**Resumen:**

Este proyecto se base en la creación de una firma digital con un hash del cuco para la solución de las colisiones inherentes a una función hash implementando en el lenguaje de Python. Además, se usará el criptosistema RSA para la generación de claves tanto públicos como privados.

**Introducción**:

Conceptos:

Hash

Algoritmo que a partir de una entrada genera una salida alfanumérica de longitud fija, donde a partir de lo generado no se puede obtener la entrada inicial.

Hash del cuco

Es un método que resuelve las colisiones en hash creando dos funciones hash, lo que da la posibilidad de dos ubicaciones en la tabla hash.

Firma digital

Las firmas digitales es un certificado digital que emite la entidad para garantizar la autenticidad de la información, evitando el repudio del mensaje. Para lograr esto se toma el mensaje que se desea enviar, se le aplica una función hash y al resultado se le aplica la clave privada del usuario que envía el mensaje. Luego, el destinatario aplica una clave privada al resultado anterior y compara con el hash que obtenido del mensaje recibido. Si ambos resultados son iguales significa que el mensaje es auténtico.

Objetivos:

Generar firmas digitales a partir del hash del cuco.

**Estado del Arte:**

**Diseño del experimento:**

**Bibliografía:**

-Firma digital en la Web Semántica: Aplicación en la Biblioteca Digita

http://www.cyta.com.ar/biblioteca/bddoc/bdlibros/cifrado\_xml/cifrado\_xml.htm

-Firma digital basada en funciones HASH y un algoritmo criptográfico híbrido

<https://tesis.ipn.mx/handle/123456789/20224>

-Pgp Jacobo Bermúdez Fernández María Casanova Vázquez

<http://sabia.tic.udc.es/docencia/ssi/old/2006-2007/docs/trabajos/02%20-%20PGP.pdf>

## - El uso de RSA en la seguridad de la información

http://www.dma.fi.upm.es/recursos/aplicaciones/matematica\_discreta/web/aritmetica\_modular/rsa2.html