Herramientas para la Evaluación de Algoritmos Criptográficos.

Liporace, Julio[1]; Cipriano, Marcelo[1,3] ; Malvacio, Eduardo; Estevez[2], Carlos; Fernández, Darío[1], García, Edith[1], López, Gabriel; Maiorano, Ariel[1] Ortega, Hugo[4]; Vera Batista, Fernando[1]

[1]Laboratorio de Investigación en Técnicas Criptográficas y Seguridad Teleinformática. Facultad de Ingeniería del Ejército (FIE), Universidad de la Defensa Nacional - UNDEF
[2] Instituto de Investigaciones Científicos y Técnicas para la Defensa – CITEDEF.-)
[3] Departamento de Ciencia y Tecnología, Universidad Nacional de Quilmes UNQ.
[4] Departamento Ciencias de la Computación. Facultad de Ciencias Exactas y Tecnología. Universidad Nacional de Tucumán

{marcelocipriano; dfernandez; verabatista}@est.iue.edu.ar
{edithxgarcia; jcliporace; maiorano; edumalvacio}@gmail.com
{hortega}@herrera.unt.edu.ar

RESUMEN

El aumento en el empleo de Internet en general y en particular de las tecnologías de Voz sobre IP, Teleconferencias, VideoStreaming, sistemas móviles y demás, han mostrado la necesidad de protegerlos mediante mecanismos criptográficos [1-2].

A los ya conocidos estudios de las propiedades matemáticas de los Generadores de Secuencias Pseudorandom generadas por Stream Ciphers [3] (algoritmos que involucran Linear Feedback Shift Registers [4], Non Linear Feedback Shift Registers [5]), Clock Controlled Generators y Autómatas Celulares, las Substitution Boxes creadas para los Block Ciphers [6] y los Generadores de Números Pseudoaleatorios que permiten evaluar propiedades criptológicas [7-8], se le debe agregar la posibilidad de la existencia de "puertas traseras" o "back-doors" presentados en recientes trabajos han sorprendido a la comunidad criptológica [9-10].

Es por ello que se persigue la creación de herramientas que permitan automatizar tales análisis y la realización de pruebas, para llevar adelante el estudio de manera veloz y eficiente. Al ser sometidos a este escrutinio en profundidad, los algoritmos podrán ser calificados de acuerdo a las propiedades que manifiesten. De esta forma, el usuario podrá decidir acerca de su uso, de acuerdo al nivel de seguridad que se precise y el que el algoritmo finalmente ofrezca.

Muchas propiedades criptológicas quedan ocultas detrás de las líneas de programación o en la complejidad matemática que compete a estos mecanismos [11]. Suele ocurrir que las explicaciones técnicas más profundas no se abordan en detalle o son parcialmente expuestas [12]. Los investigadores deben profundizar en cada algoritmo y mediante su estudio, deducir sus propiedades.

Palabras Clave

Criptología, Criptoanálisis. Stream Ciphers.

CONTEXTO

"Herramientas para la Evaluación de Algoritmos Criptográficos" (HEAC), es un proyecto de investigación y desarrollo que se presenta dando cumplimiento a la Resolución Rectoral 154/18 en el marco del Programa de Acreditación y Financiamiento de Proyectos UNDEFI, perteneciente a la Universidad de la Defensa Nacional (UNDEF). Luego de un

período de evaluación, fue seleccionado con el Nro. 340 y recibe financiamiento de la Universidad.
La investigación se lleva adelante en el contexto de la carrera de grado de Ingeniería en Informática y el posgrado en Criptografía y Seguridad Teleinformática. Ambos se dictan en la Facultad de Ingeniería del Ejército "Gral. Div. Manuel N. Savio" (FIE), perteneciente a la Universidad de la Defensa Nacional (UNDEF). Allí se llevan adelante tareas de I+D+i por parte del Grupo de Investigación en Criptología y Seguridad Informática (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 los últimos años los métodos para el diseño de algoritmos seguros han tenido un gran avance e impulso a nivel mundial. Basta recordar, entre otros:

- Los llamados en 1997 del NIST para escoger un nuevo algoritmo como estándar de cifrado llamado AES.
- El inicio en el año 2000 del proyecto del gobierno japonés llamado CRYPTREC, creado para evaluar y recomendar técnicas criptográficas para uso gubernamental e industrial. La primera "Lista de Algoritmos Recomendados" fue publicada en 2003, con una revisión en el año 2013.
- El concurso europeo e-Stream organizado por el European Network of Excellence in Cryptology (E-CRYPT) que se llevó adelante entre el 2004 y 2008 con el propósito "Identificar nuevos algoritmos de cifrado en cadena". De él surgieron 7 algoritmos: 4 pertenecientes al Portfolio correspondiente a software y 3 pertenecientes al Portfolio correspondiente a hardware.
- SHA-3 (Secure Hash Algorithm) el nuevo estándar hash, a partir de conocer a través de NIST en 2012 el vencedor del certamen (KeccaK), aunque aún puede seguir usándose SHA-2.
- PHC (Password Hashing Competition) que corrió entre 2013 al 2015, recomendando finalmente al algoritmo ARGON2 para llevar adelante el hash de claves.
- Y la aún vigente competencia CAESAR (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).

A su vez, el reconocimiento a través de normas de muchos algoritmos criptográficos fue en aumento, como ser las ISO (International Organization for Standardization). Esta es una organización internacional no gubernamental, formada por organismos de estandarización de 163 países miembros y el IEC (International Electrotechnical Commission), es una organización de normalización que actúa sobre temas eléctricos, electrónicos y tecnologías asociadas. Está formada por los organismos nacionales de normalización, al igual que la International Organization for Standardization, en las áreas mencionadas de los 83 países miembros. Muchas normas se desarrollan en común con

ISO, por ello se las llama normas ISO/IEC):

- ISO/IEC18033-3:2005 llamada "Information Technology. Security Techniques. Encryption Algorithms. Part 3: Block Ciphers" Algoritmos de Cifrado en Bloques (Block Ciphers) de 64 bits: TDEA, MISTY1, CAST-128, HIGHT. De 128 bits: AES, Camellia, SEED.
- ISO/IEC 29192-3:2012 "Information Technology. Security Techniques. Lightweight Cryptography. Part 3: Stream ciphers". Algoritmos de Cifrado en Cadena (Stream Ciphers) Enocoro y Trivium.
- ISO/IEC 18033-4:2011 "Information Technology. Security Techniques. Encryption Algorithms. Part 4: Stream Ciphers" presenta 5 algoritmos de Cifrado de Flujo: Decim-v2., KCipher-2 (K2), MUGI, Rabbit, SNOW 2.0.

Este renacimiento mundial por la búsqueda de nuevos algoritmos resulta bienvenido. Pero por sí sólo resulta insuficiente a la hora de establecer parámetros criptográficos seguros.

Cada algoritmo, cada primitiva, cada protocolo debe ser atacado mediante una técnica adecuada a su estructura. Es por ello que en la actualidad no existe una única modalidad general de criptoanálisis. Los autores ya enfocan el diseño de algoritmos de cifrado para que resulten indemnes ante los ataques conocidos. Así el impacto del Criptoanálisis resulta de peso puesto que los algoritmos criptológicos, los protocolos y también los tamaños de las claves entre otros, son seleccionados basándose en él.

Aunque el objetivo fundamental del criptoanálisis es hallar las vulnerabilidades en uno o varios aspectos de la seguridad de los algoritmos criptológicos, implícita o explícitamente, no se extingue allí su alcance. Sino que también resulta ser la herramienta fundamental a la hora de establecer la fortaleza de los mismos. No debería adoptarse ningún algoritmo si no se prueba que éste ha sido sometido a distintas técnicas de criptoanálisis y ha resistido eficientemente a las mismas

2. LÍNEAS DE INVESTIGACIÓN y DESARROLLO

Para llevar adelante la investigación y el desarrollo del proyecto, se proponen las siguientes líneas de acción:

- Investigación bibliográfica acerca de las técnicas de ataque criptoanalíticas conocidas.
- Seguimiento y/o asistencia a los congresos y workshops de relevancia y referencia del tema abordado, tanto nacionales como internacionales, acerca del progreso del criptoanálisis de los algoritmos estudiados., como así también la presentación de nuevas herramientas para la búsqueda de vulnerabilidades.
- Determinación de la metodología que se implementará a lo largo del desarrollo del proyecto.
- Elaboración de módulos para las pruebas algorítmicas.
- Aplicación de las herramientas a primitivas criptográficas en particular.

3. RESULTADOS OBTENIDOS / ESPERADOS

Es por ello que el proyecto persigue la creación de herramientas informáticas que permitan automatizar algoritmos de prueba y análisis que posibiliten la detección de debilidades y/o vulnerabilidades criptoanalíticas que pudieran ser explotadas por un atacante, mediante técnicas de criptoanálisis. Y todo ello

llevado delante de forma veloz y eficiente.
Se someterá a un análisis profundo a los algoritmos en cuestión, para así poder ser calificados de acuerdo a las propiedades que manifiesten. De esta forma, el usuario podrá decidir acerca de su uso, de acuerdo al nivel de seguridad que se precise y la que el algoritmo finalmente ofrezca.
Muchas de las propiedades criptológicas quedan solapadas u ocultas detrás de las capas del lenguaje de programación o el diseño informático del mismo, como así también, en la maraña matemática que encierran estos mecanismos. Suele ocurrir que las explicaciones técnicas más profundas no son abordadas en detalle y son parcialmente expuestas. Los investigadores deben profundizar en cada algoritmo y mediante su estudio, deducir sus propiedades.
Asimismo al considerar además el ciclo de vida de cada algoritmo, se podrá observar el avance o progreso de los ataques a los que se lo ha sometido. Muchas veces esos ataques conllevan un éxito y se van observando vulnerabilidades. La mayoría de ellas son resueltas con el advenimiento de versiones mejoradas de los mismos. Esta permanente evolución debe ir acompañada de la actualización de pruebas y demás procesos que permitan evaluar su seguridad.
Los objetivos particulares que presenta el proyecto son:

- Estudio y análisis de técnicas criptoanalíticas.
- Diseño y desarrollo de herramientas de evaluación, ataque o quiebre de aplicaciones criptográficas.
- Pruebas y testeo de las herramientas desarrolladas sobre algoritmos específicos.

4. FORMACIÓN DE RECURSOS HUMANOS

Este proyecto se lleva se lleva adelante en conjunto con la Universidad Nacional de Tucumán, mediante la colaboración de uno de sus docentes investigadores, tal como figura en el parágrafo correspondiente a los autores.
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] Wu, H. “Related-Cipher Attacks” International Conference on Information and Communication Security. (ICICS 2002), Lecture Notes in Computer Science 2513, R. Deng, S. Qing, F. Bao and J. Zhou (Eds.), pp. 447-455, Springer-Verlag, (2002).

[2] Souradyuti, P.; Preneel, B. “On the (In)security of Stream Cyphers Based on Arrays and Modular Addition”, Advances in Cryptology - proceedings of ASIACRYPT 2006, Lecture Notes in Computer Science 4284, pp. 69-83, Springer-Verlag, (2006).
[3] Fischer, W.; Gammel, B.; Kniffler, O.; Velton, J. “Differential Power Analysis of Stream Ciphers,” Topics in Cryptology-CT-RSA 2007, Springer-Verlag, LNCS, Vol. 4377, pp. 257–270. (2007).
[4] Masoodi, F.; Alam, S; Bokhari, M. “An Analysis of Linear Feedback Shift Registers in Stream Ciphers”. International Journal of Computer Applications 46, pp. 46-49, May 2012. Published by Foundation of Computer Science, New York, USA. (2012).
[5] Biryukov, A.; Shamir, A. “Cryptanalytic time/memory/data tradeoffs for stream ciphers”. In T. Okamoto, editor, ASIACRYPT, volume 1976 of Lecture Notes in Computer Science, Pp 1–13. Springer. (2000).
[6] Biryukov, A. “Block ciphers and stream ciphers: The state of the art”.IACR Cryptology ePrintArchive, Pp: 1–22. (2004).
[7]Albrecht, M.; Cid, C. “Algebraic techniques in differential cryptanalysis”. InFastSoftware Encryption, Pp 193–208. Springer-Verlag, (2009).
[8] Carlet, C.; Feng, K. “An infinite class of balanced functions with optimal algebraicimmunity, good immunity to fast algebraic attacks and good nonlinearity”. In14th InternationalConference on the Theory and Application of Cryptology and Information Security, Advancesin Cryptology (ASIA CRYPT 2008), volume 5350 of Lecture Notes in Computer Science, Pp 425–440. Springer-Verlag, (2008).
[9] Calderini M., Sala M.:”Elementary abelian regular subgroups as hidden sums for cryptographic trapdoors”. arXiv:1702.00581 (2017).
[10] Brunetta C., Calderini M., Sala M.: “Algorithms and bounds for hidden sums in cryptographic trapdoors”. arXiv:1702. 08384 (2017).
[11] Civino, R., Blondeau, C. & Sala, M. “Designs, Codes and Cryptography”. Pp 225-247. https://doi.org/10.1007/ s10623-018-0516-z. (2019)
[12] Aiston J. “Ring Theoretic Key Exchange for Homomorphic Encryption”. In: Arai K., Bhatia R. (eds) Advances in Information and Communication. FICC 2019. Lecture Notes in Networks and Systems, vol 70. Springer, Cham. Springer Nature Switzerland AG. (2019).
[13]http://evc.cin.edu.ar/informacion, página consultada el 23/2/2019.