RESUMEN

En la actualidad, las tecnologías que almacenan y procesan la información crecen cada día, creciendo a la par las amenazas que ponen en peligro dicha información. Por ello, la seguridad informática se vuelve cada vez más importante para proteger la información de personas mal intencionadas que buscan tener un acceso no autorizado. Puesto que muchos algoritmos criptográficos tradicionales ya han sido vulnerados, ha surgido la necesidad de técnicas criptográficas más seguras. En el presente trabajo se propone la implementación de dos nuevos algoritmos criptográficos en una aplicación móvil de chat. Por un lado, la criptografía neuronal, que emplea una estructura modificada de una red neuronal artificial llamada Tree Parity Machine, permite la generación de una clave criptográfica de 512 bits de longitud, sin la necesidad de enviarla por un medio inseguro. Y, por otro lado, la criptografía basada en ADN, que emplea dicha clave para el cifrado y descifrado de los mensajes dividiéndolos en bloques de longitud fija. Para cada uno de los algoritmos se realizan modelos de ataques y mediciones de su nivel de seguridad ante cada uno de ellos mediante análisis estadístico. Para ello, se ha realizado una investigación del estado actual de los dos algoritmos criptográficos, además de simulaciones y ataques en un ambiente controlado. Posteriormente, para el desarrollo de la aplicación móvil de chat se siguen los estándares y metodologías ágiles que permitan un desarrollo sostenible y resistente a cambios.

PALABRAS CLAVE:

- **CRIPTOGRAFÍA**
- **CRIPTOGRAFÍA NEURONAL**
- **TREE PARITY MACHINE**
- **CRIPTOGRAFÍA BASADA EN ADN**
- **EVALUACIÓN DE LA SEGURIDAD**

ABSTRACT

Nowadays, technologies that store and process information grow every day, unluckily the threats that endanger this information have also increased. Therefore, computer security becomes extremely important to protect the information from malicious people who seek to reach unauthorized access. Due to the fact that many traditional cryptographic algorithms have already been broken, the necessity for safer cryptographic techniques has emerged. Consequently, the present work proposes the implementation of two new cryptographic algorithms in a mobile chat application. On one hand, neural cryptography, which uses a modified structure of an artificial neural network called Tree Parity Machine, permits the generation of a cryptographic key of 512 bits in length, which does not need to be sent through an insecure medium. On the other hand, DNA-based cryptography uses this key to encrypt and decrypt messages by dividing them into blocks of fixed length. Models of attacks and measurements of their level of security have been developed for each one of the algorithms, by means of statistical analysis. For instance, an investigation of the current state of the two cryptographic algorithms has been done, as well as simulations and attacks in a controlled environment. Later, standards and agile methodologies that permit not only sustainable development, but also which have been proven to be invulnerable to changes are followed in order to design the mobile chat application.

KEYWORDS:

- **CRYPTOGRAPHY**
- **NEURAL CRYPTOGRAPHY**
- **TREE PARITY MACHINE**
- **DNA-BASED CRYPTOGRAPHY**
- **SECURITY EVALUATION**