

“CriptoRA: Criptosistema biométrico mediante la huella dactilar”

Trabajo Terminal No. — — — — - — — —

Alumnos: *Aguilar Martínez Oswaldo, Arévalo Andrade Miguel Ángel, Castro Cruces Jorge Eduardo

Directores: Dr. Luna Benoso Benjamín, Dr. Flores Carapia Rolando

*e-mail: oaguilarm1201@alumno.ipn.mx

Resumen - En este trabajo se propone el desarrollo de un criptosistema biométrico (haciendo uso del rasgo distintivo de la huella dactilar) implementado como una aplicación de escritorio para Windows que realizará las operaciones de cifrado y descifrado, enfocado a archivos binarios genéricos y archivos de texto, dirigido a empresas de la iniciativa privada que buscan que en el proceso de divulgación de archivos se pueda comprobar la identidad del remitente y del destinatario, así como la visualización correcta del contenido de los archivos para el destinatario. Brindando los servicios criptográficos de confidencialidad y autenticación a los miembros activos de la organización, ofreciendo un nivel de seguridad contra miembros de otras organizaciones en el mercado interesados en obtener y utilizar los archivos con fines distintos a los establecidos por la organización original.

Para ello, primeramente se capturarán imágenes de la huella dactilar del usuario mediante un lector de huellas dactilares, posteriormente se utilizarán operadores morfológicos de dilatación y erosión para simplificar las imágenes conservando las características principales de la forma de los objetos que la componen, además de filtros como el de la mediana para eliminar ruido impulsivo, como resultado se obtendrá una matriz de datos correspondiente a la huella. Enseguida se utilizará la matriz de datos de la huella dactilar para alimentar al clasificador kNN (con $k = 1$), el cual arrojará como salida un vector de identificación del usuario al que le pertenece la huella dactilar y se le hará corresponder la llave privada generada mediante una función Hash SHA 512 que se aplicará al vector de características del usuario identificado, esta llave privada se usará con el criptosistema RSA para el cifrado de la llave del criptosistema simétrico AES generada de manera aleatoria, la cual cifrará el archivo para poder enviarlo, asimismo el criptosistema permitirá descifrar el archivo cifrado haciendo uso del algoritmo AES con la llave de 128 bits que será cifrada por el algoritmo RSA, adicionalmente se calculará la función Hash SHA 512 del archivo original cifrado y del archivo descifrado, para verificar su autenticidad.

Palabras Clave - Criptosistema biométrico, cifrado de archivos, RSA, AES, análisis de imágenes, reconocimiento de patrones

1. Introducción

En nuestro día a día, el uso de la criptografía está en todas partes. Por ejemplo, la usamos para enviar contraseñas de forma segura a través de vastas redes para compras en línea. Los servidores bancarios y los clientes de correo electrónico también guardan sus contraseñas mediante criptografía. La criptografía se utiliza para proteger toda la información transmitida en nuestro mundo conectado a IoT, para autenticar personas y dispositivos, y dispositivos en otros dispositivos [1].

Si todas las funciones o motores criptográficos dejaran de funcionar durante un día, la vida moderna tal como la conocemos se detendría. Las transacciones bancarias no se realizarían, el tráfico de Internet se detendría y los teléfonos móviles dejarían de funcionar. En este punto, toda nuestra información importante quedaría expuesta y luego podría ser explotada para hacernos un daño inimaginable a todos [1].

La criptografía es una forma esencial de evitar que eso suceda. Protege la información y las comunicaciones mediante un conjunto de reglas que permiten que sólo aquellos previstos, y nadie más, reciban la información para acceder a ella y procesarla [1].

El principio básico de un sistema criptográfico moderno es que ya no dependemos del secreto del algoritmo utilizado, sino del secreto de las llaves. Hay cuatro objetivos esenciales de un sistema criptográfico moderno:

Confidencialidad: la información nunca puede ser revelada a alguien que no esté autorizado para verla. Autenticación: antes de intercambiar información, identifique y luego autorice tanto al remitente como al destinatario[1].

En este proyecto nos adentraremos en los métodos criptográficos modernos como la criptografía simétrica, asimétrica e híbrida (una mezcla de las anteriores).

La criptografía simétrica se caracteriza por usar la misma clave para cifrar y descifrar el mensaje de datos, es decir se basa en un secreto compartido. Es por esta razón que la seguridad de este proceso depende de la posibilidad de que una persona no autorizada consiga la clave de sesión o clave secreta [2].

Por otra parte, la criptografía asimétrica es un método relativamente nuevo, en comparación con el cifrado simétrico. El cifrado asimétrico utiliza dos claves (llave pública y privada) para cifrar un texto sin formato las cuales se intercambian a través de Internet o una gran red. Estas dos claves se encuentran asociadas matemáticamente, la llave pública es pública porque es conocida por más personas que sólo el emisor y el receptor de un determinado mensaje, la cual solamente puede cifrar. La llave privada conocida de esta forma ya que se supone que se encuentra solo en poder del receptor es aquella que puede descifrar o hacer las dos cosas (cifrar y descifrar) [3].

La biometría humana es una ciencia que analiza las distancias y las posiciones entre las partes del cuerpo para poder identificar o clasificar a las personas. Hay varios rasgos biométricos y el de interés para este proyecto, son las huellas dactilares, pero existen otras alternativas como la cara, el iris, la mano, la retina o la firma [4]. La biometría proporciona mayores niveles de garantía a los proveedores de que una persona es real al verificar un rasgo tangible como algo que el usuario tiene y algo que es el usuario [4]. La mayoría de las contraseñas y PIN de los usuarios y la información de identificación personal probablemente se hayan visto comprometidas con una violación de datos, lo que significa que los estafadores pueden acceder a miles de millones de cuentas que conservan las respuestas a los métodos de autenticación tradicionales [4]. Este es el motivo por el que la biometría está entrando en nuestras vidas cotidianas y es necesario que los informáticos o ingenieros en general tengan unos mínimos conocimientos sobre la materia [4].

Actualmente, la tecnología ha evolucionado a tal punto que permite el acceso remoto a sistemas informáticos como plataformas, servicios digitales, redes de datos, servidores, etc. Todo ello a través de sistemas de autenticación que requieren credenciales de acceso. Sin embargo, a pesar de la robustez de los sistemas de autenticación, las contraseñas y llaves de acceso son cada vez más vulnerables, pues la técnica de los atacantes ya no va dirigida a destruir la seguridad de los sistemas, sino más bien a vulnerar la confidencialidad de las llaves [5]. Es por esto que la biometría y la criptografía funcionan con el fin de aportar más seguridad a los sistemas de tecnología de la información, haciendo que las personas sean las portadoras de las contraseñas sin que las conozcan al mismo tiempo [5].

La técnica de reconocimiento por huella dactilar consiste en comparar una huella dactilar con los modelos almacenados en una base de datos, tanto para identificar como para autenticar a un usuario. Uno de los puntos de referencia de este trabajo es que la huella dactilar tiene características únicas llamadas minucias que son puntos donde los bordes terminan o se dividen; con las cuales efectuaremos la identificación y autenticación del usuario [6]. En esta clase biométrica existe un mayor número de dispositivos que en otras clases de biometrías. Debido al descenso de los precios de estos dispositivos, esta técnica está ganando aceptación [6].

Por esta razón la aplicación que proponemos cifrará, descifrá, firmará y verificará archivos de texto y archivos binarios, la generación de las llaves privadas se realizará con base en la huella dactilar del usuario quien decidirá si cifrar o descifrar un archivo.

Enseguida se muestra una tabla comparativa de trabajos relacionados con este Trabajo Terminal, donde se remarcan las características de cada uno, su lugar de desarrollo y año de realización.

| Nombre | Características | Lugar de desarrollo | Año |
|-----------------------------|---|---------------------|------|
| Criptosistema aplicado a la | Criptosistema para la información de cuentas bancarias a partir del análisis de la imagen del | México, ESCOM | 2015 |

| | | | |
|--|--|---|---------------|
| seguridad de cuentas, bancarias basado en biometría del iris [7] | iris de una persona, que sea capaz de otorgar los servicios de autenticación del usuario, cifrado y descifrado de los datos de la cuenta. | | |
| Sistema de verificación biométrico vascular. [8] | Sistema que permite la autenticación mediante la captura y verificación del patrón vascular del dorso de la mano usando una cámara digital. | México, ESCOM | 2012 |
| Criptosistema biométrico basado en firma manuscrita. [9] | Criptosistema biométrico, en forma de cifrador de ficheros para Tablet PC. Utiliza su firma manuscrita en lugar de su contraseña. | Universidad Antonio de Nebrija, España. | 2006 |
| Criptosistema biométrico mediante la huella dactilar. | Criptosistema biométrico que utiliza imágenes de la huella dactilar y genera una llave de acceso que se cifrará con la ayuda del algoritmo RSA y cifrado de archivos de texto y binarios con el algoritmo AES. | México, ESCOM | En desarrollo |

Tabla 1. Comparativa de aplicaciones.

2. Objetivo

2.1. Objetivo general

- Desarrollar un criptosistema biométrico como una aplicación de escritorio (haciendo uso del rasgo distintivo de la huella dactilar) que realice las operaciones de cifrado y descifrado de archivos binarios y archivos de texto, ofreciendo los servicios de confidencialidad y autenticación.

2.2. Objetivos particulares

- Con base a un banco de imágenes de huellas dactilares proporcionadas por individuos, se identificarán las características únicas (minucias) de cada persona y con dichas características generar su llave privada.
- Diseñar un módulo de análisis de imágenes que nos permita procesar imágenes para su filtrado y mejoramiento haciendo uso del filtro de mediana con la finalidad de eliminar el ruido impulsivo y preservar los bordes en la imagen.
- Aplicar los operadores morfológicos dilatación y erosión a las imágenes de las huellas dactilares.
- Diseñar una metodología que genere un vector de características a partir de las minucias extraídas de la huella dactilar.
- Aplicar la función Hash SHA 512 al promedio obtenido de los vectores de características por persona para generar su llave privada, posteriormente generar la llave pública.
- Diseñar un módulo que cifra y descifra archivos de texto y archivos binarios utilizando AES-128.
- Unificar todos los módulos anteriores para crear un criptosistema biométrico mediante el uso del rasgo distintivo de la huella dactilar.

3. Justificación

Los criptosistemas biométricos unen la criptografía y la biometría para beneficiarse de las ventajas de ambos campos. La criptografía es la práctica y el estudio de técnicas para la comunicación segura en presencia de terceros o adversarios. Así que no es más que el arte de proteger la información transformándola (cifrándola) en un formato ilegible, llamado texto cifrado [10]. La biometría provee la medición y el análisis estadístico de las características físicas y de comportamiento únicas de las personas. La tecnología se utiliza principalmente para la identificación y el control de acceso [11]. En este trabajo, presentamos un criptosistema biométrico que utiliza la huella dactilar, con la finalidad de cifrar archivos de texto y binarios a partir de la llave generada por la matriz de datos producida por el rasgo biométrico. Esto provee confidencialidad de la información y puede mejorar la seguridad de la comunicación entre las aplicaciones cliente y los servidores. En esencia, cuando los datos están cifrados, incluso si una persona o entidad no autorizada obtiene acceso a ellos, no podrán leerlos.

En resumidas cuentas, los criptosistemas biométricos son una tecnología que representa una poderosa herramienta en la seguridad de los sistemas de información, cuya funcionalidad se basa en la determinación precisa de la identidad del individuo en el contexto de distintas áreas, tales como compartir recursos informáticos en red, otorgar acceso a instalaciones, realizar transacciones financieras a distancia, etc [12]; contextos en los cuales los usuarios generalmente eligen una clave muy sencilla o a veces difícil y fácil de olvidar.

La tecnología de identificación personal es de suma importancia en los sistemas de seguridad, hoy en día la autenticación mediante contraseñas, claves, tarjetas magnéticas no es del agrado de las personas ya que pueden ser robadas u olvidadas fácilmente [13]. Los sistemas basados en contraseñas requieren el recuerdo exacto de la contraseña que, dependiendo de la complejidad de esta, suele ser difícil de recordar para la cognición humana. Una alternativa son los sistemas de cifrado biométrico o criptosistemas, estos ofrecen soluciones en las que ya no se requiere la memorización de una contraseña, la clave se encuentra vinculada a un rasgo biométrico. Existe una necesidad urgente de desarrollar criptosistemas biométricos para aplicaciones prácticas [14] aunado al mayor uso de la tecnología e información desarrollado en medios digitales [15]. Es por ello, que, en este trabajo, se propone el desarrollo e implementación de una aplicación de escritorio que cifrará, descifrá, firmará y verificará archivos de texto y archivos binarios utilizando la huella dactilar como identificación biométrica ya que con base en estadísticas consultadas es la modalidad biométrica más reconocible en todo el mundo con un costo relativamente bajo [16].

4. Productos o resultados esperados

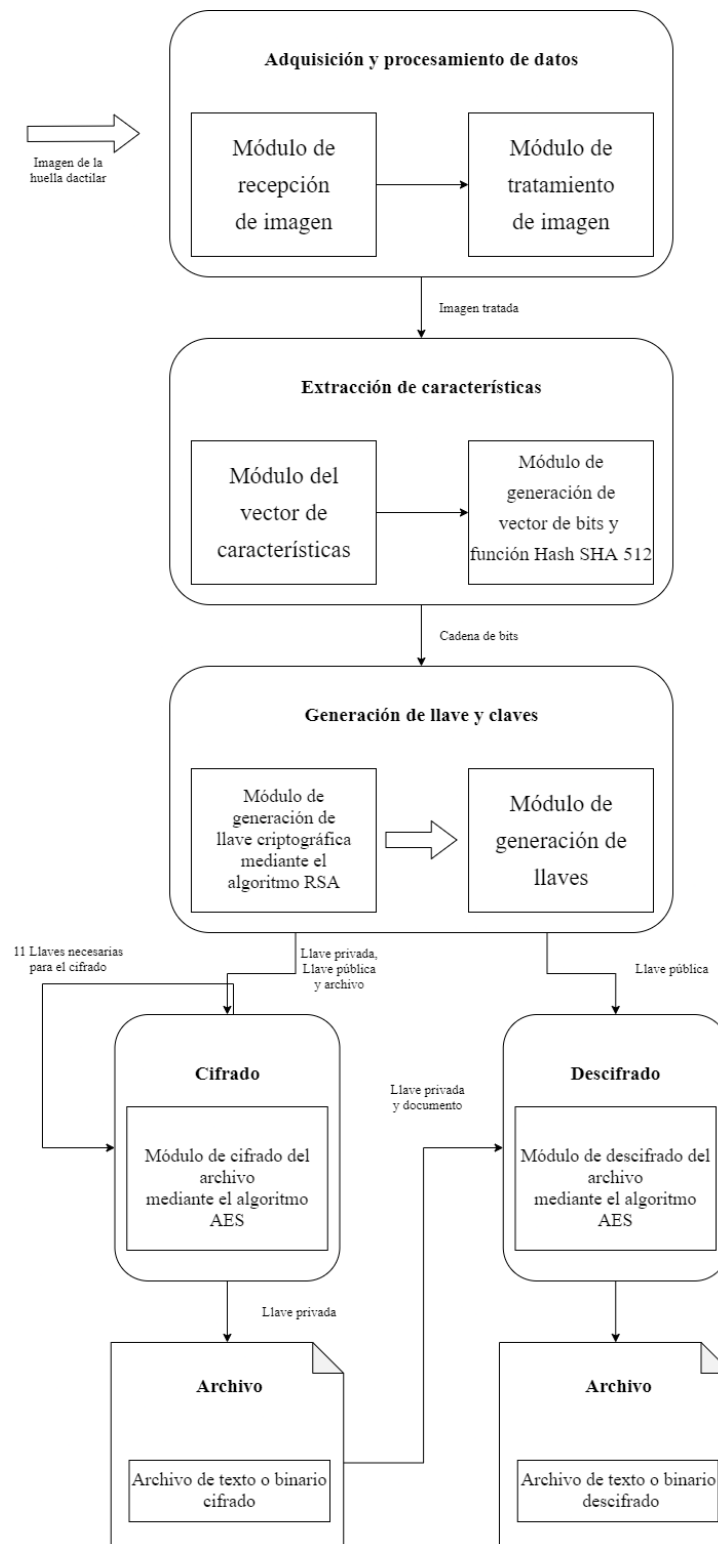


Figura 1. Arquitectura del sistema.

Módulo de recepción de imágenes: Obtiene y recibe las imágenes de la huella dactilar.

Módulo de mejoramiento de imagen: Trata las imágenes tomadas para eliminar el ruido en ellas y obtener una imagen más estilizada y manejable para su posterior uso.

Módulo de obtención de minucias: Obtiene las características que se reconocieron de la huella dactilar.

Módulo de generación de cadena de bits: Algoritmo que hace uso de la función Hash SHA 512 la cual genera una llave a partir de las características y de la información que se obtuvieron en los módulos anteriores.

Módulo de generación de llave criptográfica: Genera una llave criptográfica a partir de la cadena de bits generada por la función Hash SHA 512, con la huella dactilar.

Módulo de generación de claves: Tomando en cuenta la llave criptográfica generada crea claves.

Módulo de cifrado y descifrado: Cifra o descifra el archivo de texto o archivo binario con ayuda de las claves y la llave criptográfica, utilizando el algoritmo de cifrado AES.

Debido a que el sistema consta de varios prototipos antes de ser terminado, se espera conseguir lo siguiente, en el orden listado:

1. Prototipo de criptosistema biométrico generador de llave cifrada.
 - 1.1. Módulo de visualización y captura de imágenes.
 - 1.2. Módulo de mejoramiento y filtrado de imagen.
 - 1.3. Módulo de segmentación y clasificación del patrón de la huella dactilar.
 - 1.4. Módulo de generación de llave criptográfica.
 - 1.5. Módulo de generación de claves.
 - 1.6. Módulo de cifrado de llave.
2. Manual de usuario.
3. Manual técnico.

5. Metodología

Modelo de Prototipos o desarrollo evolutivo.

Se inicia con la definición de los objetivos globales para el software, luego se identifican los requisitos conocidos y las áreas del esquema en donde es necesaria más definición.

Debido a que se tienen diversos resultados esperados, consecutivos uno tras otro en su desarrollo e implementación, se usará esta metodología pues es básicamente prueba y error dado que si el resultado del prototipo no es el esperado se puede modificar en el siguiente prototipo. Permittiéndonos generar los prototipos que deseamos, documentando y probando con cada iteración nueva de la metodología como es principalmente la red neuronal continuando con la creación de la interfaz de la red social y así consecutivamente, con sus debidas correcciones en cada punto, hasta quedar satisfechos con el resultado y continuar hasta tener el prototipo final.

Los cambios iniciales durante el desarrollo de un proyecto son menos costosos que si se realizan en etapas tardías, como el prototipo puede cambiar varias veces la flexibilidad y adaptabilidad son su esencia, la pauta del cambio la da la retroalimentación, la cual nos permite conocer la opinión del usuario sobre cambios a la entrada o salida de un proceso, que al evaluarla nos permite obtener los requerimientos y mejorar el sistema.

El modelo de creación de prototipos tiene las siguientes seis fases SDLC de la siguiente manera:

Paso 1: Requisitos, recopilación y análisis. Un modelo de prototipos comienza con el análisis de requisitos. En esta fase, los requisitos del sistema se definen en detalle. Durante el proceso, los usuarios del sistema son entrevistados para saber cuál es su expectativa del sistema.

Paso 2: Diseño rápido. La segunda fase es un diseño preliminar o un diseño rápido. En esta etapa, se crea un diseño simple del sistema. Sin embargo, no es un diseño completo. Da una breve idea del sistema al usuario. El diseño rápido ayuda a desarrollar el prototipo.

Paso 3: Construir un prototipo. En esta fase, un prototipo real está diseñado en función de la información recopilada del diseño rápido. Es un pequeño modelo de trabajo del sistema requerido.

Paso 4: Evaluación inicial del usuario. En esta etapa, el sistema propuesto se presenta al cliente para una evaluación inicial. Ayuda a descubrir la fuerza y debilidad del modelo de trabajo. Los comentarios y sugerencias se recopilan del cliente y se proporcionan al desarrollador.

Paso 5: Prototipo de refinación. Si el usuario no está satisfecho con el prototipo actual, debe refinar el prototipo de acuerdo con los comentarios y sugerencias del usuario. Esta fase no se acabará hasta que se cumplan todos los requisitos especificados por el usuario. Una vez que el usuario está satisfecho con el prototipo desarrollado, se desarrolla un sistema final en función del prototipo final aprobado.

Paso 6: Implementar el producto y mantener una vez que el sistema final se desarrolle en función del prototipo final, se prueba y se despliega a fondo en la producción. El sistema sufre un mantenimiento de rutina para minimizar el tiempo de inactividad y evitar fallas a gran escala [17].

6. Cronograma

Ver anexo 1.

7. Referencias

- [1] Z.S. (2020, 2 abril). Cryptography: Why Do We Need It? Electronic Design. <https://www.electronicdesign.com/technologies/embedded-revolution/article/21127827/maxim-integrated-cryptography-why-do-we-need-it>
- [2] Rubén Daniel Varela Velasco, R. D. V. V. (2006, 10 julio). CRIPTOGRAFÍA, UNA NECESIDAD MODERNA. UNAM. http://www.revista.unam.mx/vol.7/num7/art56/jul_art56.pdf
- [3] Mendoza T., J. C. (2008). Demostración de cifrado simétrico y asimétrico. *Ingenius*, 3, 47-49. <https://doi.org/10.17163/ings.n3.2008.06>
- [4] Serratos, F. (2008). La biometría para la identificación de las personas. *Universitat Oberta de Catalunya*, 8-20 https://www.sistemamid.com/panel/uploads/biblioteca/2015-03-22_12-05-01117594.pdf
- [5] Rodríguez, J. D. P. (2015). Algoritmo de generación de llaves de cifrado basado en biometría facial. *INVENTUM*, 10(19), 41-51. <https://revistas.uniminuto.edu/index.php/Inventum/article/view/1415>
- [6] León P., Susan K. "Avances en técnicas biométricas y sus aplicaciones en seguridad" Universidad de Carabobo, Venezuela, 2011. [paper_de_tecnicas_biometricas\(alfa-redi.org\)](http://paper.de_tecnicas_biometricas(alfa-redi.org))
- [7] J. Fuentes, G. Moreno. "Criptosistema aplicado a la seguridad de cuentas bancarias basado en biometría del iris". Tesis. ESCOM, Instituto Politécnico Nacional. 2015.
- [8] E. Carrasco, D. Fuentes, C. Benitez, F. Hernández. "Sistema de verificación biométrico vascular". Trabajo Terminal. Escom, IPN. CDMX, 2012.
- [9] M. Freire. "Desarrollo de un criptosistema biométrico basado en firma manuscrita". Universidad Antonio de Nebrija, España, 2006.
- [10] Handbook of research on computational intelligence for engineering science and business, Hershey, PA, USA:IGI global, 2012.

- [11] Kholmatov A., Yanikoglu B. (2006) Biometric Cryptosystem Using Online Signatures. In: Levi A., Savaş E., Yenigün H., Balcısoy S., Saygın Y. (eds) Computer and Information Sciences – ISCIS 2006. ISCIS 2006. Lecture Notes in Computer Science, vol 4263. Springer, Berlin, Heidelberg.
https://doi.org/10.1007/11902140_102
- [12] J. Nair.B.J. "A Review on Biometric Cryptosystems". IJLTET, vol. 6, 2015.
- [13] Balaji, Prasanalakshmi & Sampathkumar, Kannammal & Gomathi, B. & Deepa, K. & Sridevi, R.. (2012). Biometric Cryptosystem Involving Two Traits And Palm Vein As Key. Procedia Engineering. 30. 303-310. 10.1016/j.proeng.2012.01.865.
- [14] Imamverdiyev, Y., Teoh, A., & Kim, J. (2013). Biometric cryptosystem based on discretized fingerprint texture descriptors. Expert Syst. Appl., 40, 1888-1901.
- [15] Kuzminykh, Ievgeniia & Ghita, B.V. & Shiaeles, Stavros. (2020). Comparative Analysis of Cryptographic Key Management Systems. 10.1007/978-3-030-65729-1_8.
- [16] Morais, L. (2020, 6 mayo). Biometric Data: Increased Security and Risks. 2020-05-06 | Security Magazine. <https://www.securitymagazine.com/articles/92319-biometric-data-increased-security-and-risks>
- [17] Alavi, M. "An Assessment of the Prototyping Approach to Information Systems Development". Communications of the ACM, Vol. 27, Núm. 6, junio 1984, pp. 556-563

8. Alumnos y directores

CARÁCTER: Confidencial
FUNDAMENTO LEGAL: Artículo 11 Fracc. V y Artículos
108, 113 y 117 de la Ley Federal de Transparencia y Acceso
a la Información Pública.
PARTES CONFIDENCIALES: Número de boleta y teléfono.


Aguilar Martinez Oswaldo. - Alumno de la carrera de Ing.
En Sistemas Computacionales en ESCOM, Especialidad:
Sistemas, Boleta: 2013050634 , Tel. 5515546568 ,
email: vvaldoagm@gmail.com

Firma:  Recibí documento

Arévalo Andrade Miguel Ángel. - Alumno de la carrera de Ing.
En Sistemas Computacionales en ESCOM, Especialidad:
Sistemas, Boleta: 2015100089 , Tel. 5516057697 ,
email: miguelarevalo1999@gmail.com

Firma:  Recibí documento


Castro Cruces Jorge Eduardo. - Alumno de la carrera de Ing.
En Sistemas Computacionales en ESCOM, Especialidad:
Sistemas, Boleta: 2015080213, Tel. 5521526884, email:
georgecastrocruces1515@gmail.com

Firma:  Recibí documento

Luna Benos Benjamín. - Lic. En Física y Matemáticas por
la ESFM, maestría y doctorado en Ciencias de la Computación
por el CIC. Actualmente profesor-investigador de la ESCOM
del IPN; Áreas de interés: Reconocimiento de patrones, análisis
de imágenes, morfología matemática; e-mail: blunab@ipn.mx

Firma:  Recibí documento

Rolando Flores Carapia. - Profesor en el CIDETEC del IPN.
Es miembro del Sistema Nacional de Investigadores nivel I.
Doctorado en Ciencias de la Computación por el CIC.
Áreas de interés: Procesamiento de imágenes, criptografía
y seguridad informática. e-mail: rflcarapia@yahoo.com

Firma:  R. Recibí documento.

Anexo 1: Cronogramas individuales

TT No.: — — — — —

Nombre del alumno: Aguilar Martinez Oswaldo

Título del TT: CriptoRA

| Actividad | A G O | S E P | O C T | N O V | D I C | E N E | F E B | M A R | A B R | M A Y | J U N |
|--|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|
| Fase 1: Análisis del sistema | | | | | | | | | | | |
| Introducción y estado del arte | | | | | | | | | | | |
| Marco Teórico (Reconocimiento de patrones) | | | | | | | | | | | |
| Análisis de riesgos | | | | | | | | | | | |
| Estudios de factibilidad y disponibilidad de recursos | | | | | | | | | | | |
| Análisis de requerimientos, procesos y pasos a seguir. Casos de uso, descripción de actividades en cada proceso. | | | | | | | | | | | |
| Correcciones y retroalimentación | | | | | | | | | | | |
| Fase 2: Diseño y desarrollo del sistema | | | | | | | | | | | |
| Diseño rápido del sistema | | | | | | | | | | | |
| Revisión del diagrama de bloques y modelado en UML. (Funcionamiento interno del criptosistema) | | | | | | | | | | | |
| Revisión del diagrama de clases y modelado en UML. (Representar las clases que se programaran en realidad, los objetos principales o la interacción entre clases y objetos.) | | | | | | | | | | | |
| Diagrama de secuencia y modelado en UML. (Procesos y objetos que coexisten simultáneamente, y los datos intercambiados entre ellos para ejecutar una función antes de que la línea de vida termine) | | | | | | | | | | | |
| Descripción del desarrollo y la implementación del criptosistema biométrico | | | | | | | | | | | |
| Correcciones y retroalimentación | | | | | | | | | | | |
| Preparación para presentación en TT1 (Elaboración de documentos a presentar) | | | | | | | | | | | |
| Presentación TT1 | | | | | | | | | | | |
| Fase 3: Programación de los módulos | | | | | | | | | | | |
| Construcción de prototipo inicial | | | | | | | | | | | |
| Módulo de visualización y captura de imágenes de la huella dactilar | | | | | | | | | | | |
| Módulo de mejoramiento de imagen y aplicación de filtros (Filtro mediana) | | | | | | | | | | | |

[illegible]

TT No.: — — — — —

Nombre del alumno: Arévalo Andrade Miguel Ángel
Título del TT: CriptoRA

[illegible]

Nombre del alumno: Castro Cruces Jorge Eduardo

Título del TT: CriptoRA

| Actividad | A G O | S E P | O C T | N O V | D I C | E N E | F E B | M A R | A B R | M A Y | J U N |
|--|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|
| Fase 1: Análisis del sistema | | | | | | | | | | | |
| Introducción y estado del arte | | | | | | | | | | | |
| Marco Teórico (Análisis de imágenes y morfología matemática) | | | | | | | | | | | |
| Análisis de vulnerabilidades y amenazas | | | | | | | | | | | |
| Estudios de factibilidad y disponibilidad de recursos | | | | | | | | | | | |
| Análisis de requerimientos, procesos y pasos a seguir. Casos de uso, descripción de actividades en cada proceso. | | | | | | | | | | | |
| Correcciones y retroalimentación | | | | | | | | | | | |
| Fase 2: Diseño y desarrollo del sistema | | | | | | | | | | | |
| Análisis del diagrama de bloques y modelado en UML. (Funcionamiento interno del criptosistema) | | | | | | | | | | | |
| Análisis del diagrama de clases y modelado en UML. (Representar las clases que se programaran en realidad, los objetos principales o la interacción entre clases y objetos.) | | | | | | | | | | | |
| Diagrama de secuencia y modelado en UML. (Procesos y objetos que coexisten simultáneamente, y los datos intercambiados entre ellos para ejecutar una función antes de que la línea de vida termine) | | | | | | | | | | | |
| Descripción del desarrollo y la implementación del criptosistema biométrico | | | | | | | | | | | |
| Correcciones y retroalimentación | | | | | | | | | | | |
| Preparación para presentación en TT1 (Elaboración de documentos a presentar) | | | | | | | | | | | |
| Presentación TT1 | | | | | | | | | | | |
| Fase 3: Programación de los módulos | | | | | | | | | | | |
| Módulo de visualización y captura de imágenes de la huella dactilar (Aplicación de operaciones morfológicas de dilatación y erosión) | | | | | | | | | | | |
| Módulo de mejoramiento de imagen y aplicación de filtros (Aplicación de filtro de mediana) | | | | | | | | | | | |
| Módulo de extracción de características de la huella dactilar a partir de la matriz de datos. | | | | | | | | | | | |

| | | | | | | | | | | | | | |
|---|--|--|--|--|--|--|--|--|--|--|--|--|--|
| Inspección del módulo de clasificación con el algoritmo kNN | | | | | | | | | | | | | |
| Inspección del módulo de cifrado y descifrado RSA y AES (Función Hash SHA 512) | | | | | | | | | | | | | |
| Pruebas de integración, pruebas no funcionales y retroalimentación | | | | | | | | | | | | | |
| Resultados, mejoras al prototipo y nuevas funcionalidades | | | | | | | | | | | | | |
| Construcción de prototipo de refinación | | | | | | | | | | | | | |
| Fase 4: Resultados y pruebas del sistema | | | | | | | | | | | | | |
| Manual de usuario | | | | | | | | | | | | | |
| Manual técnico (Morfología matemática, análisis de imágenes, reconocimiento de patrones) | | | | | | | | | | | | | |
| Pruebas unitarias y retroalimentación | | | | | | | | | | | | | |
| Resultados, mejoras al prototipo y nuevas funcionalidades | | | | | | | | | | | | | |
| Preparación para presentación en TT2 | | | | | | | | | | | | | |
| Presentación TT2 | | | | | | | | | | | | | |