Resumen

El cuestionamiento de las seguridades existentes en la transferencia y comunicación de datos es actualmente uno de los temas más relevantes en el ámbito tecnológico, el uso diario del internet es inevitable e indispensable como revisar el correo electrónico, realizar transacciones bancarias y visitar las redes sociales.

En el desarrollo de este proyecto se han analizado los sistemas criptográficos simétricos y asimétricos, los primeros también conocidos como de clave privada, son utilizados con una sola clave que cifra y descifra los mensajes. La principal seguridad se centra en la clave que debe ser robusta.

La criptografía asimétrica o de clave pública utiliza un par de claves, una pública y una privada con las que se cifran en la emisión y se descifra en la recepción los mensajes. Una de las principales ventajas de este tipo de criptografía es que no se comparte la clave privada que es otorgada por la entidad de certificación.

Una infraestructura de clave pública (PKI) es una combinación de hardware, software, políticas y normas de funcionamiento para la entrega de certificados digitales que identifican a un usuario, con la que se obtiene una comunicación segura, además proporciona: no repudio, confidencialidad, integridad y autenticidad en el proceso de comunicación. Con estos certificados se puede firmar documentos e incluso cifrar los datos para ser enviados.

PALABRAS CLAVE:

- **CRIPTOGRAFÍA SIMÉTRICA**
- **CRIPTOGRAFÍA ASIMÉTRICA**
- **ALGORITMOS**

Abstract

The questioning of the existing securities in the transfer and communication of data is currently one of the most relevant issues in the technological field, the daily use of the Internet is inevitable and essential, such as checking email, performing bank transactions and visiting social networks.

In the development of this project, the symmetric and asymmetric cryptographic systems have been analyzed, the former also known as private key, they are used with a single key that encrypts and decrypts messages. The main security is focused on the key, so it must be robust.

Asymmetric or public key cryptography uses a pair of keys, one public and one private, with which messages are encrypted when they are sent and decrypted when they are received. One of the main advantages of this type of cryptography is that the private key that is granted by the certification authority is not shared.

A public key infrastructure (PKI) is a combination of hardware, software, policies and operating standards for the delivery of digital certificates that identify a user, with which secure communication is obtained, it also provides non-repudiation, confidentiality, integrity and authenticity in the communication process. With these certificates you can sign documents and even encrypt the data to be sent.

KEYWORDS:

- **SYMMETRIC CRYPTOGRAPHY**
- **ASYMMETRIC CRYPTOGRAPHY**
- **ALGORITHMS**