

Tabla de Contenido

1. Introducción	1
1.1. Contexto	1
1.2. Motivación	2
1.3. Observaciones Generales	3
1.4. Objetivos	3
1.4.1. Objetivo General	3
1.4.2. Objetivos Específicos	4
1.5. Organización del Documento	4
2. Marco Teórico	5
2.1. Encriptación	5
2.1.1. Encriptación Asimétrica	6
2.1.2. Encriptación ElGamal	7
2.2. Firma Electrónica	8
2.2.1. Firma de Grupo	8
2.2.2. Firma Boneh Boyen Shacham (BBS)	9
2.3. Criptografía de Umbral	14
2.3.1. Compartición de Secretos	14
2.3.2. Compartición de Secretos Verificable	14
2.3.3. Proactividad	19
2.4. BBS Distribuido	21
3. Problema	28
3.1. Descripción del Problema	28
3.2. Requisitos de la Solución	28
3.2.1. Autenticación	28
3.2.2. Pseudo-Anonimato	28
3.2.3. Trazabilidad	28
3.2.4. Distribución	29
3.2.5. Proactividad	29
4. Solución	30
4.1. Descripción General de la Solución	30
4.2. Algoritmos	30
4.2.1. Inicialización	31
4.2.2. Emisión	31
4.2.3. Firma	32
4.2.4. Verificación	33

4.2.5.	Rastreo	33
4.2.6.	Recuperación	33
4.2.7.	Renovación	34
4.2.8.	Casos de Uso	34
	4.2.8.1. Inicio de sesión	34
	4.2.8.2. Rastreo de sesión	35
	4.2.8.3. Remplazo de administrador	35
4.3.	Implementación	36
	4.3.1. Optimización	36
	4.3.2. Arquitectura	38
	4.3.3. Interfaces	40
5.	Discusión	43
5.1.	Trabajo Propuesto	43
	5.1.1. Desarrollo de la Aplicación Web	43
	5.1.2. Evaluaciones para Usabilidad	43
	5.1.3. Ataques a Proactividad	44
5.2.	Investigación Previa no Usada en la Solución	45
	5.2.1. Firmas de Anillo	45
	5.2.2. Otros Esquemas de Firma de Grupo	45
6.	Conclusiones	46
6.1.	Revisión de Propiedades	46
6.2.	Revisión de Objetivos	46
6.3.	Requisitos para Producción	47
	Bibliografía	48