

Tabla de Contenido

Índice de Tablas	x
Índice de Ilustraciones	xi
1 Introducción	1
1.1 Sobre Buzones y Encriptación de Clave Pública	1
1.2 Motivación	2
1.3 Objetivos	2
1.3.1 Objetivo General	2
1.3.2 Objetivos Específicos	2
1.4 Organización del Documento	3
2 Antecedentes	4
2.1 Criptografía Asimétrica	4
2.1.1 Sistemas Criptográficos de clave Pública	4
2.2 Sistema Criptográfico RSA	5
2.2.1 Funcionamiento de RSA	5
2.2.2 Generación de Claves	5
2.2.3 Pequeño Ejemplo	6
2.3 Criptografía Umbral	6
2.3.1 Criptografía RSA Umbral	7
3 Análisis y Diseño	8
3.1 Actores del Algoritmo y su Interacción	8
3.2 Descripción del Algoritmo	9
3.2.1 Especificaciones de Parámetros de Entrada y Resultados del Algoritmo	9
3.2.2 Descripción General del Algoritmo	10
3.2.3 Descripción Completa de los Pasos del Algoritmo	11
3.3 Tiempo de Ejecución Aleatorizado del Algoritmo	16
3.4 Capa de Comunicación	17
3.5 Lenguaje de Programación: Erlang	18
4 Implementación	20
4.1 Módulo de Comunicación	20
4.2 Módulos de Pasos	21
4.2.1 Pasos	22
4.2.2 Patrón General de Comunicación	23
4.3 Módulo del Algoritmo Completo	25

4.4	Módulos Locales	26
4.4.1	Módulo de Polinomios	26
4.4.2	Módulo de Funciones Matemáticas	26
4.5	Estructura del Código	27
4.6	Metodología	28
4.6.1	Control de Versiones	28
4.6.2	Entorno de Trabajo	28
4.6.3	Compilación	28
5	Pruebas y Resultados	29
5.1	Descripción de las Pruebas	29
5.1.1	Pruebas Locales	29
5.1.2	Pruebas Distribuidas	29
5.1.3	Verificaciones de Correctitud	30
5.2	Parámetros Utilizados	31
5.3	<i>Hardware</i> Utilizado	31
5.3.1	Pruebas Locales	31
5.3.2	Pruebas Distribuidas	31
5.4	Resultados Obtenidos	32
5.4.1	Relaciones entre Intentos y Tiempos	34
5.5	Comparación entre Esperanza Teórica de Intentos y Promedio Obtenido	35
6	Conclusiones	37
6.1	Trabajo Futuro	38
7	Bibliografía	39
A	Tablas de Resultados Completos	41

Índice de Tablas

5.1	Valores de <code>MNodes</code> y <code>T</code> utilizados al correr las prueba	31
5.2	Valores de las Pendientes de las Aproximaciones Lineales	34
5.3	Intentos Esperados para Distintos Tamaños de Módulos	35
A.1	Resultados obtenidos para tres nodos y un cliente en modo local	41
A.2	Resultados obtenidos para cinco nodos y un cliente en modo local	41
A.3	Resultados obtenidos para tres nodos y un cliente en modo distribuido	42
A.4	Resultados obtenidos para cinco nodos y un cliente en modo distribuido	42
A.5	Comparación entre promedio de intentos esperado y promedio de intentos obtenidos. El promedio obtenido fue calculado con 5 ejecuciones	42

Índice de Ilustraciones

3.1	Esquema de Interacción entre Cliente y Nodos	8
3.2	Esquema de los Pasos del Algoritmo	11
3.3	Esquemas de Comunicación	18
4.1	Flujo de Comunicación entre procesos	21
4.2	Estructura del Código	27
5.1	Resultados obtenidos para tres nodos y un cliente en modo local	32
5.2	Resultados obtenidos para cinco nodos y un cliente en modo local	33
5.3	Resultados obtenidos para tres nodos y un cliente en modo distribuido	33
5.4	Resultados obtenidos para cinco nodos y un cliente en modo distribuido	34
5.5	Comparación entre Promedio Obtenido y Promedio Esperado	36