DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS E INFORMÁTICA

TEMA: ESTUDIO COMPARATIVO DE ALGORITMOS DE FIRMA DIGITAL UTILIZANDO CRIPTOGRAFÍA ASIMÉTRICA RSA Y CRIPTOGRAFÍA BASADA EN CURVAS ELÍPTICAS

AUTOR: AYALA JACHO, WENDY ARACELLY

DIRECTOR: ING. GALÁRRAGA, FERNANDO

CODIRECTOR: ING. CAIZAGUANO, CARLOS

SANGOLQUÍ

2016

RESUMEN

En el presente trabajo se realiza el estudio comparativo de algoritmos de firma digital entre el esquema criptográfico asimétrico RSA (Rivest, Shamir y Adleman) y el esquema criptográfico basado en curvas elípticas ECDSA (Elliptic Curve DSA). La necesidad de establecer canales de comunicación más seguros en un mundo donde el desarrollo tecnológico avanza a pasos agigantados es indispensable, aún más con la aparición de las computadoras cuánticas donde la capacidad de cálculo ha reducido los tiempos de descifrado de años a días; es por ello que la implementación de algoritmos criptográficos, cuyo descifrado sea más complejo, mejora las posibilidades del resguardo de la información. Por lo tanto, en este proyecto, se analiza los fundamentos matemáticos de los algoritmos de firma digital asimétricos como ElGamal, Rabin, Fiat Shamir, Shor y de curvas elípticas como Diffie-Hellman, ElGamal, Menezes-Vanstone, dando un enfoque especial a los algoritmos de firma electrónica RSA y ECDSA. Los algoritmos en mención, han sido codificados en el ambiente de desarrollo Java, con sus respectivas librerías, con el fin de establecer el algoritmo RSA o el algoritmo ECDSA posee las mejores características para el respaldo de información, considerando la arquitectura del lenguaje de programación. Se ha tomado en cuenta los estándares propios de los algoritmos de firma electrónica asimétricos y de curvas elípticas para que la comparación sea adecuada y arroje resultados que además de medibles sean sustentables. Los resultados obtenidos en este estudio se los visualiza a través de gráficos estadísticos, producto de la cuantificación de los tiempos de respuesta obtenidos en el proceso.

PALABRAS CLAVES:

- **CRIPTOGRAFÍA**
- **FIRMA DIGITAL**
- **CURVAS ELÍPTICAS**
- **RSA**
- **ECDSA**

ABSTRACT

This work is about a comparative study of digital signature algorithms between the asymmetric cryptographic scheme RSA (Rivest, Shamir and Adelman) and the cryptographic scheme based on elliptic curves ECDSA (Elliptic Curve DSA). It is necessary and indispensable to establish safer channels of communication around the world because of the big technological development, especially with the advent of quantum computers where capacity has reduced calculation time decryption from years to days; for that reason the implementation of cryptographic algorithms whose decryption is more complex improves the chances to keep the information safe. The content of this project analyses mathematical foundations of asymmetric digital signature algorithms such as ElGamal, Rabin, Shamir Fiat, Shor and elliptic curves as Diffie-Hellman, ElGamal, Menezes-Vanstone are analyzed, with special focus on RSA and ECDSA respectively. The algorithms have been codified into Java development environment with their respective libraries in order to establish which of them has the best features for data backup; for that reason the architecture of language was considered. Also as part of the study, it has taken in count the levels of security, number of bits according to the level of security and algorithm's own standards in order to have sustainable and measurable results. The form of analysis of the study is developed using Stat Graphs as a product of quantification of response time obtained along the whole process.

KEY WORDS:

- **CRIPTOGRAPHY**
- **DIGITAL SIGNATURE**
- **ELLIPTIC CURVES**
- **RSA**
- **ECDSA**