Algoritmos criptográficos ligeros para aplicaciones de seguridad en expediente clínico electrónico.

Light cryptographic algorithms for security applications in electronic clinical records.

Luis Alberto Espinosa Calvo (1).
Estudiante, Instituto Tecnológico Nacional de México campus Tuxtla Gutiérrez.
luisespinosacalvo@gmail.com.

Miguel Morales Sandoval (2). Centro de Investigación y de Estudios Avanzados del Instituto Politécnico Nacional Unidad Tamaulipas. mmorales@tamps.cinvestav.mx.

Aida Guillermina Cossío Martínez* (3). Instituto Tecnológico Nacional de México campus Tuxtla Gutiérrez.
acossio_m@yahoo.com.mx.

*corresponding author.

Artículo recibido en noviembre 11, 2019; aceptado en diciembre 09, 2019.

Resumen.

En la actualidad la mayoría de las instituciones médicas están tendiendo hacia el uso de los expedientes clínicos electrónicos, estas instituciones en su mayoría cuentan con equipos computacionales limitados y con características que si no obsoletas, son bajas. El manejo electrónico de los expedientes requiere de dos consideraciones muy importantes la seguridad y el consumo computacional; en este sentido existen algoritmos criptográficos ligeros que permiten alcanzar algunas características de seguridad como autenticación, integridad, y confidencialidad de la información teniendo como objetivo también utilizar la mínima cantidad de recursos posibles.

Palabras clave: algoritmos criptográficos ligeros, consumo computacional, expediente clínico electrónico, desempeño, seguridad.

Abstract.

Nowadays, the most medical institutions are tending to the use of electronic health records, these institutions mostly have limited computer equipment with features that if not obsolete, they are low. The electronic handling of the records requires two very important considerations; namely security and computational consumption; In this sense, there are lightweight cryptographic algorithms that allow us to achieve certain security features such as authentication, integrity, and confidentiality of the information, and aiming to use the minimum amount of possible resources.

Keywords: light cryptographic algorithms, computational consumption, electronic health record, performance, security.

1. Introducción.

De acuerdo al sistema nacional de salud en el manual del expediente clínico electrónico se define al expediente clínico electrónico "como el conjunto de información ordenada y detallada que recopila cronológicamente todos los aspectos relativos a la salud de un paciente y a la de su familia en un periodo determinado de su vida".

Cuando se habla sobre expedientes clínicos electrónicos (ECE), se hace referencia al envió de la información a través de internet bajo la estructura cliente servidor usado para resguardar, accesar, modificar y compartir la información del seguimiento de cada uno de sus pacientes los cuales emplean algoritmos criptográficos convencionales, en algunos casos, consiguiendo un menor desempeño y una mala eficiencia.

Encontrando como alternativa el uso de los algoritmos criptográficos ligeros que permiten tener una mejor eficiencia y un menor consumo computacional, dichos algoritmos usados en el presente trabajo están regidos por la National Institute of Standards and Technology (NIST) que evalúa y estandariza a los algoritmos criptográficos ligeros para dispositivos limitados existentes en el mercado consiguiendo con el uso de ellos como confidencialidad, integridad y autenticación.

Según el senado de la republica coordinación de comunicación social en un boletín emitido el 27 de enero del 2019 nos dice que la información electrónica de los pacientes está disponible únicamente en la Ciudad de México, Morelos, Colima, Mexicali, Monterrey y Guadalajara, teniendo cada una de estos un sistema de operaciones propio.

Actualmente los hospitales llevan un control digital de la información de sus pacientes para lo cual se usa el estándar Fast Healthcare Interoperability Resources (FHIR) para el cuidado de la salud e intercambio de datos, publicado por Health Level Seven International (HL7).

De acuerdo con el estándar Fast Healthcare Interoperability Resources (FHIR) que se refiere al acceso del expediente clínico electrónico, éste debe estar limitado por mecanismos de seguridad entre los que se encuentra la autenticación y cifrado. Con fines de intercambio de información entre Prestadores de Servicios de Salud los Sistemas de Información de Registro Electrónico para la Salud (SIRES) deben implementar mecanismos de autenticación, de cifrado y de firma electrónica avanzada para mantener la seguridad del API RESTful (International, 2018).

En este proyecto y en apego a la estándar Fast Healthcare Interoperability Resources (FHIR), se busca explorar la pertinencia de usar cifrado criptográfico ligero para garantizar los servicios de seguridad del expediente clínico electrónico (ECE), de forma que el despliegue de una aplicación segura de manipulación del expediente clínico electrónico (ECE) bajo un contexto de computo móvil sea viable y tenga un bajo overhead.

El uso e implementación del expediente clínico electrónico ha sido impulsado por gobierno federal y estatal, sin embargo, a la fecha aún no se ha conseguido que éste se use ampliamente en los distintos sistemas de salud del país. Por ejemplo, en el estado de Tamaulipas en Cd. Victoria entre los años 2019 y 2022 será implementado el "Expediente Clínico Electrónico" el cual permitirá digitalizar los expedientes médicos de la Secretaria de Salud de Tamaulipas de modo que estos puedan ser consultados de manera simultánea tanto en centros de salud como hospitales, de acuerdo con lo revelado por la secretaria de salud de Tamaulipas, Jesús Molina Gamboa (Echartea, 2018).

El proyecto de estudio de algoritmos criptográficos ligeros para aplicaciones de seguridad en el expediente clínico electrónico será usado por cualquier persona que necesite el medio por el cual se puedan evaluar futuras propuestas de seguridad.

Para evaluar se usará una aplicación de software que modele la operación de un sistema de expedientes clínicos electrónicos (ECE) que al mismo tiempo permitirá agilizar diversos procesos de los sistemas de salud con el cual se pondrán a pruebas los puntos de seguridad en la creación, almacenamiento y uso del mismo, para garantizar la seguridad de los datos de sus pacientes reduciendo al mismo tiempo el consumo producido en el equipo de cómputo.

El prototipo ayuda en los siguientes puntos:

- Para el análisis de algoritmos de seguridad y será el medio para evaluar nuevas propuestas de seguridad de datos.
- Manipular el expediente clínico electrónico por distintos actores de un sistema de salud (pacientes, enfermera, medico, especialista, farmacia, entre otros muchos), ubicados posiblemente en distintos lugares geográficos.
- Gestionar y registrar las transacciones de un expediente clínico electrónico (ECE), bajo en entorno de operación distribuido.
- Operar con recursos computacionales bajos.

2. Método.

Algoritmos criptográficos ligeros.

Los algoritmos criptográficos ligeros usados para el desarrollo del prototipo de expediente clínico electrónico están diseñados para trabajar con dispositivos de bajo rendimiento, dichos algoritmos buscan asegurar la información sin perder el óptimo desempeño y asegurar un consumo computacional bajo.

Los datos utilizados para hacer las pruebas de rendimiento para cada uno de los algoritmos criptográficos ligeros están conformados por los datos del paciente y el reporte diagnóstico contenido en el expediente clínico electrónico.

Los datos contenidos del paciente son los datos demográficos e información relevante acerca del paciente, los datos contenidos en el reporte diagnostico son las interpretaciones diagnosticas, que incluye el contexto clínico.

De acuerdo al proyecto se consideraron algoritmos criptográficos ligeros que trabajan con el cifrado por bloques como son el caso de XTEA, Blowfish, AES, GOST25147 los cuales nos proporcionan tamaños de bloques más pequeños que los algoritmos criptográficos convencionales, tamaños de llaves mas pequeños que van desde los 80 bits pero de acuerdo a lo establecido en la NIST se usaron llaves de 112 bits, rondas más simples con una preferencia de S-box de 8 bits y programar llaves más simples que generan sub claves sobre la marcha que impiden el aumento de memoria, la latencia y el consumo de energía.

Dichos algoritmos son usados en el prototipo para cifrar la información JSON que es generada de forma automática por HAPI FHIR con los datos obtenidos de las interfaces de usuario de manera que la información pasa por el algoritmo regresando datos alfanuméricos como se muestra en la
figura 6 en el apartado de “content” que sirven como una representación del cifrado para observar el cambio de los datos enviados.

Tipos de algoritmos criptográficos ligeros.

Los algoritmos criptográficos se dividen en tres grandes familias: Primitivas criptográficas (sin clave), criptografía de clave simétrica, criptografía de clave pública como se muestra en la
figura **1**.

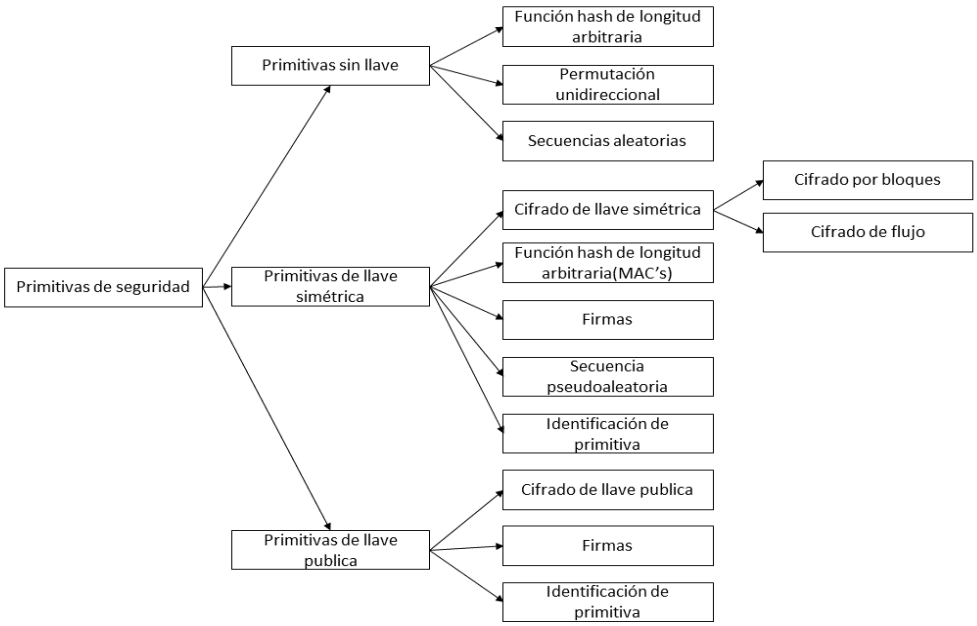

Figura 1. Vista general de la familia de algoritmos criptográficos.

Cada una de las tres grandes familias son evaluadas bajo los siguientes criterios:

1. Nivel de seguridad: A menudo se mide en términos de del tamaño de las claves usadas en los algoritmos criptográficos, en número de bits. Actualmente, el nivel de seguridad recomendado para un algoritmo simétrico o de clave privada es de 128-bits, para un algoritmo asimétrico o de clave pública es de 2048-bits y para una primitiva criptográfica como las funciones hash, el tamaño de su salida debe ser de 256-bits.
2. Funcionalidad: Se refiere al tipo de servicio de seguridad que el algoritmo ofrece. En el caso de los algoritmos simétricos o de clave probada, éstos ofrecen solo el servicio de confidencialidad. Los algoritmos asimétricos o de clave pública ofrecen el servicio de autenticación, integridad y no repudio. Las primitivas criptográficas como las funciones hash pueden proveer el servicio de confidencialidad.
3. Métodos de operación: Está determinado por la forma en la que los algoritmos procesan los datos de entrada. Generalmente, todos los algoritmos criptográficos son iterativos, operan mediante distintas rondas y en cada una se aplican algoritmos no determinísticos. Los cifradores pueden operar por bloques (los datos se dividen en bloques de tamaño fijo y cada uno se procesa a la vez) o por flujo (los datos se procesan al vuelo, por ejemplo, en las comunicaciones tipo streaming). De igual forma, existen diversos modos de operación, principalmente en los cifradores simétricos, por ejemplo, el modo CBC usa el resultado del bloque cifrado previo para cifrar el bloque siguiente.
4. Desempeño: esta hace referencia al rendimiento del algoritmo criptográfico, por ejemplo, cuantos bits por segundo puede procesar.
5. Facilidad de implementar: hace referencia a la dificultad de implementar el algoritmo a nivel de software y hardware.

- **Primitivas sin clave o hash.**

  El hash es la transformación de una cadena de caracteres generalmente más corto que la cadena original. Estas primitivas tienen como entrada un conjunto de elementos, que suelen ser cadenas de bits que pasan por un algoritmo matemático que asigna datos de tamaño arbitrario a una cadena de bits de longitud fija, y de tal forma que a partir de dicha cadena no se pueden recrear los datos de entrada.

a) **Propiedades:** Las funciones criptográficas hash se utiliza para mantener la seguridad de los datos y reducirlos a un tamaño razonable para posteriormente validar la misma información (Nathan Landman, Christopher Williams, & Eli Ross, 2019).

Cumpliendo con las siguientes propiedades mencionada por Reyna García Belmont para considerarse seguras:

- Unidireccional: Imposibilidad de encontrar el mensaje a partir del hash.
- Compresión: El mensaje de cualquier longitud se reduce a una longitud fija al ser convertido en un hash.
- Facilidad de cálculo: facilidad de calcular la función hash a partir del mensaje.
- Difusión: Complejidad en la función de todos los bits del mensaje evitando modificaciones en los bits, en caso de presentar modificaciones la mitad de sus bits se ve afectado.
- Colisión débil: se refiere a encontrar una segunda entrada que que tenga la misma salida que la primera entrada es decir x para encontrar $x' \neq x$ tal que $h(x) = h(x')$.
- Colisión fuerte: Se refiere a encontrar dos entradas distintas x, x' que se agrupa en la misma salida, es decir, que $h(x) = h(x')$.

b) **Ventajas:** La salida de los caracteres siempre tiene la misma longitud, por lo que esto se puede tener en cuenta al procesar o almacenar el resumen del mensaje. Algo que se resalta es que la salida es mucho más corta que la entrada, por lo que el procesamiento y el almacenamiento se pueden hacer mucho más rápido.

c) **Desventajas:** Una de las desventajas de estos algoritmos son que las colisiones hash son inevitables, esto es, que dos mensajes generen el mismo código hash. A medida que la longitud del código hash es más grande, es menos probable que exista una colisión. Durante mucho tiempo se usó la función hash SHA-1, la cual genera códigos hash de 160-bits. Esto supone que se pueden calcular 2^{160} distintos códigos hash o, dicho de otra forma, que la función hash solo soporta un máximo de 2^{160} mensajes diferentes antes de que inevitablemente exista una colisión. Actualmente, la longitud de hash recomendada para evitar colisiones es de al menos 224-bit y recomendablemente, de 256-bits.

- **Primitivas de clave simétrica.**

Se considera un esquema de cifrado que consiste en los conjuntos de transformación de datos cifrados y datos descifrados $\{E_e : e \in K\}$ y $\{D_d : d \in K\}$ donde de K denota a un conjunto llamado espacio clave (key space), y donde cada elemento $e \in K$ únicamente determina un bisección de M (el espacio del mensaje) a C(el espacio de texto cifrado) denotado por E_e donde $E_e$es llamada un función de cifrado, siendo E_e únicamente reservado para recuperar texto plano de cada texto cifrado distinto. Para cada $d \in K$, D_d denota una bisección de C (el espacio del texto cifrado) a M (el espacio del mensaje), (ejemplo. $D_d : C \rightarrow M$) donde D_d es llamado una función de descifrado (A. Menezes, 1996).

a) **Propiedades:**
Las primitivas de claves simétricas son:

- Ligeras.
- Rápidas.
- Compacto.

b) **Ventajas:**
A continuación, se dirán algunas de las ventajas de las primitivas de clave simétrica:

- Los criptosistemas que usas cifrados simétricos son más rápidos.

- Los datos cifrados son más seguros, a un que los datos sean interceptados no podrán ser legibles si no se obtiene la llave, la posibilidad de descifrado es nula.
- Utiliza autenticación de contraseña para comprobar la identidad del receptor en los criptosistemas simétricos.
- El mensaje solo es accesible a un solo tipo de llave.

c) **Desventajas:**
La desventaja principal es el establecimiento de los secretos compartidos que deben usar tanto el emisor como el receptor. Estas claves pueden establecerse off-line, pero es altamente inviable hacer esto. La otra opción es establecer las claves por un canal seguro. De hecho, unos de los problemas mayores de la criptografía simétrica es encontrar un método eficaz para estar de acuerdo en el intercambio de claves seguras. Este problema se le llama el problema de distribución de claves.

- **Primitivas de clave pública o asimétrica.**

Este tipo de cifrado se usa un par de claves relacionadas entre sí, de tal forma que la clave privada invierte la operación realizada con la clave pública y viceversa. La generación de esta pareja de claves debe ser tal que a partir de la clave privada se puede crear la clave pública, pero no al revés. La relación entre la pareja de claves es de forma matemática. Un mensaje cifrado con la clave pública solo puede ser descifrado con la clave privada, la cual debe mantenerse siempre segura.

a) **Propiedades:**
Normalmente se manejan dos tipos de llaves una privada y otra publica, la pública es conocida por todo el mundo y la privada únicamente por el propietario, entonces no importa si se conoce la llave publica o el texto cifrado no se podrá obtener la clave privada que es independiente de la clave pública o del texto cifrado.
El cifrado asimétrico proporciona:
- Confidencialidad
- Integridad
- Autenticación
- No repudio

b) **Ventajas:**
Algunas de las ventajas de usar el cifrado asimétrico son los siguientes:
- No es necesario intercambiar llaves, por lo tanto, se elimina el problema de distribución de llaves.
- Las claves privadas no necesitan ser transmitidas o reveladas a alguien.

c) **Desventajas:**
La desventaja de las primitivas de clave pública es la relación matemática que debe existir entre la pareja de clave pública y privada y la dificultad para que a partir de la clave pública no se pueda derivar la clave privada, hace necesario usar problemas matemáticos difíciles y tamaños de llave relativamente grandes. Todo esto implica mayor tiempo de procesamiento para generar las claves, para las operaciones de cifrado y descifrado y para el almacenamiento. Para un nivel de seguridad similar, la longitud de una clave en cifrado de clave pública puede ser hasta 20 veces más grande que una clave en el cifrado simétrico.

3. Desarrollo.

El actual prototipo de expediente clínico electrónico fue desarrollado para tratar el tema de seguridad en un ambiente médico, una falla de acceso no autorizado permite a terceros modificar los datos del paciente que podría traer consecuencias tales como un tratamiento equivocado debido a que su historial médico fue alterado poniendo en riesgo la integridad y salud del paciente.

El proyecto se desarrolló en 4 etapas:

- Fase de inicio: En esta fase se identifican todas las entidades externas (personas y sistemas) que interactúan con el sistema y definir las interacciones.
- Fase de elaboración: desarrollo de la compresión del problema, establecer un marco de trabajo arquitectónico para el sistema, desarrollar el plan del proyecto. Al terminar la fase debemos de tener el modelo de requerimientos del sistema, una descripción arquitectónica y un plan de desarrollo del software.
- Fase de construcción: comprende el diseño del sistema, la programacion y las pruebas.
- Fase de transición: se ocupa de poner en un entorno abierto a diferentes circunstancias.

El prototipo desarrollado cifra la información para asegurar que no se tenga acceso no autorizado, consiguiendo resguardar la información mediante el uso de algoritmos criptográficos ligeros los cuales permiten obtener seguridad y un mejor rendimiento. Que a diferencia de los algoritmos convencionales estos permiten generar bloques de información más pequeños.

De los algoritmos criptográficos ligeros usados se obtiene el tiempo que se tarda en generar el expediente clínico electrónico como primera variable y hemos usado el consumo computacional como segunda variable.

A continuación, se describen las características del servidor con las que fueron hechos las pruebas son las siguientes:

- Dual-Core AMD Opteron(tm) Processor 2220
- 4 GB RAM
- 1 TB
- Ubuntu 14.06 LTS

Las características del cliente con las que fueron hechas las pruebas son las siguientes:

- Windows 10
- Procesador Intel Celeron
- Java 1.8
- 2 GB RAM

Se desarrollaron interfaces para obtener los datos del paciente para crear un expediente clínico electrónico digital usando HAPI FHIR.

Estas interfaces permitirán introducir información que posteriormente se cifrará utilizando cada uno de los algoritmos criptográficos y será enviada al servidor para así comprobar el tiempo en generar el expediente y el consumo computacional.

A continuación, se describen los pasos a seguir para introducir los datos del paciente a las interfaces desarrolladas:

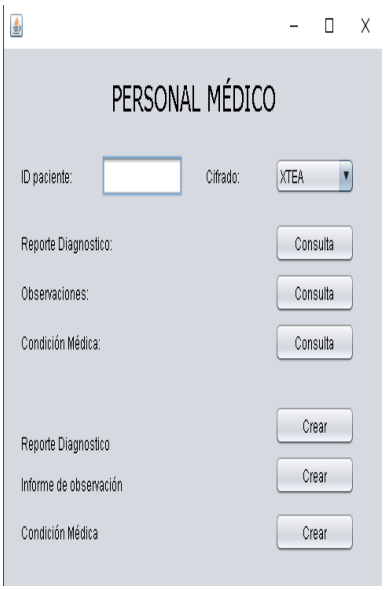

Figura 2. Menú de Personal Médico.

Como primer paso para usar el menú de personal médico debemos de presionar sobre el botón de crear reporte diagnostico sin asignar el ID del paciente en caso contrario este mostrara una pestaña para registrar los datos del paciente correspondientes al reporte diagnóstico.

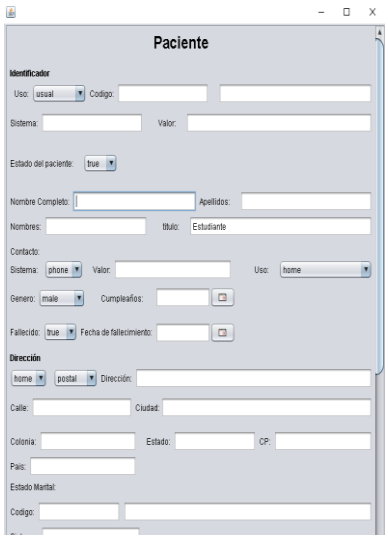

Figura 3. Formulario para registrar datos del paciente.

Una vez que la pestaña del paciente es mostrada, se llenará el formulario con los datos del paciente, los códigos requeridos serán introducidos de acuerdo a lo marcado por el estándar FHIR y se presionará siguiente para seguir con el formulario de reporte diagnóstico.

Figura 4. Interfaz gráfica de usuario.

Una vez que es mostrado el formulario de reporte diagnóstico se llenará con los datos pertenecientes al paciente y los códigos requeridos serán introducidos de acuerdo a lo marcado por el estándar FHIR, concluido el formulario se presionara al botón de enviar para generar el JSON y enviar al servidor.

El JSON generado durante el envío contendrá toda la información recolectada en los formularios como se muestra en la siguiente figura cuya estructura es dada automáticamente por HAPI FHIR.


```
{
  "resourceType": "DiagnosticReport",
  "id": "4955",
  "meta": {
    "versionId": "1",
    "lastUpdated": "2019-10-03T03:24:07.936-05:00"
  },
  "text": {
    "status": "generated",
    "div": "<div xmlns=\"http://www.w3.org/1999/xhtml\"><div class=\"hapiHeaderText\"> Acyclovir [Susceptibility] </div><table class=
\"hapiPropertyTable\"><tbody><tr><td>Status</td><td>APPENDED</td></tr><tr><td>Issued</td><td>03 octubre 2019 00:00:00</td></tr><tr><td
>Conclusion</td><td>conclusion del reporte diagnostico</td></tr></tbody></table></div>"
  },
  "contained": [
    {
      "resourceType": "Patient",
      "id": "1",
      "active": true,
      "name": [
        {
          "use": "usual",
          "text": "Luis EC",
          "family": "Espinosa",
          "given": [
            "Luis"
          ],
          "prefix": [
            "Estudiante"
          ],
          "period": {
            "start": "2019-10-03T00:00:00-05:00"
          }
        }
      ],
      "telecom": [
        {
          "system": "phone",
          "value": "1233080539",
          "use": "mobile",
          "rank": 1,
          "period": {
            "start": "2019-10-03T00:00:00-05:00"
          }
        }
      ],
```


Figura 5. Datos de Paciente y Reporte Diagnóstico.

Dicha estructura JSON es generada por HAPI FHIR nos permite seguir el estándar FHIR para posteriormente cifrar los datos del expediente clínico electrónico con los algoritmos criptográficos ligeros como XTEA, AES, Blowfish y GOST25147 transformándolo en un binario que contiene al paciente y al reporte diagnostico obteniendo un JSON de la siguiente manera para ser enviado al servidor como se muestra en la figura 6.


```
{
  "resourceType": "Binary",
  "id": "4954",
  "meta": {
    "versionId": "1",
    "lastUpdated": "2019-10-03T00:19:06.336-05:00"
  },
  "contentType": "application/json+fhir",
  "content": "BCLm6X62hYUJL937BDqW9aGnBu87/CLKizfyqhK8+QkXVtY37IJI+mFiXQ2d+77ASN2NXwrS7EvwqG3LbZcR8RPvRaS4Qb2dJRQNPKISgM/HQ7tvkT88sKrW
qN7otm9cGbcw9h8W/YBSbVYrQxLx8ilcALDK29s3iIuNAQlV+HB9eKUnGQnrGXxU50gEqLzeVDu4EBukt0cJKMO87fx6Om403dcgWFM5+KYT3FDn0DlmaMyYooaZ++KdBob79e
6KRJfvS/ABLittTEZ6/e8JRtSV9WLeGWucTnc/F2CQNu0tLLLeWhnBvxviL8NMKdaV38aI9pRmjje/9Vgbotl0S3XjtvugnsFKvz3R9Q+O1KmfZVvfaqt2/7WhYjT2mDSzsKnb
kvS2YUC404/HiYa0u36LBCoViyqhiIuNAQlV+HA51TxxuPnZ6UWK1ZblZcmk0y5rkoJSvUtfCSXZmLY9I9/GiPaUZo43v/VYG6LZdEtI47b7oJ7BSr890fUPjtSpn2Vb32qrdv
+XmQna7CSBBLjere4zo+qyU8/yI6s3D4WdipS7osEJ3i2yoZm16Ja097GxMHiLJmRPqbFjVsSarMTZ9WTmiG0WLbKhmbXolrTuRmo9TTfZmwFiEoh89yuy8SaLw75ZcKsWOst2
6RFS82FiXQ2d+77AgsHpBZbk5JspyH1gridaplPXPrKGBAtDyhEUxdMjLNLWNyGcz98W6xF/kcMDq+VzMbnOTsT2hifLtqR2MejXvkLpPnmzPS8RF+7kD2M74pcmObk9Kn304l
r6NHppsv9DfMZkcqyfERCPaUTb1ep6d+m9/MzwGQWFfsMZIuJCw1r1yeT1GNz0aef4YKnXA2QTB/IQ+ZOQjmH29Y8pK2afT+f3HE72jPFWE+9FpLhBvZ3NeTtvgix3LTgn0Nrw
iORv6RQFKR0aJqLvA88c3QJTzOyB4FJOSHUHyBBCexaY9Wi7JKpCIPrwr9VgZAvqwft2b3cPhhfncPfcA4fiZJAUoJdb9S7fOVw2vYPeQWnSLiAT+DAxhtIvKb7QzuLBfztUWB
h3gf9JP9/qszB0o412LdTNcdNFCdLJyhEUxdMjLNIbCA2P6yHaXctdciJcggyYBln+hMLVDX7HlrfxbQGcqtPL7yVuwAqtexmJ7xlfUHNDnXPGAzoDYLqKPyk82/IeEveJ7tld
XX6SqoOuqpyfP2VhQlOq/OPvCABcTH0/T7HREeBRx/5aJEHZmYrG4U8GwJq8+h75QfsphT+zeda2+pP0NeSPpVinFOOECx+EC757Xzcf9bhCGftVKnEc/hApYSt/NIAwR1iYYz
j+lcGVrJ44DQ4JP0rK3UpypNk/ehNZJcgoWDnJGJA5cK5KzB/Thlnqwr+r+4gzf1BMTqQEvnxHMN/0w355fiBzKYAmt04pZEIwvlA0Jhsqq7NRYdxgQyo9BcBm3FP/jT8jvSCg
QHMynBJEHF/J6b2TcnDypNNPYWV7a2ROHQ=="
}
```


Figura 6. Datos cifrados del expediente clínico electrónico.

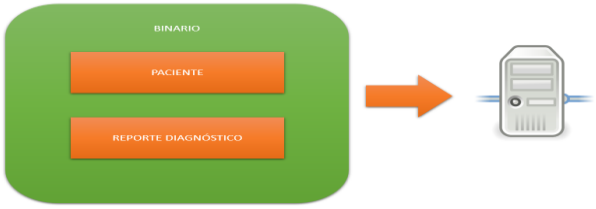

Figura 7. Representación gráfica del contenido binario enviado al servidor.

A continuación, se muestra los datos del tiempo que se tarda en generar el expediente clínico electrónico, recurso computacional consumido y el tamaño del expediente clínico electrónico que son enviados al servidor.

Tabla 1. Resultados de rendimiento del Expediente Clínico Electrónico.

Peso extra (MB)	Tipo de cifrado	Tiempo de latencia (milisegundos)	Consumo computacional (MB)	Tamaño del Expediente (MB)
0	Sin cifrar	4091	51	2.59
	AES	4688	47	2.59
	Blowfish	4794	47	2.59
	XTEA	5453	71	2.59
	GOST25147	5444	71	2.59
5	Sin cifrar	4748	314	11.8
	AES	5944	318	11.8
	Blowfish	5775	318	11.8
	XTEA	6293	322	11.8
	GOST25147	7672	369	11.8
10	Sin cifrar	4972	607	23.7
	AES	6135	611	23.7
	Blowfish	6121	611	23.7
	XTEA	6786	621	23.7
	GOST25147	8371	564	23.7
15	Sin cifrar	Tiempo excedido	-	35.5
	AES	Tiempo excedido	-	35.5
	Blowfish	Tiempo excedido	-	35.5
	XTEA	Tiempo excedido	-	35.5
	GOST25147	Tiempo excedido	-	35.5
	Sin cifrar	Tiempo excedido	-	47.4
	AES	Tiempo excedido	-	47.4

20	Blowfish	Tiempo excedido	-	47.4
	XTEA	Tiempo excedido	-	47.4
	GOST25147	Tiempo excedido	-	47.4

Como se puede observar en la tabla 1 debido a las limitaciones de nuestro gestor de base datos con la perdida de memoria en expedientes clínicos electrónicos con pesos superiores a 24 MB hemos podido observar que Blowfish es uno de los algoritmos que mejor rendimiento obtiene a medida que el expediente clínico electrónico es de mayor tamaño.

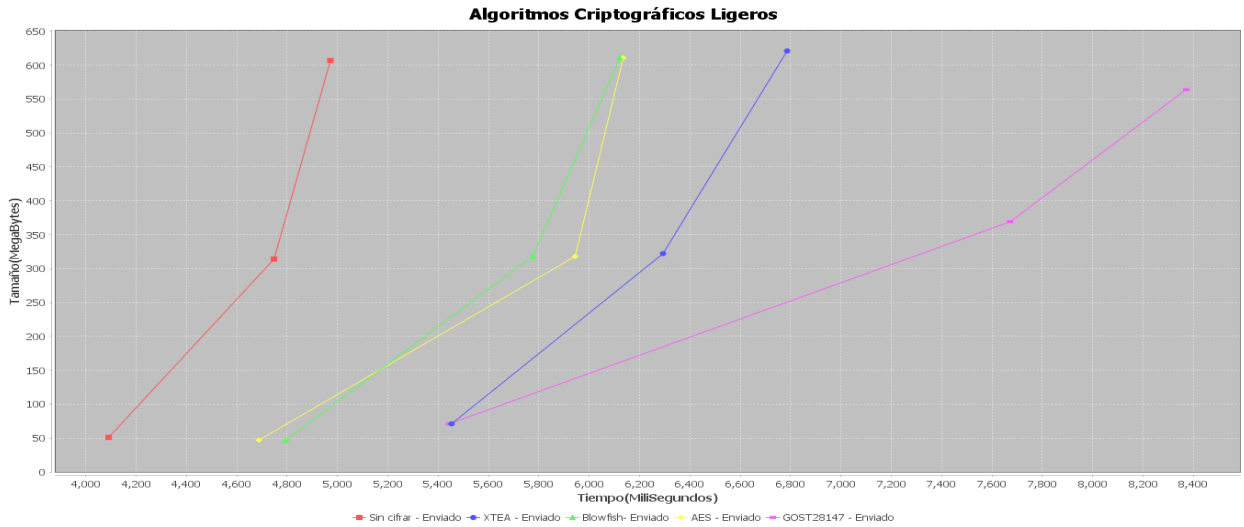

Figura 8. Grafica de resultados de los algoritmos criptográficos ligeros.

Y como se muestra en la figura 8 el algoritmo de mayor desempeño que se muestra en la gráfica es Blowfish teniendo un menor tiempo en procesamiento y un menor consumo computacional en comparación con los demás algoritmos criptográficos ligeros.

Conclusiones.

Los algoritmos criptográficos ligeros aseguran la información, pero elevan el consumo computacional a medida que el expediente clínico electrónico se eleva en tamaño notando que algunos de ellos no tienen un consumo tan elevado permitiendo asegurar la información sin tener que perder el desempeño original de la aplicación, observando que el cliente depende de la capacidad del servidor y los recursos disponibles para trabajar los datos de los pacientes, una limitación encontrada es el gestor de base de datos el cual solo nos permite trabajar con expedientes clínicos electrónicos de tamaños menor a 25 MB.

Por eso es importante considerar la robustez del sistema manejador de base de datos para no tener limitaciones como es el caso de Jetty el cual con datos superiores a 20 MB hay perdidas de memoria con la información recibida y almacenada en la base de datos.

Créditos.

Al Centro de Investigación y de Estudios Avanzados del Instituto Politécnico Nacional por permitirme desarrollar este proyecto.

Agradecimientos.

Le extiendo mi principal agradecimiento al Dr. Miguel Morales Sandoval y a la M.C. Aida Guillermina Cossio Martínez por el apoyo que me han brindado durante el desarrollo del proyecto.

Referencias Bibliográficas.

A. Menezes, P. v. (1996). *Handbook of Applied Cryptography.* no disponible: CRC Press.

Echartea, A. (20 de septiembre de 2018). Harán ´Expediente Clínico Electrónico´. Permitirá digitalizar documentos médicos. *El mañana*, pág. 1.

International, H. (27 de Diciembre de 2018). Obtenido de HL7 FHIR: https://www.hl7.org/fhir/security.html.

Nathan Landman, Christopher Williams, & Eli Ross. (19 de July de 2019). *BRILLIANT*. Obtenido de BRILLIANT.ORG: https://brilliant.org/wiki/secure-hashing-algorithms/

Información de los autores.

Luis Alberto Espinosa Calvo, Estudiante de ingeniería en sistemas computacionales, desarrollo de tesis en el CINVESTAV unidad Tamaulipas. Área de interés seguridad informática y desarrollo de software sobre plataformas Linux y Windows.

Miguel Morales Sandoval, es Doctor en Ciencias Computacionales, con líneas de investigación en Seguridad Informática, Esquemas y algoritmos criptográficos, Ingeniería de Software y de Hardware (FPGAs), Sistemas de información y Bases de Datos. Miembro del Sistema Nacional de Investigadores desde 2010, actualmente Investigador Nacional Nivel 1 (vigencia hasta 2019), con experiencia en docencia (licenciatura y posgrado), direcciones de tesis de posgrado y desarrollo de proyectos con financiamiento. Miembro adherente de la Academia Mexicana de Computación.

Aida Guillermina Cossío Martínez, es Maestra en Ciencias en Administración por el Instituto Tecnológico de Tuxtla Gutiérrez en 2002. Es profesora de tiempo completo del área de Ingeniería en Sistemas Computacionales desde 1994. Se especializa en la formulación y evaluación de proyectos, así como el emprendimiento y desarrollo de planes de negocio.