

Tabla de Contenido

1. Introducción	1
1.1. Objetivo General	2
1.1.1. Objetivos Específicos	2
2. Antecedentes	3
2.1. Definiciones y conceptos matemáticos	3
2.1.1. Permutación	3
2.1.2. Conjuntos	3
2.2. Criptografía	3
2.2.1. Encriptación y desencriptación	4
2.2.1.1. Encriptación simétrica	4
2.2.1.2. Encriptación asimétrica	4
2.2.1.3. Encriptación homomórfica	5
2.2.1.4. Desencriptación parcial	5
2.2.2. Mezcla verificable	5
2.2.3. Red de mezcla o mixnet	6
2.3. Algoritmos criptográficos	7
2.3.1. Algoritmo de Rijndael	7
2.3.2. Algoritmo de ElGamal	7
2.3.3. Algoritmo de Paillier	7
2.3.4. Algoritmo de Furukawa	8
2.3.5. Algoritmo de Nguyen	8
2.4. Implementación de votaciones electrónicas en EVoting	10
2.5. Arquitectura de nube por Amazon Web Services	11
2.5.1. Amazon Lambda	11
2.5.2. Amazon Simple Storage Service	12
2.5.3. Amazon Step Functions	12
2.5.4. Amazon Serverless Application Model	12
3. Descripción e implementación de la solución	13
3.1. Descripción del problema	13
3.2. Descripción general de la solución	13
3.3. Requisitos de la solución	13
3.4. Mezcla verificable	14
3.4.1. Investigación y evaluación de algoritmos	14
3.4.2. Implementación	14
3.4.3. Optimización	17

3.4.4. Pruebas unitarias	18
3.5. Red de Mezcla	18
3.5.1. Evaluación de soluciones	18
3.5.2. Comparación entre arquitectura serverless y tradicional	19
3.5.3. Serverless Application Model	20
3.5.4. Step Functions	20
3.5.5. API	23
3.6. Aplicación Web	25
3.7. Validación y rendimiento	28
3.8. Mezcla distribuida	30
4. Conclusiones	32
4.1. Trabajo futuro	32
Bibliografía	34
Anexos	36
A. Step Function	36
B. Interfaz de aplicación web	42