Algoritmo de Cifrado para Sistemas Móviles

Castro Lechtaler, Antonio[1, 2]; Cipriano, Marcelo[1]; 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.
Escuela Superior Técnica, Facultad de Ingeniería. Instituto Universitario del Ejército.
[2] CISTIC/FCE - Universidad de Buenos Aires.

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

RESUMEN.

Este proyecto de investigación persigue elaborar el diseño y desarrollo de un ***Algoritmo de Cifrado para Sistemas Móviles*** que por sus propiedades de velocidad, compactibili- dad y robustez; pueda ser implementado en equipos de comunicaciones que funcionan so- bre Sistemas Móviles.

Se esperan obtener resultados teóricos, prácticos y la realización de un desarrollo experimental.

Los modernos algoritmos criptológicos responden a principios y filosofías diferentes a las que se llevaban a cabo antaño. Uno de los principios de diseño es que el algoritmo debe demostrar su resistencia a los ataques conocidos. Para ello deben contemplarse instancias o funciones, desde la mismísima etapa de diseño que demuestren su capacidad de resistir tal o cual ataque. Así demostrar la robustez y resistencia del algoritmo frente a un conjunto conocido de ataques.

Por ello los diseñadores deben estar en conocimiento y mantenerse actualizados en cuanto a los avances que se efectúen en Criptoanálisis.

Palabras Clave:

Criptografía. Criptosistemas de Clave Privada, Stream Ciphers. Sistemas Móviles

CONTEXTO.

El *Grupo de Investigación en Criptología y Seguridad Informática (GICSI)* pertenece al *Laboratorio de Investigación en Técnicas Criptográficas y Seguridad Teleinformática (CriptoLab)* pertenece a los *Laboratorios de Informática (InforLabs)* de la *Escuela Superior Técnica "Gral. Div. Manuel N. Savio" (EST)*, dependiente de la *Facultad del Ejército, Universidad Nacional de la Defensa (UNDEF)*. El mismo se enmarca en el área de la carrera de grado de *Ingeniería en Informática* y del posgrado en *Criptografía y Seguridad Teleinformática* que se dictan en esta institución.

1. INTRODUCCIÓN.

Se entiende aquí por Sistemas Móviles (SM) a aquellos Sistemas de permiten la realización de comunicaciones en posiciones fijas, como también en movimiento: como equipos de tipo VHF[1] y telefonía móvil que requieren de enlaces confidenciales y deben recurrir a la criptografía para obtener tales servicios. Sin embargo no todo sistema de cifrado que ofrezca seguridad puede ser montado sobre tales plataformas.

Estos dispositivos no cuentan con los mismos recursos de hardware y software que otros que están fijos o no tiene sus limitaciones.

El uso eficiente de los recursos de los que el Sistema Móvil disponga será preponderante. Es por ello que si un criptosistema puede demandar una cantidad de recursos mayor a lo disponible (espacio de carga útil, tiempo de

[1] Very High Frequency: rango de frecuencias de 30 MHz a 300 MHz. Empleado por sistemas satelitales, televisión, radiodifusoras de FM, bandas aéreas y marítimas, entre otras.

ejecución o retardos en la implementación, energía consumida, memoria requerida, etc.) puede que atente contra el sistema que pretende proteger.

Tal es el caso de diversos dispositivos cuyas misiones dependen del uso eficiente de sus recursos. En particular los vehículos aéreos no tripulados del Proyecto LIPAM del Ejército Argentino, los cascos de RAIOM[2] proyecto que lleva adelante CITEDEF[3] (en ambos proyectos se realizaron aportes desde el Cripto-Lab).[4]

También se pueden mencionar otros sistemas y vehículos, como el PANHARD francés que el Ejército y otras fuerzas poseen y que le fue encomendado a la EST para su modernización.

Es por ello que el diseño de un criptosistema compacto, veloz y austero en el consumo de los recursos se hace indispensable para dar respuesta a la seguridad de los canales de datos, comando y control o cualquier otro que se precise proteger y dotar de confidencialidad.

Otros temas a investigar son la existencia o no de claves débiles que generan ciclos cortos o debilidades en el cifrado. Y demostrar ser inmune a los ataques criptoanalíticos conocidos, como el Criptoanálisis Diferencial, Lineal, Algebraico, Cube Attack, entre otros[1-5].

2. LÍNEAS DE INVESTIGACIÓN, DESARROLLO E INNOVACIÓN.

Hemos dividido el proyecto en 4 etapas de investigación y desarrollo:

a) Estudio y análisis de algoritmos que satisfacen los requerimientos y condiciones de entorno del proyecto.
b) Personalización, diseño y desarrollo del algoritmo:
- Estudio de sus vulnerabilidades y ataques conocidos.
- Implementación y pruebas del algoritmo.

c) Determinación de las propiedades criptológicas:
- Estudio de las propiedades.
- Experiencias de laboratorio.

d) Ejecución de los test y demás pruebas de robustez criptológica.
- Diseño y programación de los test.
- Diseño e implementación de los ataques.
- Análisis de los resultados obtenidos.
- Redacción del informe final
- Puesta a punto del algoritmo a entregar

3. RESULTADOS Y OBJETIVOS.

Garantizar la seguridad de las comunicaciones mediante el diseño de un esquema de cifrado y descifrado bajo la modalidad Stream Cipher o Cifrado en Cadena, para que por medio de una Clave Privada pueda dotar de confidencialidad a uno o varios canales de comunicaciones de un Sistema Móvil.

El mismo deberá, ante todo, demostrar su robustez por medio de sus propiedades matemáticas pertinentes. A su vez, la Secuencia Cifrante (Key Bit Stream)[6] que de él se obtenga, deberá satisfacer todos los requisitos aceptados por la comunidad científica que deben tener las Secuencias Seudo-Aleatorias: Test de Golomb, de NIST, Die Hard y demás, es- tudio de la longitud de recursión, complejidad lineal y período.

Ahorrar recursos económicos al realizar un desarrollo propio y nacional, frente a los costos en equipos y algoritmos comprados en el exterior y en moneda extranjera.

El incremento del Know-How que tendrá el equipo a lo largo de la vida del proyecto será una económica Formación de Recursos Humanos en beneficio de los alumnos del equipo.

4. FORMACIÓN DE RECURSOS HUMANOS.

Los docentes investigadores de este proyecto se encuentran dictando las asignaturas *Matemática Discreta, Paradigmas de Programación I, II* y *Criptografía y Seguridad Telein-*

[2] RAIOM: Realidad Aumentada para la Identificación de Objetivos Militares.
[3] CITEDEF: El Instituto de Investigaciones Científicas y Técnicas para la Defensa; ex Instituto de Investigaciones Científicas y Técnicas de las Fuerzas Armadas (CITEFA)
[4] El Laboratorio de Criptografía y Seguridad Teleinformática realizó algunos aportes a ambos proyectos.

formática. Desde allí se invita a los alumnos a participar en los proyectos de investigación que se llevan adelante. Es por ello que los alumnos *LEIRAS*, *F. MIGLIARDI A., MONTANARO, L. ROMERO, E. y UVIEDO, G.* han demostrado su interés y se han sumado en calidad de colaboradores.

El *Cap. Pérez, P.* integra el equipo de investigación desde el año 2015 y se espera que este año realice su Proyecto Final de Carrera en un tema afín con este proyecto de investigación.

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 obteni- dos, desea expresar su compromiso a no reali- zar cualquier actividad personal o colectiva que pudiera afectar los derechos humanos, o ser causa de un eventual daño al medio am- biente, a los animales y/o a las generaciones futuras.

5. BIBLIOGRAFÍA

[1] 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.

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

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

[4] 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

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

[6] Biryukov A., Shamir A. (2000) Cryptanalytic Time/Memory/Data Tradeoffs for Stream Ciphers. In: Okamoto T. (eds) Ad- vances in Cryptology — ASIACRYPT 2000. ASIACRYPT 2000. Lecture Notes in Computer Science, vol 1976. Springer, Berlin, Heidelberg.