Criptoanálisis del algoritmo RSA con un tamaño mayor de 330 bits basado en técnicas de factorización.

Anteproyecto de Trabajo de Grado

Lina Fernanda Hidalgo López

Director: Ing. Esp. Siler Amador Donado

Universidad del Cauca

Facultad de Ingeniería Electrónica y Telecomunicaciones
Departamento de Ingeniería de Sistemas
Programa de Ingeniería en Electrónica y Telecomunicaciones

Popayán, Noviembre de 2015

TABLA DE CONTENIDO

LISTA DE ILUSTRACIONES

LISTA DE TABLAS

1. PLANTEAMIENTO DEL PROBLEMA

El algoritmo RSA (*Rivest, Shamir y Adleman*) es uno de los más seguros en la actualidad, ya que emplea una clave de ciframiento numérica bastante grande que convierte la información en una cadena de bits o en un archivo binario que solo puede ser descifrada por los integrantes de la comunicación. El funcionamiento del RSA está basado en expresiones exponenciales en aritmética modular, por tanto los mensajes están protegidos por claves generadas al multiplicar dos números primos que tienen como resultado claves mayores a $300\ bits$ o 100 dígitos decimales elegidos al azar. Teniendo en cuenta lo anterior el proyecto pretende realizar un estudio para claves mayores a 330 bits, ya que el tiempo que requiere el criptoanálisis de estos tamaños de clave no supera los cuatro meses de procesamiento de máquina [1].

En la actualidad el problema del RSA se ha desarrollado en torno a cómo fortalecer el algoritmo de seguridad matemáticamente, haciendo cada vez más difícil la forma de vulnerar los sistemas que lo utilizan, encontrando números primos muy grandes que permitan cifrar la información, haciéndola cada vez más difícil de robar. Por otra parte países asiáticos han desarrollado investigaciones para vulnerar este algoritmomediante: mecanismos hardware [21], matemática modular [15] o semejanzas entre el RSAy otros algoritmos de seguridad [19], con el fin de probar posibles formas de vulnerarlo, pero hasta ahora aunque algunos casos han sido exitosos por separado, no logran ser tan eficientes como los métodos de factorización, resultado de la convergencia de todos estos estudios. Existen muchos métodos de factorización, la diferencia entre cada uno de ellos se encuentra en que no todos son eficientes en el manejo de números primos demasiado grandes, algunos de ellos se quedan cortos para procesar números muy grandes o tardan demasiado tiempo. Por tanto hoy en día logran destacarse tan solo tres de estos métodos de factorización, como los más útiles y empleados por los investigadores y hackers en el mundo [14].

Dado que no siempre estas nuevas formas de quebrantar el RSA son efectivas y útiles para todos los tamaños de números primos, se ve la necesidad de volver a los métodos de factorización de números primos grandes para lograr tener una solución efectiva para cualquier tamaño de mensaje. Por lo tanto, este trabajo busca resolver el problema del RSA mediante una forma completa, evaluando, caracterizando y ejecutando los mejores métodos de factorización bajo las mismas condiciones computacionales con el fin de encontrar cuál de ellos resuelve con mayor rapidez un tamaño de RSA mayor a 330 bits empleando un mismo tamaño de mensaje. De esta forma se logrará hacer una diferenciación respecto a los trabajos realizados anteriormente, haciendo uso de las investigaciones de RSA realizadas en la actualidad y unificándolas en un solo sistema.Por lo anterior surge la pregunta de esta propuesta de grado [2]: ¿es posible estimar el desempeño de los métodos de factorización con base en las investigaciones realizadas en los últimos años para vulnerar un tamaño de RSA mayor a 330 bits empleando condiciones de entorno predefinidas?

Por ahora, esta es una pregunta que no ha sido totalmente resuelta en estudios relacionados al criptoanalisis, por la poca información de cómo se realizó el proceso en su totalidad.

2. ESTADO DEL ARTE

El concepto de cifrado asimétrico o de clave pública apareció en 1976 como resultado de un trabajo de criptografía realizado por *Whitfield Diffie* y *Martin Hellman.* Quienes proponen un sistema par de claves, una pública para cifrar el mensaje antes de la transmisión y una privada para descifrar el mensaje en el receptor. Lo cual permite establecer una comunicación segura por medio de un canal de comunicación inseguro ya que la clave pública permite intercambiar mensajes libremente sin necesidad de comprometer la seguridad de la comunicación, por lo tanto si uno de los miembros de la comunicación no posee la clave privada del transmisor, este no podrá descifrar el mensaje y se mantendrá oculto. Gracias a la popularidad de este tipo de cifrado, se introduce el concepto de firma digital, que permite transmitir mensajes de forma privada verificando la autenticación del mensaje frente a posibles falsificaciones[3].En la ilustración 1 se ilustra gráficamente el proceso de cifrado asimétrico.

Ilustración 1: Esquema de un sistema asimétrico o de clave pública. Fuente: Autor.

El algoritmo RSA es un tipo de cifrado asimétrico conocido por que permite cifrar y firmar el mensaje digitalmente al mismo tiempo. Este algoritmofue desarrollado en 1977 por: Ronald Linn Rivest, Adi Shamir y Leonard Adleman, razón por la que el algoritmo adoptó su nombre, usando las iniciales de los apellidos de sus creadores, este algoritmo puede describirse en tres simples pasos: generación de claves (pública y privada), cifrado y descifrado [4].El concepto de seguridad del RSA nace bajo la siguiente hipótesis: “En los últimos trescientos años muchos matemáticos famosos han trabajado en un método eficiente para factorizar números primos, y en la actualidad la factorización de números primos se basan en el método de Legendre, método con el cual aún no es posible en un tiempo razonable factorizar un número primo de 200 dígitos”, con la cual era clara la necesidad de evaluar nuevos métodos de factorización capaces de vulnerar este algoritmo en un tiempo considerable, dado que en el momento los métodos existentes no eran capaces de resolver tamaños de clave mucho mayor a los 200 dígitos decimales.

Gracias a la complejidad para robar la información de este cifrado, muchos encontraron en él la mejor opción para proteger información sensible. En la actualidad el algoritmo RSA es parte de la ISO 9796-1[1][6]. También muchas empresas reconocidas como: Apple, Microsoft, Google, Oracle, Facebook, entre otros lo emplean como medio de protección de la información.

2.1 Retos RSA

En 1977 los laboratorios RSA lanzaron un reto a nivel mundial con el cual pretendían desafiar a programadores, criptógrafos, matemáticos y aficionados a descifrar un mensaje numérico de 120 cifras decimales, publicado con su exponente público y módulo. El problema fue bautizado como RSA-120 [7] y no fue hasta 1993 cuando cuatro jóvenes:Thomas Denny, Bruce Dodson, Arjen Lenstra, Walter Lioen, Mark Manasse, lograron descifrar el mensaje en cooperación con algunas universidades europeas empleando el método de factorización de *quadratic sieve*[2] o criba cuadrática[7]. En principio este logro se desarrolló en torno a un análisis comparativo entre dos métodos de factorización existentes en la época: el QS (criba cuadrática) y el NFS (Criba de cuerpo numérico). Obteniendo como resultado una predicción de futuros tiempos de procesamiento necesarios para vulnerar tamaños de RSA mayores a 120 dígitos en millones de instrucciones por segundo (MIPS[3]), el tiempo total del experimento fue aproximadamente.

De todos los tamaños de RSA lanzados al público para ser descifrados, el más famoso de todos ellos fue el RSA -129[5] dígitos, el cual ofrecía un premio de USD 100 por descifrar el mensaje contenido. Pero solo fue1994 que el premio fue cobrado y donado a la fundación “Free Software Foundation”, por más de 1000 máquinas que se unieron con el fin de obtener el premio. Este proyecto de RSA recibió el nombre de: “***The Magic Words are Squeamish Ossifrage”.*** El curioso nombre fue dado por el mensaje que estuvo escondido por más de diecisiete años y que fue revelado al mundo utilizando el método de quadratic sieve (QS).Gracias a la colaboración de 600 personas que aportaron tiempo de cómputo de unas 1600 máquinas (2 eran un fax), durante aproximadamente seis meses el mensaje fue finalmente encontrado.

Durante casi 10 años no se registró ningún reto de RSA roto, has que el 5 de diciembre de 2003 el equipo de la universidad de Bonn (Bundesamt für Sicherheit in der Informationstechnik) conformado por J. Franke y T. Kleinjung, anuncinciaron la factorización del RSA de 174 dígitos (**RSA 576 bits**), empleando el método de factorización de Criba de cuerpo numérico genérico (GNFS) utilizando hardware del Instituto de Computación de Bonn en Alemania [8]. Pocos datos se conocen sobre este

---

[1]Una firma digital debe ser verificable por un tercero sin que este conozca el secreto del firmante. Para un esquema basado en un criptosistema de clave pública. La primera realización de firmas digitales se basaba en el criptosistema RSA, que es ahora la clave pública más utilizada.

[2]Es un algoritmo de factorización de enteros y, en la práctica, el segundo método más rápido conocido. Es todavía el más rápido para enteros que tienen 100 o menos dígitos decimales, y es considerado mucho más sencillo que la criba de cuerpos numéricos. Es un algoritmo de factorización de propósito general, lo que significa que su tiempo de ejecución únicamente depende el tamaño del entero a ser factorizado.

[3]MIPS o Millones de instrucciones por segundo.Es una forma de medir la potencia de los microprocesadores. Sin embargo, esta medida solo es útil para comparar procesadores con el mismo conjunto de instrucciones y usando técnica para medir el rendimiento de un sistema o componente del mismo en este caso el compilador del equipo.

proyecto, por tanto es un poco difícil establecer detalles del mismo. Sin embargo dos años más tarde en 2005 nuevamente. Franke, T. Kleinjung y F. Bahr, M. Boehm, hacen el anuncio de haber encontrado el mensaje oculto tras el RSA de 193 dígitos (**RSA 640 bits)** [9]. Todo empezó como un reto para vulnerar el RSA en menos de 100 días empleando el método de GNFS nuevamente, como resultado el proyecto se tomó 5 meses en total para obtener los factores primos y descifrar el mensaje[10].

Finalmente en diciembre de 2009 Kleinjung, Thorsten, Aoki, Kazumaro, Franke, Jens, Lenstra, Arjen K, Thomé, Emmanuel, Bos, Joppe W, Gaudry, Pierrick, Kruppa, Alexander, Montgomery, Peter L, Osvik, Dag Arne, Te Riele, Herman, Timofeev, Andrey y Zimmermann, Paul, reportaron la factorización del RSA de 232 dígitos (**RSA-768 bits**) usando el método de factorización NFS, este proceso les tomo aproximadamente 20años de procesamiento de maquina en diferentes universidades alrededor del mundo y 4 meses para ser descubierto el mensaje. En su artículo exponen una posible predicción para romper el RSA 1024, que hasta el momento no registra publicación y algunas experimentaciones con diferentes variantes del método QS con el fin de encontrar los factores primos con mayor rapidez [11].

Algo en común que presentan todos estos artículos es que pocos de ellos explican claramente la forma en cómo se logró quebrantar el algoritmo RSA, casi todos ellos están enfocados a exponer los resultados encontrados, pero ninguno habla sobre una metodología clara de trabajo o el tipo de programación usada para llegar a estos resultados.

2.2 Estudios del RSA en la actualidad

Actualmente los estudios de RSA están enfocados hacia diversos campos, algunos exploran la posibilidad de descubrir los secretos del RSA tras la matemática que lo rodea, experimentando a través de los diferentes métodos de ataque [20], otros ven la posibilidad de quebrantar el RSA mediante ataques de potencia examinando bit a bit este algoritmo por medio de curvas de consumo energético al analizar el tamaño del mensaje cifrado y el comportamiento energético al factorizar pequeñas cifras [17]. Por otra parte algunos proponen nuevos métodos de análisis para recuperar las llaves de la comunicación, unos proponen nuevos esquemas de análisis de RSA en el cual se obtenga la llave privada por fuerza bruta y se factorice la pública [15], mientras que otros examinan la posibilidad de realizar ataques de detección y corrección de errores [19], estableciendo pequeños rangos de error para detectar computacionalmente por que se tarda tanto en conseguir los factores primos que componen el tamaño del mensaje y corregirlo, mejorando así los tiempos de procesamiento (t-test y BB- Attack), finalmente otros grupos han enfocado sus investigaciones a robar las llaves de comunicación individualmente escuchando el número de revoluciones del disco duro al procesar una factorización, recolectando información sobre el tipo de software empleado como herramienta de procesamiento [21],

El resultado de todos estos nuevos experimentos da como resultado métodos alternos al de factorización, pero que de una u otra forma convergen a la factorización de números primos para llegar al resultado de sus análisis [19]. El gobierno enfoca sus esfuerzos a fortalecer matemáticamente el algoritmo haciéndolo cada vez más fuerte incrementando o disminuyendo los tamaños de las llaves o componentes del algoritmo. Sin embargo los científicos e investigadores están logrando encontrar una forma alternativa de vulnerarlo.
El éxito de estos estudios han logrado sobrepasar las expectativas, pero pese a eso no todos han logrado pasar la barrera de los RSA rotos hasta la fecha. Infortunadamente no

todos son métodos prácticos, la mayoría de ellos aún se encuentran en fase experimental y teórica y pocos han dado un resultado práctico, por lo tanto hasta no encontrar un nuevo mecanismo que arroje resultados tanto teóricos como prácticos, el método de factorización seguirá vigente como uno de los más eficientes para descifrar el RSA

2.3 Metodologías de factorización empleadas

Existen múltiples métodos de factorización, algunos son capaces de factorizar hasta un cierto tamaño de número, como una cota máxima de utilidad para ser empleado según el caso, mientras que otros son capaces de factorizar todo tamaño de número desde el más pequeño al más grande. En la factorización de número primos se destacan algunos métodos de factorización, para un tamaño menor a 100 o 50 cifras decimales son útiles métodos como [22]:

1. Método de factorización directa o criba de Eratóstenes
2. Método de Fermat
3. Método de Euler
4. Método de Dixon
5. Williams p+1 Factorization Method
6. Método de Pollar rho
7. Método de Pollar p-1
8. Método de las fracciones continúas
9. Método de las curvas elípticas

La razón por la cual esto métodos no son útiles para tamaños factorizar tamaños grandes de números primos es el proceso matemático de iteraciones u operaciones, las cuales pueden volverse casi infinitas para un número de 620 cifras decimales, lo cual retrasaría los procesos que lo requieran [14].

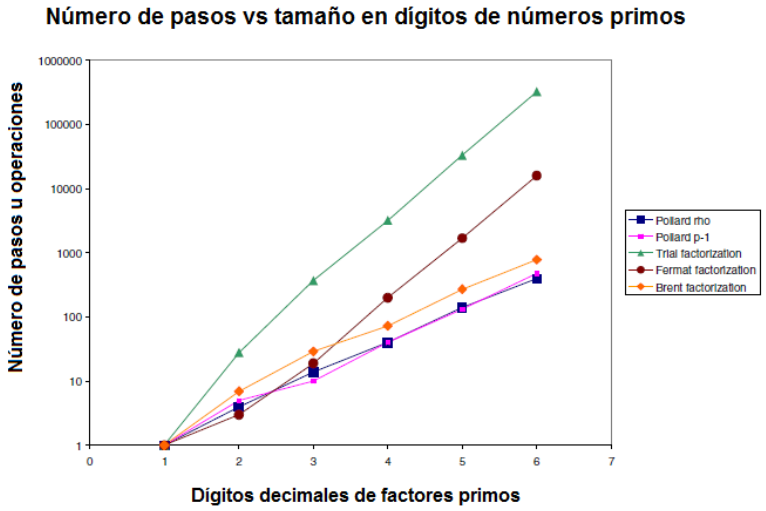

Ilustración 2: Número de pasos según el algoritmo de factorización, tomado de "Integer Factorization Algorithms" de Connely Barnes [14].

Actualmente el método de factorización de criba cuadrática y sus variaciones matemáticas son los métodos más eficientes a la hora de resolver factorizaciones matemáticas de números demasiado grandes, tomando un tiempo de operación matemática mayor a los tres meses como mínimo registrado [12].

El método de factorización de **criba cuadrática (QS)**fue desarrollado porCarl Prometanse, un matemático estadounidense especializado en teoría de números. Prometanse junto con Dixon y Kraitchik, formuló en 1981 el algoritmo de criba cuadrática (Quadratic Sieve) el cual permitió en su momento factorizar números enteros grandes. La criba consiste básicamente de 10 pasos[13] los cuales permite factorizar de forma rápida números menores a 110 cifras decimales. El QS fue el método de factorización más rápido desarrollado hasta 1993, cuando se desarrolló la criba de cuerpo numérico (Number Field Sieve) que en la actualidad es el más eficiente para resolver factorizaciones de números muy grandes.

La **criba general de cuerpo numérico (GNFS**) o *genericnumber field sieve* es el método más eficiente para factorizar números enteros de tamaño mayor a 110 dígitos. Matemáticamente se describe como una expresión que depende de logaritmos naturales y expresiones exponenciales. La criba general del cuerpo de números no solo calcula las potencias primas de un número "*n*" sino que también puede reducir o factorizar cualquier número.Este método se puede entender como una mejora de la criba cuadrática que puede factorizar un número grande "*n*", mediante la gestión o búsqueda de números lisos de tamaño $n^{1/2}$, ya que al ser valores menores a "*n*" incrementan la posibilidad de ser números con factores primos pequeños, lo cual hace que el GNFS sea un algoritmo robusto en cuanto a la búsqueda de números que el algoritmo anterior.

Una vez el GNFS halla los posibles factores primos, realiza el procesamiento de los datos en cuerpo numérico, lo cual incrementa la complejidad del método. El tiempo de ejecución de la criba del cuerpo de números es super-polinomial pero sub-exponencial en el tamaño de la entrada [13].

3. OBJETIVOS

3.1 Objetivo general

Realizar el criptoanálisis del algoritmo RSA de tamaño mayor a 330 bits empleando una configuración computacional predefinida con el fin de evaluar tres métodos de factorización de números primos.

3.2 Objetivos específicos

- ✓ Definir las métricas o medidas con las cuales se puede seleccionar los métodos de factorización más eficientes en la actualidad para criptoanalizar.
- ✓ Diseñar las pruebas para el criptoanálisis del RSA a partir de las métricas de evaluación definidas.
- ✓ Analizar comparativamente el rendimiento de los métodos de criptoanálisis a partir de la evaluación de las métricas de los métodos de factorización.

4. APORTES

Este trabajo pretende generar un punto de partida para futuros investigadores interesados en el criptoanálisis de algoritmos RSA. Ya que es una de las áreas poco estudiadas en la Universidad del Cauca, se pretende:

1. Establecer parámetros que permitan diferenciar algunos de los métodos de factorización de números grandes para optimizar procesos de criptoanálisis a futuro
2. Aportar un posible modelo de pruebas a realizar a partir de la identificación de las métricas de evaluación para generar un criptoanálisis eficiente.
3. Contribuir a futuras investigaciones de RSA el método de factorización más eficiente para criptoanalizar cualquier tamaño de RSA.

5. METODOLOGIA

Las fases de este proyecto dependen de la realización de la fase anterior, para tener una mayor claridad en cómo se desarrollará este proyecto se han numerado y descrito cada fase a continuación:

- **Fase 1:** Búsqueda de métodos de factorización matemáticos para criptoanálisis del RSA. Trabajos pasados relacionados con la investigación y descripción del funcionamiento del algoritmo matemáticamente y físicamente.
    - Búsqueda bibliográfica
    - Clasificación de la información
- **Fase2:** Caracterización de las técnicas de factorización de números grandes a partir de modelos existentes empleados anteriormente para el criptoanálisis del algoritmo RSA.
    - Observación de la información
    - Descripción de las características
    - Jerarquización
- **Fase 3:**Selección de la información a partir de los criterios establecidos en la fase anterior.
    - Filtrado de métodos de factorización
    - Diferenciación entre soluciones matemáticas y computacionales.
- **Fase 4:** Evaluación de un prototipo generado a partir del análisis teórico. Como observación este proyecto no desarrollará el prototipo funcional, simplemente se enfocará en proponer una posible solución al grupo de investigadores que lo desarrollará con base en la investigación que se está realizando.
    - Selección del tipo de pruebas que se realizarán al prototipo.
    - Aplicación de las pruebas.
- **Fase 5:** Documentación del proceso y resultados del proyecto.

6. ACTIVIDADES Y CRONOGRAMA

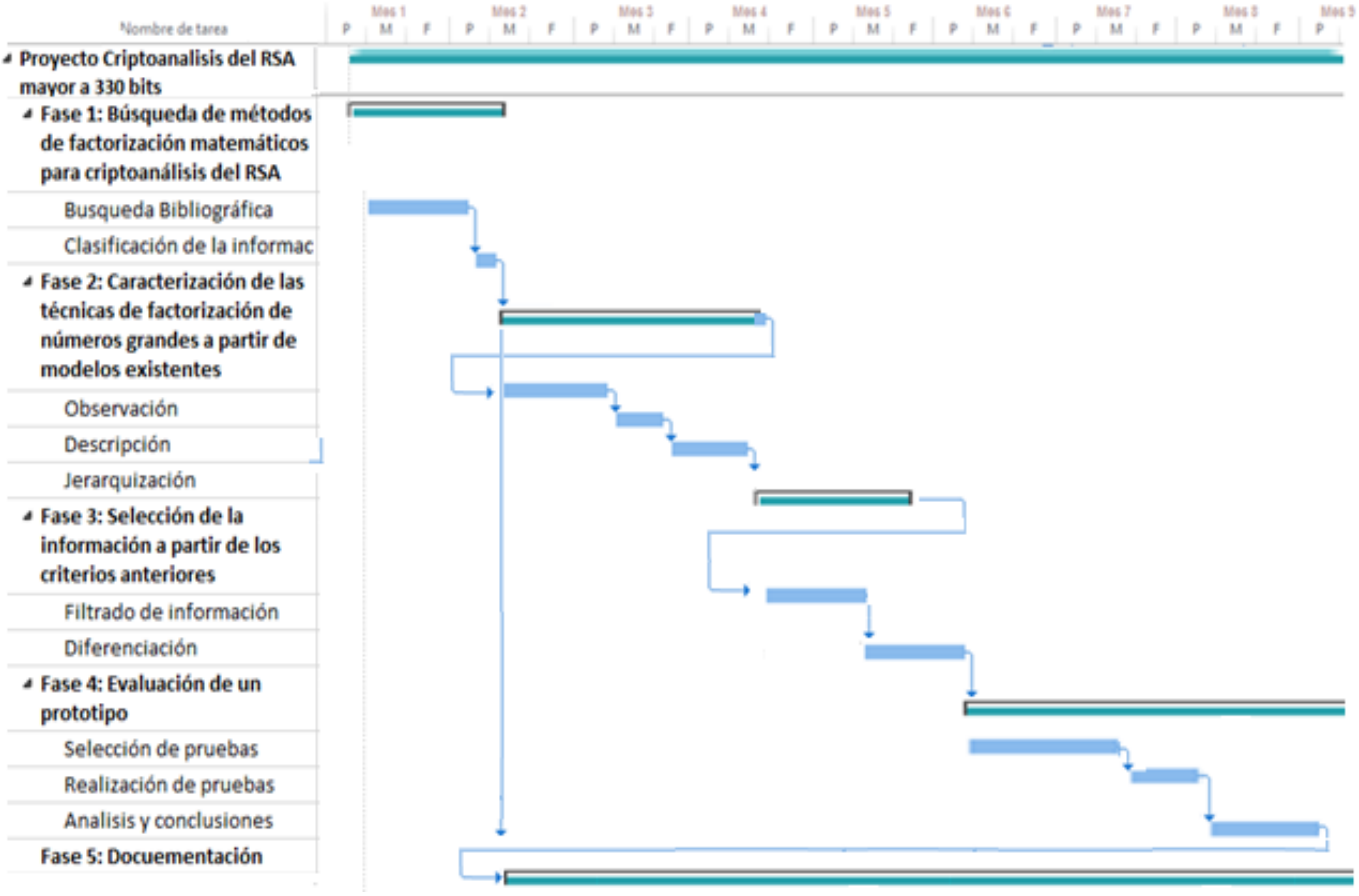

Ilustración 3: Cronograma de actividades

7. RECURSOS, PRESUPUESTO Y FUENTES DE FINANCIACIÓN

RUBROS	FUENTES		TOTAL
	ESTUDIANTE	*DEPARTAMENTO*	
RECURSOS HUMANOS			
Director	-	$ 1.878.840,00	**$ 1.878.840,00**
Estudiantes	$ 22.546.080,00	-	**$ 22.546.080,00**
RECURSOS TECNICOS			
Recursos Hardware			
Equipo	$ 2.000.000,00	-	**$ 2.000.000,00**
Recursos Software			
Software	-	-	
Recursos Bibliográficos			

Documentación	$ 150.000,00	$ 100.000,00	**$ 250.000,00**
SUBTOTAL	$ 24.696.080,00	$ 1.978.840,00	**$ 26.674.920,00**
Recursos Varios			
Comunicación	$ 525.421,48	-	**$ 525.421,48**
AUI	$ 5.359.299,06	-	**$ 5.359.299,06**
TOTAL	$ 55.276.880,54	$ 2.078.840,00	**$ 57.355.720,54**

Tabla 1. Presupuesto

8. CONDICIONES DE ENTREGA

Una vez finalizado el proyecto se hará entrega de:

- Monografía de tesis donde se consigne la fundamentación teórica y los resultados
- Artículo científico para ser enviado a una revista indexada, en el que se expongan los principales aportes del proyecto.

9. REFERENCIAS

[1] D. M. Bressoud, Factorization and Primality Testing, in Springer, Board, Ed. New York ,USA, 1989.

[2] C.A Henk. V. Tilborg, S. Jajodia, Encyclopedia of Cryptography and Security, Volume 1, vol. 0. Springer Science & Business Media, 2011.

[3] J.M. Basart, J. Rifá, M. Villanueva, Fonaments de matemàtica discreta, in Criptografía y Seguridad en Computadores, S. Publicaciones, Ed. Barcelona, España: Universitat Autònoma de Barcelona, 1999.

[4] J. R. Aguirre, Seguridad informática y Criptografía. Universidad Politécnica de Madrid, Madrid, 2004.

[5] D. Atkins, M. Graff, a Lenstra, and P. Leyland, The magic words are squeamish ossifrage, Adv. Cryptology— …, pp. 263–277, 1995.

[6] S. Halevi, D. Coppersmith, F. Grieu, J.S. Coron, “Cryptanalysis of ISO/IEC 9796-1,” Paris, Francia, 2009.

[7] M.S. Manasse, T. Denny, B. Dodson; A.K. Lenstra, “On the factorization of RSA-120,” pp. 166–174, 1993.

[8] RSA Laboratories - RSA-576 is factored! [Online]. Available: http://www.emc.com/emc-plus/rsa-labs/historical/rsa-576-factored.htm. [Accessed: 27-Nov-2015].

[9] H. Youm, M. Youg, Information Security Applications: 10th International Workshop, WISA 2009, Busan, Korea, August 25-27, 2009, Revised Selected Papers. Springer Science & Business Media, 2010.

[10] RSA Laboratories - RSA-640 is factored! [Online]. Available: http://www.emc.com/emc-plus/rsa-labs/historical/rsa-640-factored.htm. [Accessed: 02-Dec-2015].

[11] T. Kleinjung, K. Aoki, J. Franke, A. K. Lenstra, E. Thomé, J. W. Bos, P. Gaudry, A. Kruppa, P. L. Montgomery, D. A. Osvik, H. Te Riele, A. Timofeev, and P. Zimmermann, Factorization of a 768-Bit RSA modulus,Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 6223 LNCS, pp. 333–350, 2010.

[12] S.Y. Yan, Cryptanalytic Attacks on RSA, vol. 15. Springer Science & Business Media, 2007.

[13] J. Fernandez, Implementacion de la Criba Cuadratica (Quadratic Sieve) en C++ ~ Code Botic. [Online]. Available: http://www.codebotic.com/2015/07/implementacion-de-la-criba-cuadratica.html. [Accessed: 27-Nov-2015].

[14] Barnes, C. Integer Factorization Algorithms. Oregon: Oregon State University. (2004).

[15] Aboud, S. J. An efficient method for attack RSA scheme. In 2009 Second International Conference on the Applications of Digital Information and Web Technologies (pp. 587–591). IEEE, 2009

[16] Amiel, F., Villegas, K., Feix, B., & Marcel, L. Passive and Active Combined Attacks: Combining Fault Attacks and Side Channel Analysis. In Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC 2007) (pp. 92–102). IEEE,2007.

[17] Bertoni, G. M., Breveglieri, L., Cominola, A., Melzani, F., & Susella, R..Practical Power Analysis Attacks to RSA on a Large IP Portfolio SoC. In 2009 Sixth International Conference on Information Technology: New Generations (pp. 455–460). IEEE, 2009.

[18] Chen, C., Wang, T., Kou, Y., Chen, X., & Li, X. Improvement of trace-driven I-Cache timing attack on the RSA algorithm. Journal of Systems and Software, 86(1), 100–107,2013.

[19] Chen, C., Wang, T., & Tian, J. Improving timing attack on RSA-CRT via error detection and correction strategy. Information Sciences, 232, 464–474, 2013.

[20] Chmielowiec, A. Fixed points of the RSA encryption algorithm. Theoretical Computer Science, 411(1), 288–292, 2010.

[21] Genkin, D., Shamir, A., & Tromer, E. RSA key extraction via low-bandwidth acoustic cryptanalysis. Lecture Notes in Computer Science (including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 8616 LNCS(PART 1), 444–461, 2014.

[22] MOOC Crypt4you UPM (n.d). [Online]. Available: http://www.criptored.ipm.es/crypt4you/RSA/leccion8/leccion08.html. [Accessed: 19-Oct-2015]

ACTA DE PROPIEDAD INTELECTUAL

UNIVERSIDAD DEL CAUCA FACULTAD DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES

ACTA DE ACUERDO SOBRE LA PROPIEDAD INTELECTUAL DEL TRABAJO DE GRADO

En atención al acuerdo del Honorable Consejo Superior de la Universidad del Cauca, número 008 del 23 de Febrero de 1999, donde se estipula todo lo concerniente a la producción intelectual en la institución, los abajo firmantes, reunidos el día __ del mes de _____ de 2016 en el salón del Consejo de Facultad, acordamos las siguientes condiciones para el desarrollo y posible usufructo del siguiente proyecto.

Materia del acuerdo: Trabajo de grado para optar el título de Ingeniero Electrónico en Telecomunicaciones.

Título del Proyecto: **Criptoanálisis del algoritmo RSA con un tamaño mayor de 330 bits basado en técnicas de factorización.**

Objetivo del proyecto: Evaluar al menos tres métodos factorización de números primos grandes para realizar el criptoanálisis del algoritmo RSA de tamaño mayor a 330 bits, empleandoun mismo tamaño de mensaje y una configuración computacional predefinida.

Duración del proyecto: 9 meses.

Cronograma de actividades: Definido en el anteproyecto.

La participante del proyecto, la estudiante de pregrado Lina Fernanda Hidalgo López identificada con la cédula de ciudadanía número 1.061.748.025 de Popayán respectivamente, a quien en adelante se le llamará "estudiante", el ingeniero Siler Amador Donado en calidad de Director del trabajo de grado, identificado con la cédula de ciudadanía número 72.168.640 de Barranquilla a quien en adelante se le llamará "docente", y la Universidad del Cauca, representada por el ingeniero Oscar Josué Calderón identificado con la cédula de ciudadanía número 12.139.176 de Neiva en su calidad de Decano de la FIET, manifiestan que:

1. La idea original del proyecto es del docente quien la propuso y presentó al Departamento de Telecomunicaciones, que la aceptó como tema para el proyecto de grado en referencia.

2. La idea mencionada fue acogida por el estudiante como proyecto para obtener el grado de Ingeniero en Electrónica y Telecomunicaciones, quienes la desarrollarán bajo la dirección del docente.

3. Los derechos intelectuales y morales corresponden al docente y a la estudiante.

4. Los derechos patrimoniales corresponden al docente, al estudiante y a la Universidad del Cauca por partes iguales y continuarán vigentes, aún después de la desvinculación de alguna de las partes de la Universidad.

5. La participante se compromete a cumplir con todas las condiciones de tiempo, recursos, infraestructura, dirección, asesoría, establecidas en el anteproyecto, a estudiar, analizar, documentar y hacer acta de cambios aprobados por el Consejo de Facultad, durante el desarrollo del proyecto, los cuales entran a formar parte de las condiciones generales.

6. La estudiante se compromete a restituir en efectivo y de manera inmediata a la Universidad los aportes recibidos y los pagos hechos por la Institución a terceros por servicios o equipos, si el comité de Investigaciones declara suspendido el proyecto por incumplimiento del cronograma o de las demás obligaciones contraídas por el estudiante; y en cualquier caso de suspensión, la obligación de devolver en el estado en que les fueron proporcionados y de manera inmediata, los equipos de laboratorio, de cómputo y demás bienes suministrados por la Universidad para la realización del proyecto.

7. El docente y la estudiante se comprometen a dar crédito a la Universidad y de hacer mención del Fondo de Fomento de Investigación, en los informes de avance y de resultados, y en registro de éstos, cuando ha habido financiación de la Universidad o del Fondo.

8. Cuando por razones de incumplimiento, legalmente comprobadas, de las condiciones de desarrollo planteadas en el anteproyecto y sus modificaciones, alguno de los participantes deba ser excluido del proyecto, los derechos aquí establecidos concluyen para él. Además se tendrán en cuenta los principios establecidos en el reglamento estudiantil vigente de la Universidad del Cauca en lo concerniente a la cancelación y la pérdida del derecho a continuar estudios.

9. El documento del anteproyecto y las actas de modificaciones si las hubiere, forman parte integral de la presente acta.

10. Los aspectos no contemplados en la presente acta serán definidos en los términos del acuerdo 008 del 23 de febrero de 1999 expedido por el Consejo Superior de la Universidad del Cauca, del cual los participantes del acuerdo aseguran tener pleno conocimiento.

Ing. Siler amador Donado
Director

Ing. Oscar Josué Calderón
Decano

Lina Fernanda Hidalgo López
Estudiante