# Estudio de Técnicas de Criptoanálisis

Castro Lechtaler, Antonio[1, 2]; Cipriano, Marcelo[1,3]; García, Edith[1],
Liporace, Julio[1]; Maiorano, Ariel[1]; Malvacio, Eduardo[1]; Tapia, Néstor[1];

[1]Laboratorio de Investigación en Técnicas Criptográficas y Seguridad Teleinformática.
Facultad de Ingeniería del Ejército -FIE. Universidad de la Defensa Nacional - UNDEF
[2] CISTIC/FCE - Universidad de Buenos Aires.
[3] Departamento de Ciencia y Tecnología, Universidad Nacional de Quilmes UNQ.

acastro@est.iue.edu.ar , marcelocipriano@est.iue.edu.ar,
{edithxgarcia; jcliporace; maiorano; edumalvacio; tapianestor87}@gmail.com

## RESUMEN

El proyecto de investigación propone estudiar las diferentes técnicas de Criptoanálisis, alcances y límites de las mismas, su marco de aplicación y su implementación mediante módulos interconectables mediante un framework.

Se orientarán las aplicaciones hacia los generadores de secuencias seudoaleatorias Stream Ciphers (*LFSR´s*[1], *NLFSR´s*[2], *CCG´s*[3] y *CA´s*[4]).

El desarrollo de herramientas de criptoanálisis permitirá la evaluación de algoritmos de cifrado para comprobar su robustez frente a los ataques que pudiera recibir, prestando sus funciones.

Entre las técnicas a abordar se encuentran las técnicas de Criptoanálisis Lineal [1], Diferencial [2-3], Algebraico, Guess-and-Determine [4] y Cube Attack [5], entre otras.

Este conjunto de herramientas posibilitará la realización de Análisis de Algoritmos de Cifrado, Generadores de Secuencias Seudoaleatorias, Primitivas Criptológicas, Protocolos de Seguridad, entre otros.

***Palabras Clave***

*Criptología, Técnicas de Criptoanálisis. Secuencias Seudoaleatorias.*

## CONTEXTO

En el marco de la carrera de grado de Ingeniería en Informática y el posgrado en Criptografía y Seguridad Teleinformática que se dictan en la Facultad de Ingeniería del Ejército (FIE) "Gral. Div. Manuel N. Savio", Universidad de la Defensa Nacional (UNDEF) se llevan adelante tareas de I+D+i por parte del Grupo de Investigación en Criptología y Seguridad Informática (GICSI).

GICSI depende del Laboratorio de Investigación en Técnicas Criptográficas y Seguridad Teleinformática (CriptoLab) perteneciente al Laboratorio Informática (InforLab). Y está conformado por docentes investigadores, profesionales técnicos y alumnos de dicha área.

## 1. INTRODUCCIÓN

En agosto de 2011, en una conferencia dada en el evento Techonomy[6] el CEO de Google Eric Schmidt sentenció que "la humanidad hasta el año 2003 había creado alrededor de 5 EB[5] de información" y luego "hoy en día, esa cantidad de información se genera cada 2 días y la tendencia va en aumento" [7-9].

[1] Linear Feedback Shift Registers: registros de desplazamiento realimentados linealmente.

[2] Non Linear Feedback Shift Registers: registros de desplazamiento realimentados no linealmente.

[3] Clock Controlled Generators: generadores controlados por reloj.

[4] Cellular Automata: autómata celular.

[5] ExaByte: $2^{60}$ bytes de información.

La transmisión y almacenamiento de información requiere tomar una serie de medidas de protección manteniendo su confidencialidad, autenticidad e integridad. La falta total o parcial de medidas de seguridad se convierte en una amenaza latente. Cabe preguntarse entonces por la calidad y características de algoritmos criptográficos que se encargan de su protección y resguardo.

En la etapa de diseño de una primitiva criptográfica sus autores tienen en cuenta los ataques que éste pueda sufrir, a partir de las técnicas criptoanalíticas conocidas y a ellas lo someten, demostrando así su resistencia. Esta práctica ha llevado a los modernos algoritmos de cifrado a sortear amenazas, cuidadosa y eficientemente desarrolladas para atacarlos. Cada algoritmo, cada primitiva, cada protocolo debe ser atacado mediante una técnica adecuada a su estructura.

Por ello es que hay diferentes y variados ataques criptográficos y no existe uno que sirva para todos los algoritmos[6]. A su vez tampoco existe un único algoritmo que satisfaga todas las necesidades y requerimientos. Tal es así que suele llamarse a concurso para satisfacer la demanda de nuevos mecanismos que deberán mostrar su robustez y resistencia. Por ejemplo:

- el llamado en 1997 del *NIST* para escoger un nuevo algoritmo como estándar de cifrado llamado *AES* [10].
- El concurso europeo e-*Stream* en 2004, organizado por el *E-CRYPT* [11] del cual superaron todas las pruebas y ataques, 7 algoritmos.
- el llamado a concurso del NIST para escoger un nuevo algoritmo como estándar SHA-3, finalizado en 2012. Aunque aún no se da de baja al SHA-2 por no demostrar, hasta el momento, debilidades.
- La vigente competencia CAESAR7 (Competition for Authenticated Encryption: Security, Applicability, and Robustness) la cual ha emitido un portfolio de los algoritmos que han llegado a la final del certamen en 2018, entre los que se encuentran home v1, ordering addendum v1.3v1.4 v1.41 (Jérémy Jean, Ivica Nikolić, Thomas Peyrin, Yannick Seurin). [12].

## 2. LÍNEAS DE INVESTIGACIÓN y DESARROLLO

Para llevar adelante este proyecto de investigación se siguen las siguientes líneas de investigación y desarrollo:

- Mediante el estudio de bibliografía actualizada y la asistencia a Cursos, Congresos y Workshops específicos, se profundizará en el estado del arte del Criptoanálisis y los nuevos ataques que se han desarrollado.
- Estudio, análisis y selección de los generadores de secuencias cifrantes.
- Relevamiento de los métodos criptoanalíticos que se analizarán.
- Estudio de técnicas criptográficas para la determinación del o los métodos de ataque adecuados a la estructura del algoritmo estudiado.
- Implementación de los métodos de criptoanálisis.

[6] El ataque por Fuerza Bruta puede aplicarse a cualquier algoritmo. El método consiste en probar todas las claves posibles, hasta encontrar la clave utilizada. Por las longitudes de las claves que se emplean actualmente, es posible que logre romper un criptosistema en varias veces la edad del universo. Es por ello que suele ser desaconsejable su implementación.

[7] CAESAR: Competition for Authenticated Encryption: Security, Applicability, and Robustness.

- Análisis de los resultados obtenidos.

## 3. RESULTADOS OBTENIDOS / ESPERADOS

Al realizar el estudio, análisis de las técnicas y herramientas de criptoanálisis, se persigue llevar adelante el diseño de aplicaciones criptográficas, evaluación y búsqueda de vulnerabilidades

El Criptoanálisis persigue:

- Obtener de la/s clave/s del cifrado.
- Encontrar patrones estadísticos en la salida del sistema.
- Desarrollar nuevas técnicas criptoanalíticas.
- Analizar el algoritmo de generación de la/s clave/s y estudiar su vulnerabilidad.

## 4. FORMACIÓN DE RECURSOS HUMANOS

Los docentes investigadores del proyecto dictan las asignaturas Criptografía y Seguridad Teleinformática, Matemática Discreta y Paradigmas de Programación I, II. Desde esas cátedras se invita a los alumnos a participar. Es por ello que 3 de ellos han demostrado su interés y se han sumado en calidad de colaboradores. En particular, el alumno Leiras, Facundo ha presentado su postulación en 2018 para la beca "Estímulo a las Vocaciones Científicas" (EVC) otorgadas por el Consejo Interuniversitario Nacional (CIN) por encuadrarse en las condiciones requeridas [13]. La misma le ha sido otorgada, iniciando en breve sus actividades respectivas.

Se desea destacar que el incremento del Know-How que tendrá el grupo de investigadores a lo largo de la vida del proyecto será una importante y económica Formación de Recursos Humanos en beneficio de sus integrantes y de la institución en la cual desarrollan sus actividades científico-docentes.

Por último y atendiendo a la responsabilidad ética y social que compete a la actividad científica y tecnológica, el Grupo Integrante de este Proyecto de Investigación, ya sea durante su ejecución o por la aplicación de los resultados obtenidos, desea expresar su compromiso a no realizar cualquier actividad personal o colectiva que pudiera afectar los derechos humanos, o ser causa de un eventual daño al medio ambiente, a los animales y/o a las generaciones futuras.

## 5. BIBLIOGRAFÍA


[1] Muller F., Peyrin T. "Linear Cryptanalysis of the TSC Family of Stream Ciphers". Roy B. (eds.) Advances in Cryptology - ASIACRYPT 2007. Lecture Notes in Computer Science, vol. 3788. Springer, Berlin, Heidelberg. 2005.

[2] Ding C.; "The differential cryptanalysis and design of natural stream ciphers". In: Anderson R. (eds.) Fast Software Encryption. FSE 1993. Lecture Notes in Computer Science, vol. 809. Springer Berlin, Heidelberg.

[3] Wu H., Preneel B. "Differential Cryptanalysis of the Stream Ciphers Py, Py6 and Pypy". Naor M. (eds.) Advances in Cryptology. EUROCRYPT 2007. Lecture Notes in Computer Science, vol. 4515. Springer Berlin, Heidelberg. 2007.

[4] Pasalic, E.; "On Guess and Determine Cryptanalysis of LFSR-Based Stream Ciphers"; IEEE Transactions on Information Theory. Vol. 55 Ed.7º, 2009.

[5] Dinur I., Shamir A. "Cube Attacks on Tweakable Black Box Polynomials". Advances in Cryptology - EUROCRYPT 2009. Lecture Notes in Computer Science, vol 5479. Springer, Berlin, Heidelberg. 2009.

[6] https://techonomy.com/ consultada el 27/2/19.

[7] https://readwrite.com/2010/08/04/goole_ceo_schmidt_people_arent_ready for_the_tech/. Consultada el 27/2/19.

[8] https://techcrunch.com/2010/08/04/schmidt-data/. Consultada el 27/2/19.

[9] Hilbert,m; López, p, “The World’s Technological Capacity to Store, Communicate, and Compute Information”. Science. 01 Apr 2011. Vol. 332, Issue 6025, pp. 60-65.
DOI: 10.1126/science.1200970.
[10] Daemen, J.; Rijmen, V.; “The Design of Rijndael: AES - The Advanced Encryption Standard”. Springer. New York. 2002.
[11] http://www.ecrypt.eu.org/stream/ Consultada el 10-3-18.
[12] https://competitions.cr.yp.to/caesar.html. Consultada el 10-3-18.
[13]http://evc.cin.edu.ar/informacion consultada el 23/2/2018.