Jornada de Investigación – 2018

Resumen del Proyecto de Investigación Nro 310

"Software Abierto para la Evaluación de Sistemas Criptológicos Integrados"

1. Introducción

Las comunicaciones del siglo XXI precisan de más y mejores algoritmos de cifrado, de autenticación y de integridad de la información que posibiliten la confidencialidad e integridad de las comunicaciones. El estudio y análisis de las propiedades matemáticas de dichos algoritmos permite evaluar sus propiedades criptológicas e identificar su nivel de robustez y seguridad.

2. Objetivo

Diseño y Desarrollo de un software abierto que permita la evaluación de las propiedades criptográficas y de seguridad de secuencias pseudoaleatorias procedentes de algoritmos Stream Ciphers, Block Ciphers o Generadores de Números Seudoaleatorios.

3. Etapas del proyecto

a) Búsqueda y análisis de técnicas criptoanalíticas.
b) Estudio de factibilidad.
c) Selección.
d) Elaboración de los módulos y pruebas.
e) Integración de los módulos en un marco general.

4. Formación de Recursos Humanos

El equipo de investigadores está formado por 11 docentes y 2 alumnos de EST y 1 docente de la Universidad Nacional de Tucumán. Se espera postular a los alumnos para la beca EVC – CIN 2019.

5. Publicaciones

Cipriano, M.; Malvacio, E.; Estevez, C.; Fernández, D.; García, E.; López, G.; Liporace, J.; Maiorano, A.; Vera Batista, F. "*Software Abierto para la Evaluación de Sistemas Criptológico*" XX Workshop de Investigadores en Ciencias de la Computación WICC 2018, ISBN 978-987-3619-27-4, Universidad Nacional del Nordeste. Corrientes. 2018.