UNIVERSIDAD DE COSTA RICA
ESCUELA DE INGENIERÍA ELECTRICA
ESTRUCTURAS ABSTRACTAS DE DATOS Y ALGORITMOS
PARA INGENIERÍA
PROPUESTA LIBRERÍA CRIPTOGRÁFICA EN C++
GEYKE93

ESCUELA DE INGENIERIA ELECTRICA
UNIVERSIDAD DE COSTA RICA

GABRIEL JIMÉNEZ LEIVA B23466
CARLA VEGA JARQUÍN B06763

1 Justificación

La aparición de la informática y el uso masivo de las comunicaciones digitales han producido un número creciente de problemas de seguridad. Las transacciones que se realizan a través de la red pueden ser interceptadas. La seguridad de esta información debe garantizarse. Este desafío lleva al estudio de los algoritmos, protocolos y sistemas que se utilizan para proteger la información y dotar de seguridad a las comunicaciones y a las entidades que se comunican. Los criptógrafos investigan, desarrollan y aprovechan técnicas matemáticas que les sirven como herramientas para conseguir sus objetivos.

2 Metodología

En este trabajo se busca partir del método de encriptación basado en los números primos y ejemplificar sus implementaciones en la criptografía antigua y la moderna. Dentro de esta última, estudiaremos a Ronald Linn Rivest y NSA (National Security Agency) que han sido pioneros de la época y quienes cuyo trabajo ha cambiado y clasificado la criptografía a través métodos que pensamos utilizar para la creación de la librería que es el fin del proyecto.

2.1 Tabla de algoritmos

Encriptacion simétrica	Encriptacion asimétrica	Hash function
AES (Rijndael)	RSA	SHA2(256-512)

Table 1: Métodos de encriptación

3 Objetivos

3.1 Objetivo General

Crear una librería de encriptacion que proporcione métodos de encriptación simétrica (AES), asimétrica (RSA) y funciones hash (SHA2).

3.2 Objetivos Específicos

- Implementar un algoritmo de encriptación y desencriptación simétrica AES (Rijndael) y otro asimétrica RSA utilizando conocimientos en el lenguaje de programacion C++: operaciones booleanas, funciones algebraicas, cifrado por bloques y otras herramientas útiles para la criptografía.
- Implementar una función hash SHA2, tanto en su versión SHA-256 para sistemas de 32 bits como SHA-512 para 64 bits.
- Mencionar los algoritmos criptográficos y funciones hash de librerías como Crypto++, Beecrypt y hashlib++.

- Estudiar las implementaciones de algoritmos criptográficos y funciones hash en un sistema como SSH.

4 Referencias

References

[1] http://beecrypt.sourceforge.net/doxygen/c++/index.html

[2] http://sourceforge.net/projects/cryptopp/?source=recommended

[3] http://sourceforge.net/projects/hashlib2plus/?source=recommended

[4] http://www.aescrypt.com/

[5] http://es.wikipedia.org/wiki/Ronald_Rivest

[6] http://es.wikipedia.org/wiki/SSH

[7] http://es.wikipedia.org/wiki/RSA

[8] http://es.wikipedia.org/wiki/Funci%C3%B3n_hash

[9] http://www.openssh.org/

[10] mirror.math.ku.edu/tex.../pgfgantt/pgfgantt.pdf

5 Anexo

La distribución del trabajo a través del diagrama de Gantt se planificó de la siguiente manera: