Escuela Superior Técnica
Desde 1930
INSTITUTO UNIVERSITARIO.

CRIPTOLAB

Laboratorio de Criptografía y Seguridad Teleinformática

C-RAIOM

Criptología
aplicada a la
Realidad
Aumentada para la
Identificación de
Objetivos
Militares

14 de mayo de 2014

Seminario Regional de Ciberdefensa

CONTEXTO DEL TRABAJO A PRESENTAR

La Escuela Superior Técnica Gral. Manuel N Savio, Facultad de Ingeniería del Instituto Universitario del Ejército entre sus Carreras de Postgrado tiene la Carrera de Especialización en Criptografía y Seguridad Teleinformática de duración 1 año.

La misma esta acreditada por la Comisión Nacional de Evaluación y Acreditación Universitaria - CONEAU por 6 años (periodo máximo de acreditación que otorga dicha Agencia).

Además, la Especialización ha sido categorizada como "B" - Muy Buena.

La Carrera tiene Grupos de Investigación que están trabajando en el Laboratorio de Criptografía y Seguridad Teleinformática donde se desarrolla este proyecto.

CONTEXTO DEL TRABAJO A PRESENTAR

El Instituto de Investigaciones Científicas y Técnicas para la Defensa – CITEDEF está desarrollando el Proyecto RAION- Realidad Aumentada para la Identificación de Objetivos Militares

Dicho Proyecto necesitaba encriptar el enlace entre el dispositivo que captura las imágenes y el Centro de Comando y Control que las recibía para fines operacionales.

El Cripto Lab con acuerdo con dicho Programa tomó a su cargo el desarrollo del sistema de cifrado que podría utilizarse para tal fin.

De este acuerdo comenzó el desarrollo que hoy presentamos

CONTEXTO DEL TRABAJO A PRESENTAR

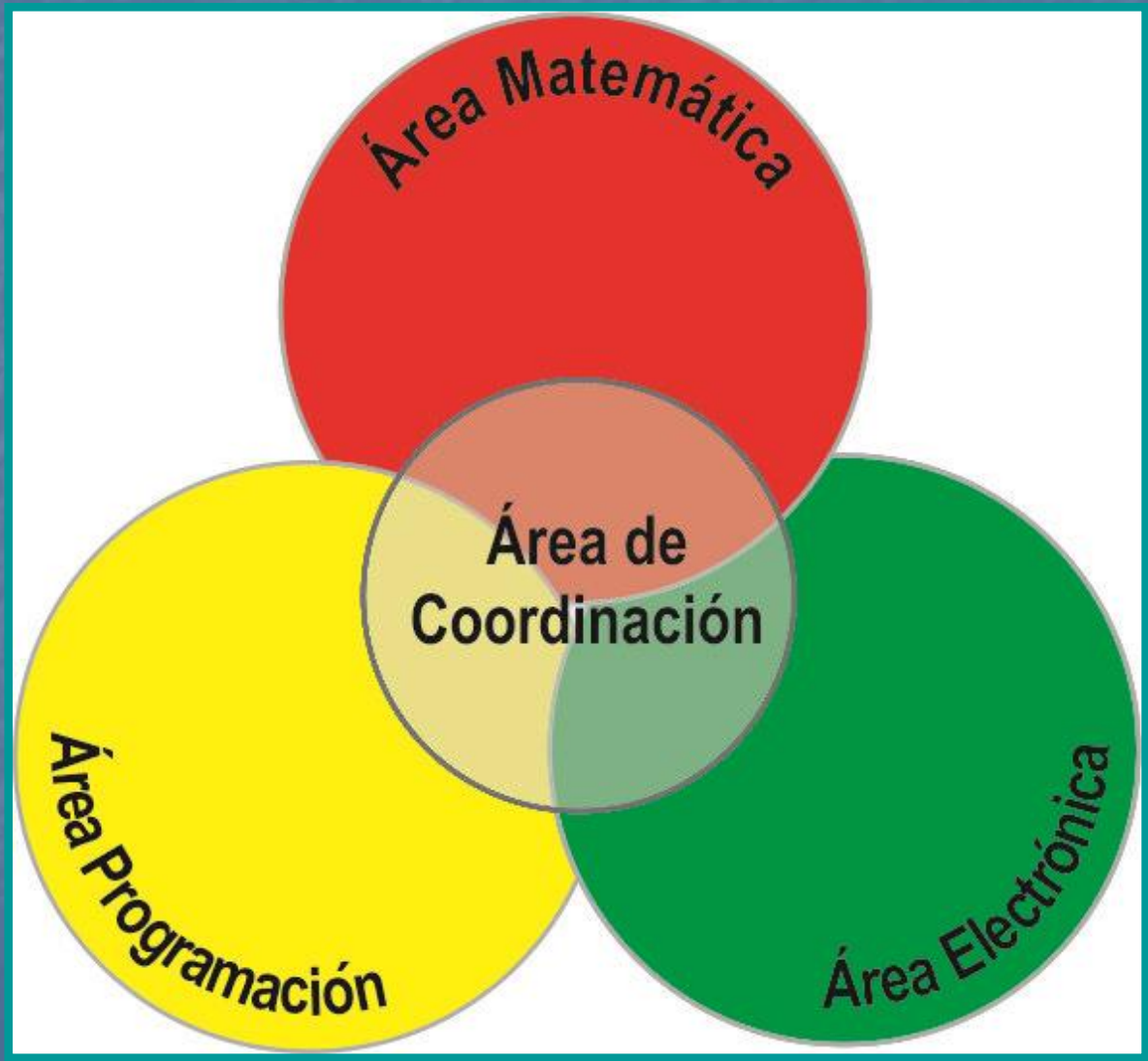
En el marco del Programa de Investigación y Desarrollo para la Defensa (PIDDEF) 2012-2014, elaborado por la Subsecretaría de Investigación Científica y Desarrollo Tecnológico del Ministerio de Defensa, la Gerencia de Informática del Instituto de Investigaciones Científicas y Técnicas para la Defensa (CITEDEF), se encuentra desarrollando tecnologías aplicadas al campo de la Realidad Aumentada (RA).

La utilización de RA permitirá a las fuerzas militares contar con información precisa del entorno donde se está ejecutando las operaciones militares, ayudando a la toma de decisiones.

La Escuela Superior Técnica ha colaborado, a requerimiento, con (CITEDEF) en la aplicación de Criptografía para la protección de enlaces con información sensible.

A continuación se describirá brevemente el desarrollo de tal aplicación .

LABORATORIO DE CRIPTOGRAFÍA Y SEGURIDAD TELEINFORMÁTICA



C-RAIOM

Laboratorio de Criptografía y Seguridad Teleinformática

Realidad Aumentada, un salto al futuro

Diario La Nación:
http://www.lanacion.com.ar/1499038-realidad-aumentada-un-salto-al-futuro

C-RAIOM

Laboratorio de Criptografía y Seguridad Teleinformática

Realidad Aumentada, un salto al futuro desde CITEDEF

MILITAR ARGENTINA

CLICK AQUÍ PARA VOLVER A LA PÁGINA PRINCIPAL

CITEDEF – REALIDAD AUMENTADA: ESTRATEGIA EN EL ÁREA DE INGENIERÍA DEL SOFTWARE

mayo 29, 2012 *de marcelocimino*

Como parte de la estrategia de I+D en el área de la ingeniería del software que lleva adelante la Gerencia de Informática (GEINF) del CITEDEF a cargo del Ing. Hugo Ballesteros, se están estudiando tecnologías aplicadas al campo de la Realidad Aumentada (RA), entendiéndose como tal al conjunto de sistemas (equipos y software) que añaden información virtual adicional al entorno físico que nos rodea.

El estudio de la RA posibilitará el desarrollo de nuevos sistemas de identificación de objetos para el uso de la Defensa, a fin de contar con un avance tecnológico de vanguardia en este aspecto, posicionando a la Argentina como país especializado en la aplicación de este tipo de tecnología de carácter interdisciplinario. La utilización de RA permitirá a las fuerzas militares contar con información precisa del entorno donde se está ejecutando las operaciones militares, ayudando a la toma de decisiones.

En respuesta a estos estudios avanzados de nuevas tecnologías se presentó a fines de 2011 un proyecto en el marco de los PIDDEF 2012-2014, denominado RAIOM (Realidad Aumentada para la Identificación de Objetivos Militares). Este Proyecto consiste en el diseño de un "framework" específico para el desarrollo de software vinculado con la RA en el área militar y relacionado al concepto de "Guerra o Batalla Ubicua", en donde cada soldado de un grupo de combate utiliza equipamiento de RA individual (pantallas flexibles,

Comenzó a ser desarrollado en el Instituto de Investigaciones Científicas y Técnicas para la Defensa (CITEDEF) por la Gerencia de Informática (GEINF) del CITEDEF que estaba a cargo del Ing. Hugo Ballesteros, Ing. Carlos Esteves, jefe del Departamento de Desarrollo de Software y M. Ing. Alejandro Mitaritonna co-director del proyecto (actual Director).

C-RAIOM

Laboratorio de Criptografía y Seguridad Teleinformática

¿Qué es Realidad Aumentada?

Es un concepto que se utiliza para definir una visión directa o indirecta de un entorno físico del mundo real, cuyos elementos se combinan con elementos virtuales para la creación de una realidad mixta en tiempo real.

C-RAIOM

Laboratorio de Criptografía y Seguridad Teleinformática

Proyecto RAIOM

Realidad Aumentada para la Identificación de Objetivos Militares

El proyecto consiste en el desarrollo de software para ser aplicado en dispositivos móviles, que utilizan la tecnología de Realidad Aumentada (RA) como **soporte cognitivo para la mejora de la conciencia situacional** en operaciones militares.

C-RAIOM

Laboratorio de Criptografía y Seguridad Teleinformática

Realidad Aumentada

Imágenes capturadas por el dispositivo de Realidad Aumentada y enviadas al CCC.

Imágenes recibidas en CCC y envío de información o directivas.

Enlace a proteger

C-RAIOM

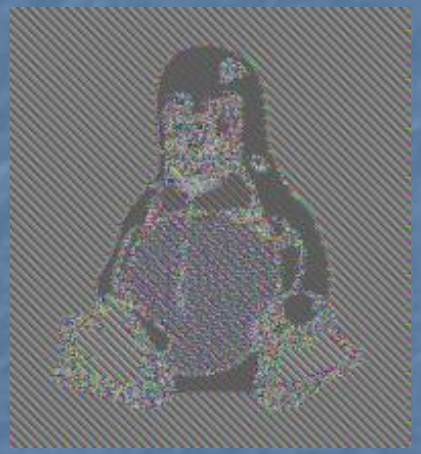
Laboratorio de Criptografía y Seguridad Teleinformática

Singularidades con los sistemas de cifrado de imágenes y video

Se tuvo presente que en muchos casos, aun usando un muy buen algoritmo, no se obtiene un buen resultado. Un ejemplo podría ser el siguiente

AES – 256 bits

Modo ECB



Se aprecia, aún luego del cifrado, un fantasma de la imagen original

AES = Advance Encryption Standard ⊙ ECB = Electronic Code Book

C-RAIOM

Laboratorio de Criptografía y Seguridad Teleinformática

Algoritmo Seleccionado
Generalidades

Esquema Criptológico seleccionado:

- cifrado en flujo o cadena (Stream Cipher)

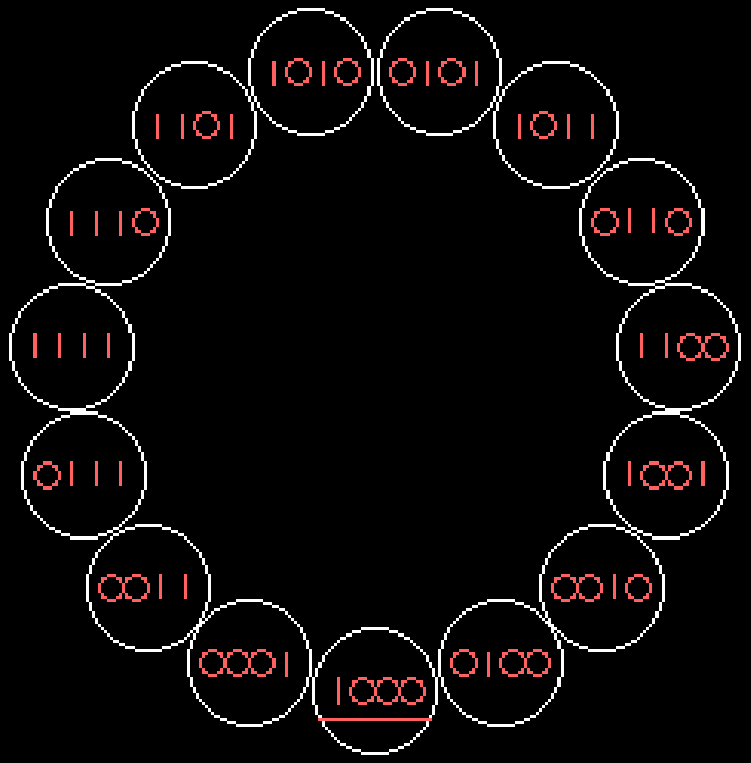
Se seleccionó para la aplicación la Familia Trivium

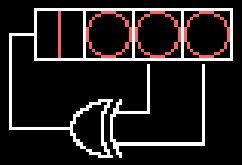
Cualidades:

- Velocidad de ejecución.
- Requieren mínima capacidad de cómputo para su uso.
- Proveen seguridad y autenticación en el mismo proceso.
- Fortaleza y resistencia (hasta el momento) a los ataques criptoanáliticos.
- Es posible modificar el sistema para particularizarlo.
- Seguridad y velocidad aún con imágenes y video.

ESQUEMAS DE CIFRADO EN FLUJO O CADENA

LFSR Linear Feedback Shift Register
(Registro de Desplazamiento con Retroalimentación Lineal)





Ejemplo: 2^4-1

Trivium: $2^{288}-1$

Trivium Toy: $2^{96}-1$

TRIVIUM

El algoritmo en cadena o stream Cipher TRIVIUM fue diseñado por Christophe De Cannière y Bart Preneel.

Se presentó en noviembre de 2004 en el e-Stream Stream Cipher Project perteneciente a la Organización Criptográfica Europea ECRYPT, resultando finalista en hardware.

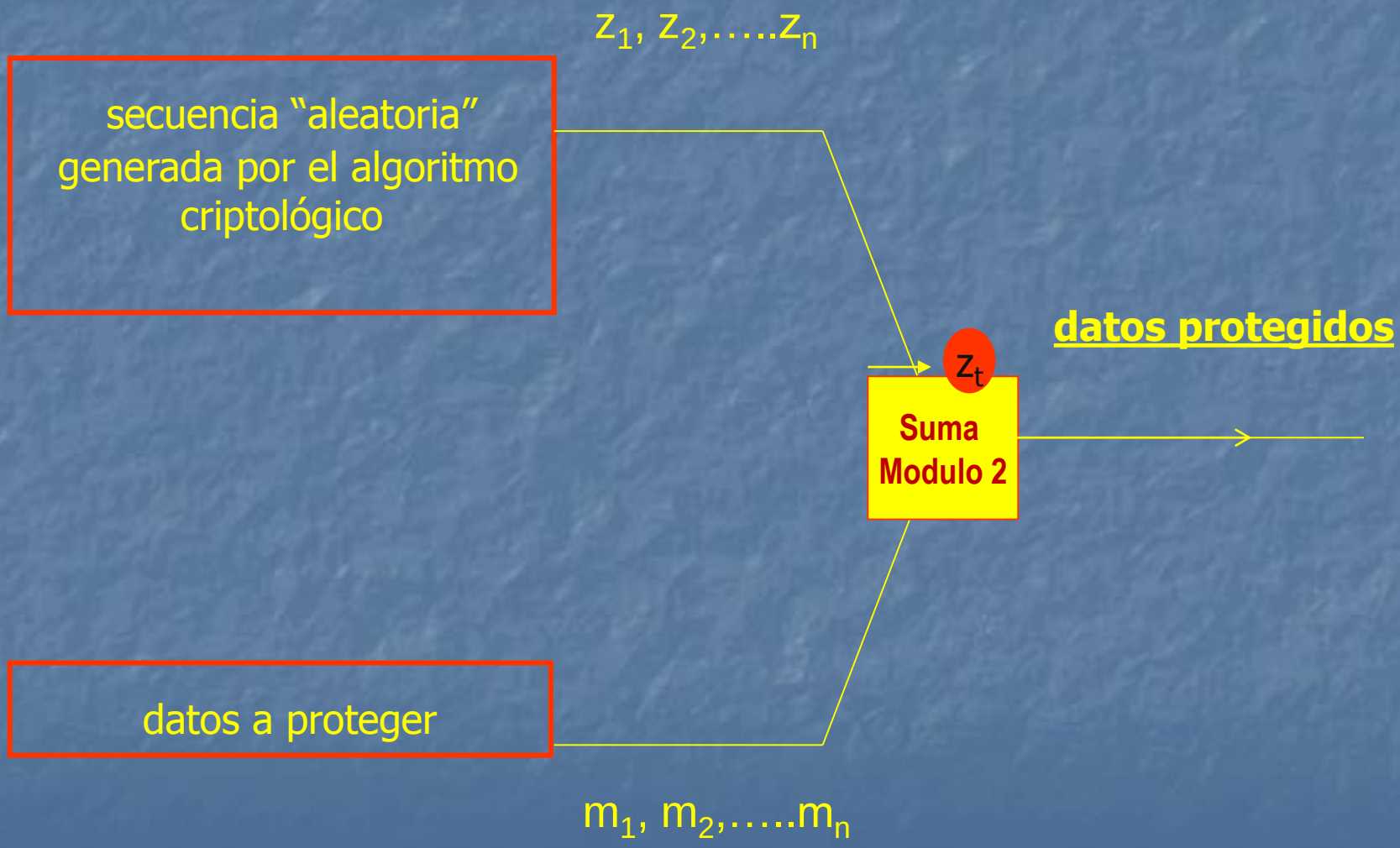
Genera 2^{64} bits de secuencia cifrante (key bit stream K_t) y utiliza una clave secreta y cada vector de inicialización tiene 80 bits.
(2^{80} bits es un número aproximado al de las moléculas de H_2O contenidas en 36 gramos).

Consta de tres registros desplazables no lineales (NLFSR) de longitudes 93, 84 y 111 (total 288 bits).

La idea principal, detrás del diseño de este algoritmo, es aplicar los principios utilizados en la construcción de cifrados en bloques de modo tal de crear componentes criptológicamente equivalentes en el cifrado en cadena.

Hasta el momento ha sido resistente a los ataques criptoanáliticos conocidos.

ESQUEMA DE FUNCIONAMIENTO



DEL TRIVIUM AL TRIVIUM TOY

- ✓ Se comenzó estudiando el período del generador. (Problema abierto)
- ✓ Se estudiaron propuestas de extensión del TRIVIUM (Modelos extendidos).
- ✓ Como consecuencia de estos estudios se desarrolló un modelo reducido que se denominó TOY.
- ✓ La idea fue efectuar estos estudios sobre un algoritmo mas pequeño y más práctico.
- ✓ La reducción que se realizó respetó los principios de diseño del algoritmo original.
- ✓ El TOY ha resultado, en base a las pruebas realizadas, ser más eficiente que el TRIVIUM; y tan seguro como lo es el Trivium lineal original.

TRIVIUM vs TRIVIUM TOY

- ✓ Los resultados de los Test estadísticos de Marsaglia aplicados al Toy resultan, en algunos casos, superiores a los aplicados al generador original.
- ✓ De igual manera, algunos de los Test estadísticos del NIST (National Institute of Standards and Technology) aplicados al Toy, también superan al original.
- ✓ Distintas implementaciones del Toy resultaron más eficientes que el algoritmo Trivium original.
- ✓ Hasta el momento el modelo reducido, que en un principio sólo fue creado para criptoanalizar al generador Trivium, resulta ser más eficiente.
- ✓ En nuestro actual trabajo hemos demostrado algebraicamente que el Trivium toy lineal es criptológicamente tan seguro como el Trivium lineal original.

EFICIENCIA DEL TOY

- ✓ **Hasta el momento los modelos reducidos, que en un principio sólo fueron creados para criptoanalizar a los generadores Trivium, Bivium, y toda la misma familia, resultaron tener la misma robustez criptológica frente a los test estadísticos para secuencias pseudoaleatorias.**

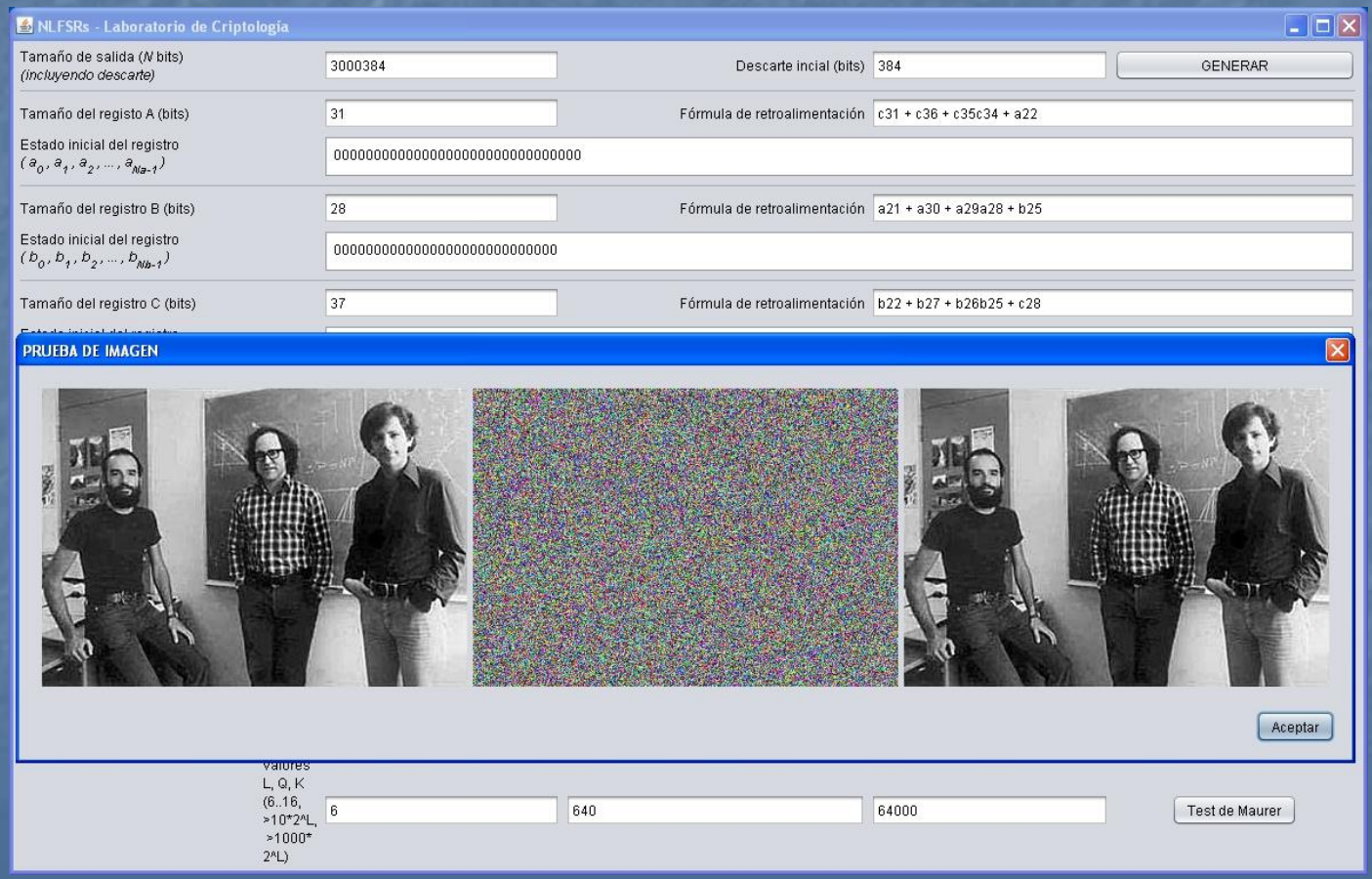
Estos resultados de la investigación fueron presentados ante:

1) Castro Lechtaler, A.; Cipriano, M.; García, E.; Liporace, J. Maiorano, A. y Malvacio, E. **Model Design for a Reduced Variant of a Trivium Type Stream Cipher**. Proceedings of the 19th Argentinean Congress on Computer Science - II Workshop Computer Security (WSI). ISBN 978-987-23963-1-2. pp. 1.483 a 1.491. Mar del Plata, Argentina. Octubre de 2013.

2) Castro Lechtaler, A.; Cipriano, M.; García, E.; Liporace, J.; Maiorano, A.; Malvacio, E. "**Análisis y estudio del período de los algoritmos Trivium y Trivium To**y". XVI Workshop de Investigadores en Ciencias de la Computación - WICC 2014. Ushuaia, Argentina. Mayo de 2014. ISBN (en trámite).

3) Castro Lechtaler, A.; Cipriano, M.; García, E.; Liporace, J.; Maiorano, A.; Malvacio, E. "**Trivium vs. Trivium Toy**". Workshop de Seguridad Informática – WSegI. 43 JAIIO - 43 Jornadas Argentinas de Informática. Buenos Aires. Argentina. Septiembre de 2014. (en evaluación).

Sujetos de prueba para imagen en PC: Rivest – Shamir - Adleman




EJERCITO ARGENTINO
ESCUELA SUPERIOR TECNICA


CL
CRIPTOLAB

DEMO


EJERCITO ARGENTINO
ESCUELA SUPERIOR TECNICA


CL
CRIPTOLAB

GRACIAS