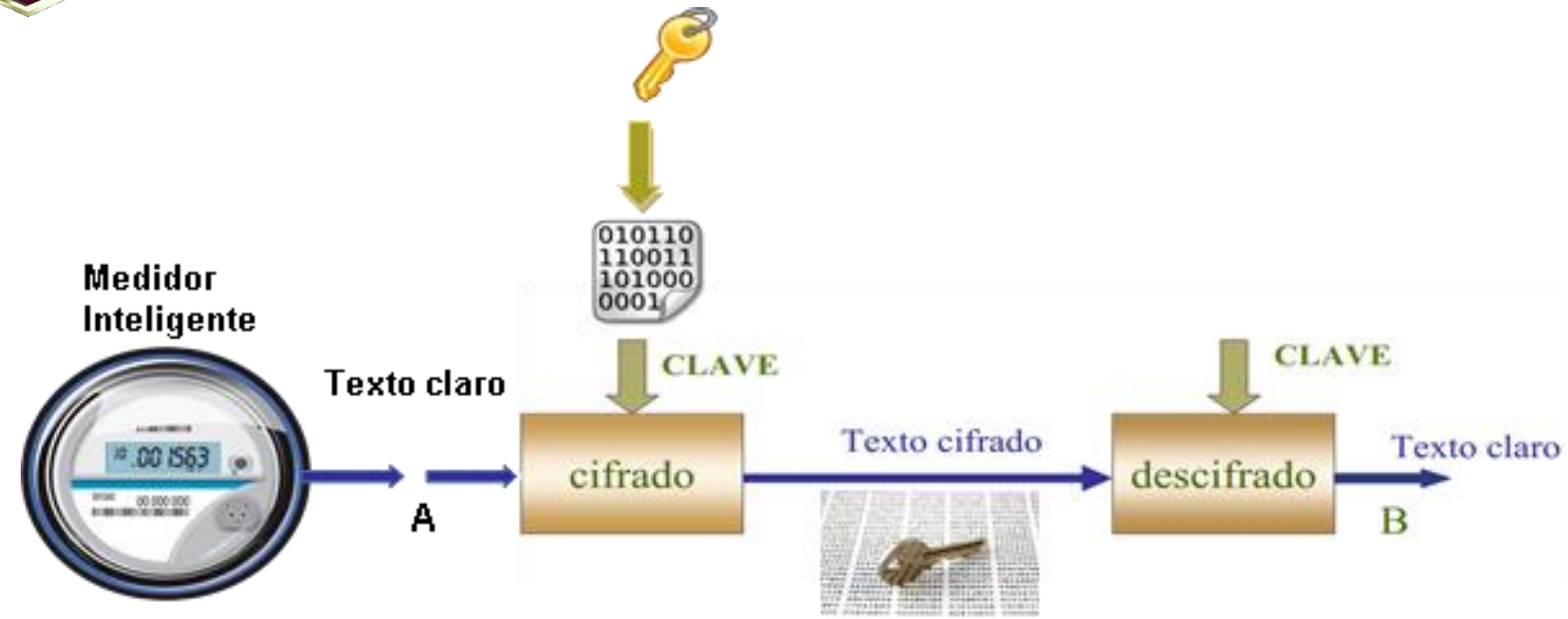
• Impacto

Vulnerabilidad



http://h30499.www3.hp.com/t5/image/serverpage/image-id/60193i94E791486D73C841/image-

Cifrado de datos



Mapeo logístico

$$f(x_t) = \mu x_t(1 - x_t)$$

$0 < \mu < 4, 0 < x_t < 1$

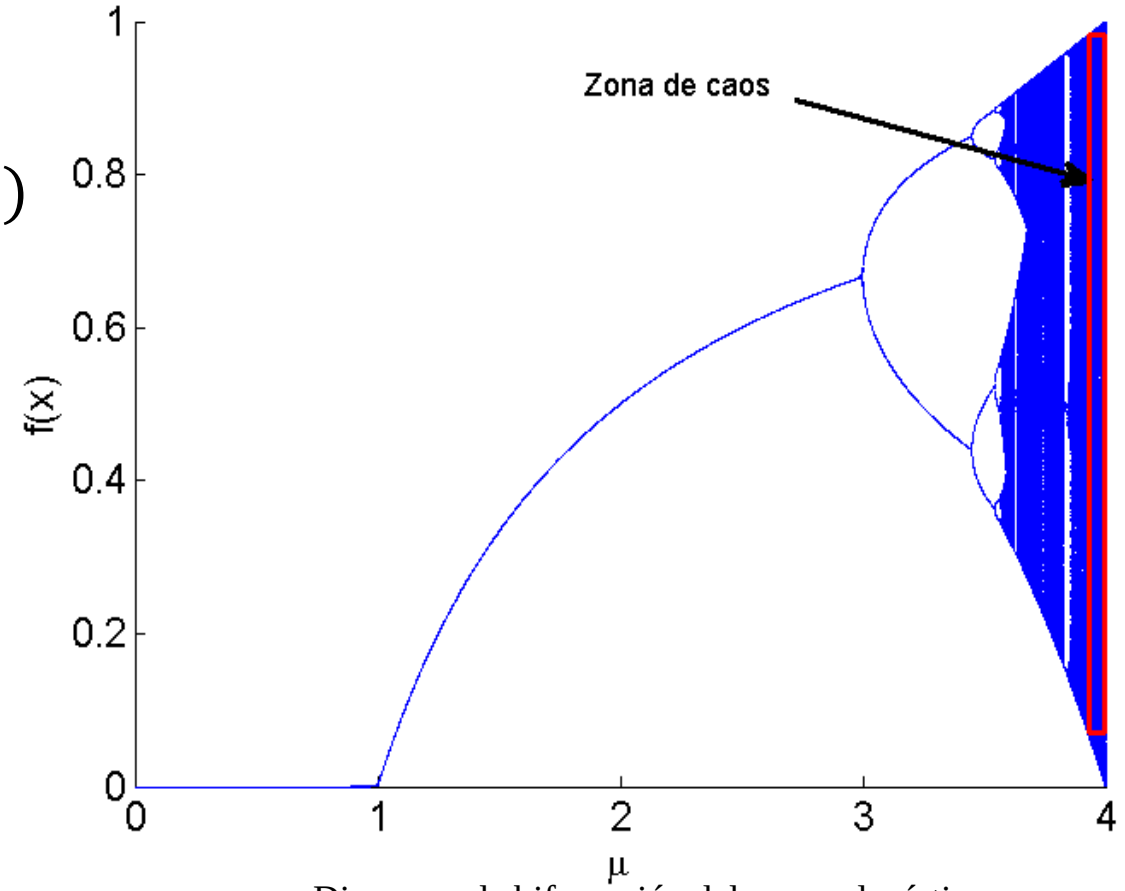


Diagrama de bifurcación del mapeo logístico.

Diagrama de Exponentes de Lyapunov

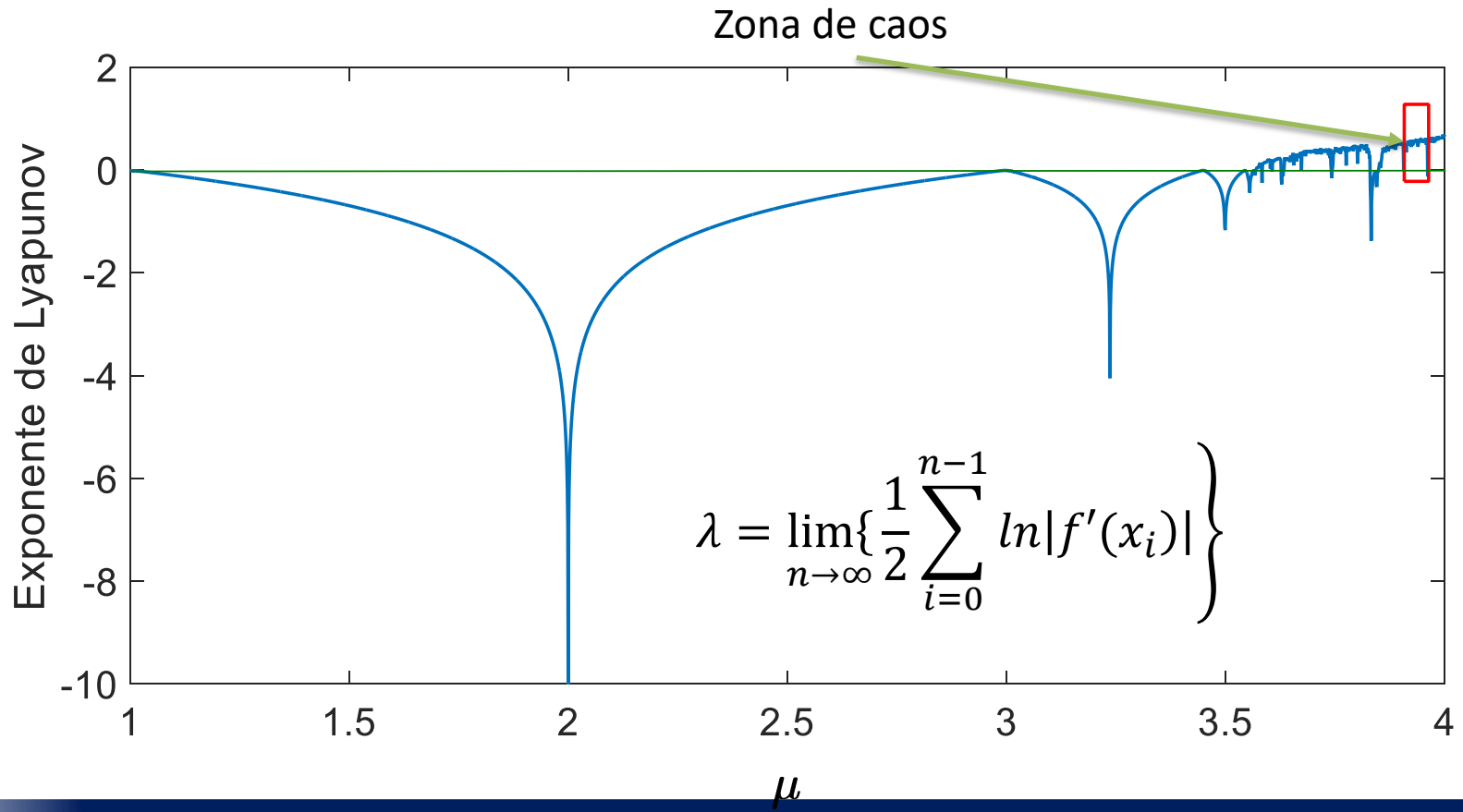


Diagrama de bloques

Ecuación Generadora1

$x_{t+1} = \mu x_t(1 - x_t)$

$\mu = 3.86$ y $x_t = 0.004$

Ecuación Generador2

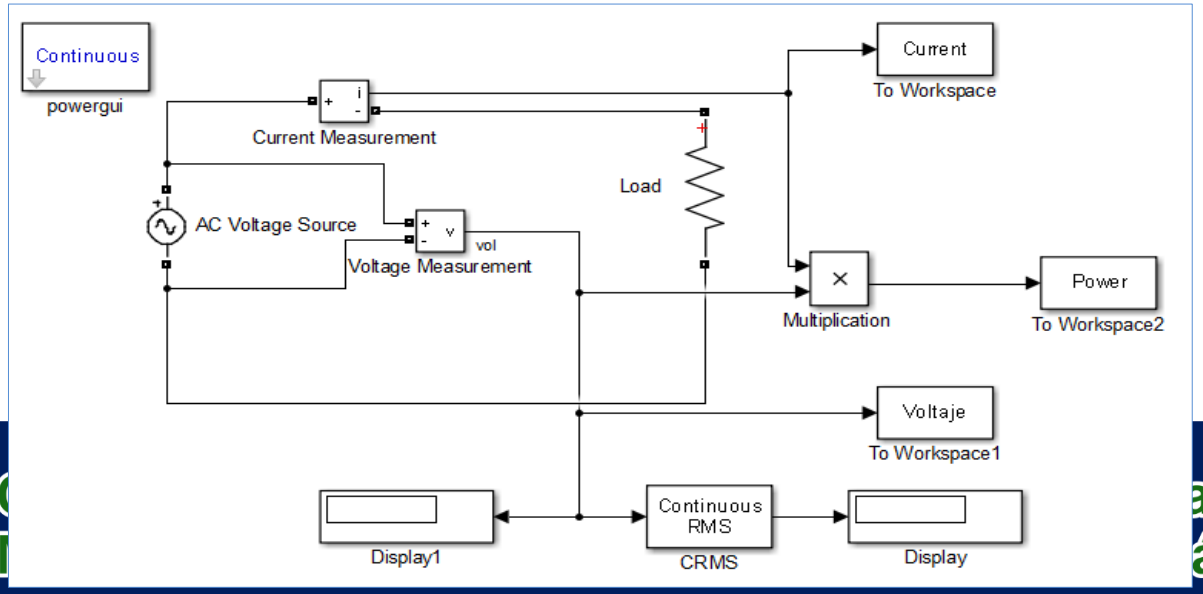
$x_{t+1} = \mu x_t(1 - x_t)$

$\mu = 3.89$ y $x_t = 0.019$

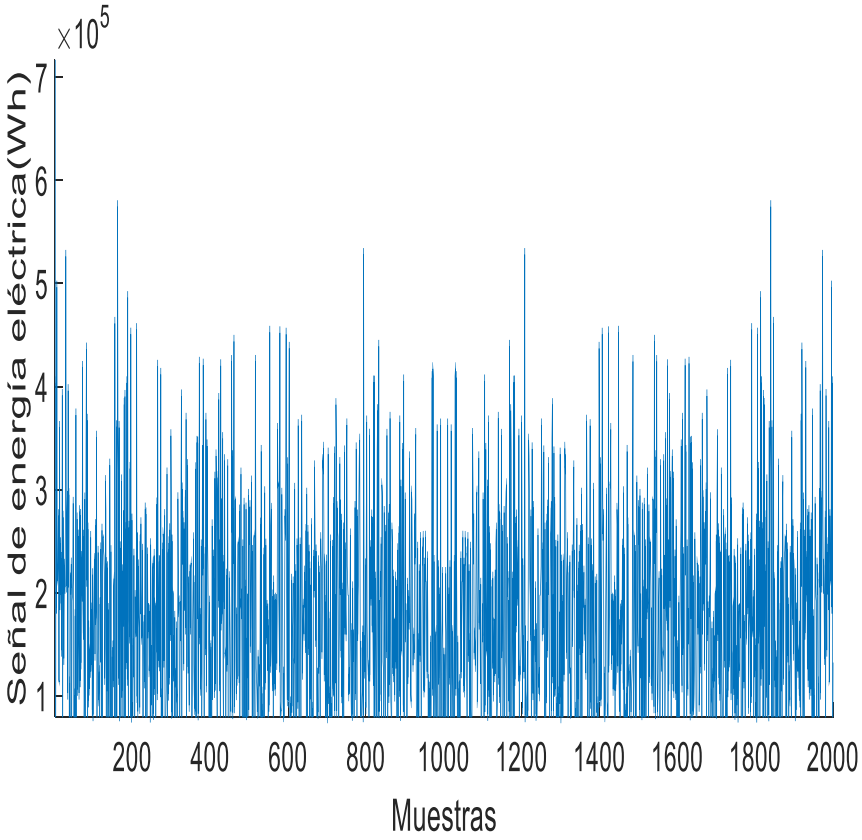
Generador Congruencial

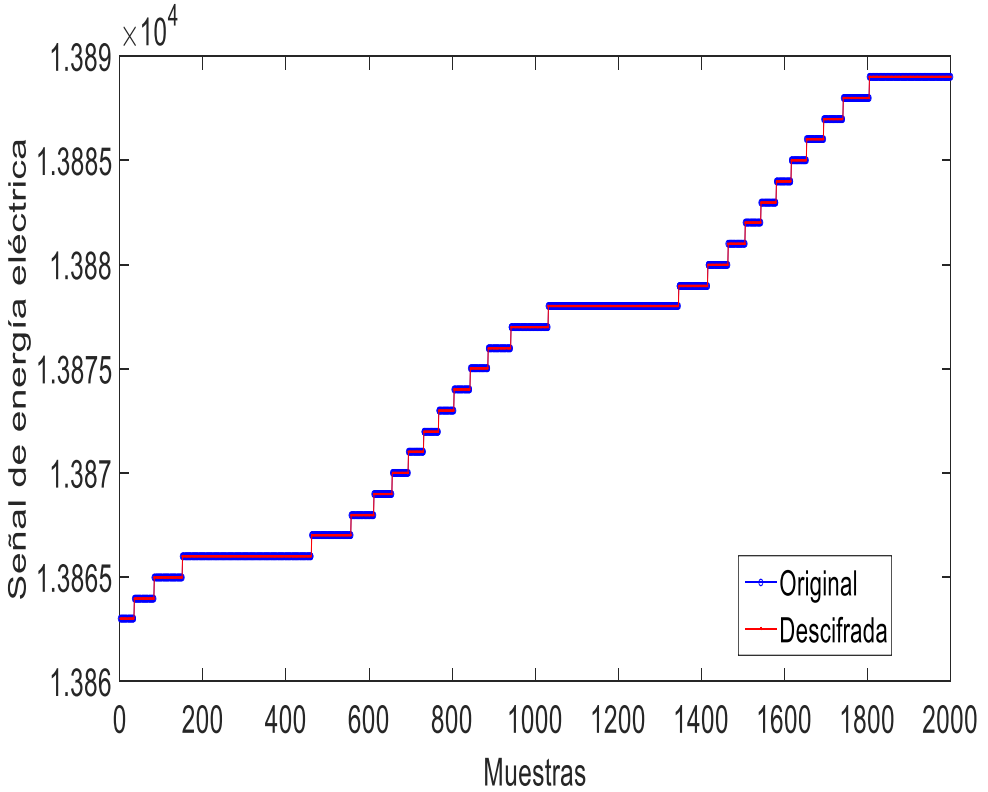
$X_{n+1} = (aX_n + c) \bmod m$

Criptograma



Señal cifrada y recuperada





Evaluación

Statistics	Function	Obtained	Expected
Correlation coefficient	$c = \frac{n\sum x_i y_i - \sum x_i \sum y_i}{\sqrt{n\sum x_i^2 - (\sum x_i)^2}\sqrt{n\sum y_i^2 - (\sum y_i)^2}}$	-0.0008	0
Entropy	$H = \sum_{i=1}^{2^2} P(S_i)\log_2 P(S_i)$	7.5788	**8**
Mean cuadratic error	$ECM = \frac{1}{n}\sum_{i=1}^{n} (\hat{Y}_i - Y_i)^2$	**0**	**0**

Estándares Federales de Procesamiento de Información (FIPS)

Test	Obtained P-value	Status
APPROXIMATE ENTROPY	0.809791	OK
BLOCK FREQUENCY	0.491789	OK
CUMULATIVE SUMS	0.412876	OK
CUMULATIVE SUMS	0.312923	OK
FFT	0.804313	OK
FRECUENCY	0.406539	OK
LINEAR COMPLEXITY	0.750305	OK
LONGEST RUNS OF ONES	0.504821	OK
NONOVERLAPPING TEMPLATE	0.5094025	OK
OVERLAPPING TEMPLATE	0.313653	OK
RANK	0.885113	OK
RUNS	0.436975	OK
NONPERIODIC TEMPLATES	0.5094025	OK
SERIAL	0.381633	OK
UNIVERSAL STATISTICAL	0.877240	OK

Conclusiones

Se propone criptograma basado en el caos.

La originalidad de nuestro generador de secuencias pseudoaleatorias se encuentra en la mezcla apropiada de comportamientos dinámicos mapas caótica y su perturbación, con el fin de mejorar su complejidad y el espacio de clave secreta, que corresponde a los parámetros de control sistemas caóticos.

Por lo tanto, las secuencias pseudo-aleatorios producidos a partir del generador de flujo de claves criptográficas tienen propiedades adecuadas en términos de calidad de la aleatoriedad, en los que su validez se demostró a través de las pruebas estadísticas del NIST.

Referencias bibliográficas

1. Mogollon, M. (2007). Cryptography and security services: mechanisms and applications. Hershey, PA: CyberTech, 51-97

2. Rajan, B. and Saumitr, P. (2006). A novel compression and encryption scheme using variable model arithmetic coding and coupled chaotic system. IEEE Transactions on circuits and system (4) I- 53

3. Jiménez, M., Flores, F. and González, G. (2015). System for Information Encryption Implementing Several Chaotic Orbits.Ingeniería, Investigación y Tecnología, 16(3), 335-343.

4. Radwan, A., AbdElHaleem, S. and Abd-El-Hafiz S. (2016). Symmetric encryption algorithms using chaotic and non-chaotic generators: A review. Journal of Advanced Research. 7(2), 193–208.

5. Ye, R. (2011). A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism. Optics Communications, 284(22), pp.5290-5298.

6. Martínez-González, R., Díaz-Méndez, J., Palacios-Luengas, L., López-Hernández, J. and Vázquez-Medina, R. (2015). A steganographic method using Bernoulli's chaotic maps. Computers & Electrical Engineering

7. National Institute of Standards and Technology. "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications" Revision 1, Special Publication 800-22. Revised January 2016.

ECORFAN®