ALGORITMO BIDIRECCIONAL DE ENCRIPTACIÓN BASADO EN TLS, PHP Y JAVASCRIPT

WILMER HERNEY MUÑOZ GOMEZ
CARLOS REINALDO GARCIA NASTAR
EDILSON ANDRES ROSERO VELASQUEZ

INGENIERÍA DE SISTEMAS
FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS

INSTITUTO TECNOLÓGICO DEL PUTUMAYO
MOCOA, Junio 14 de 2017

ALGORITMO BIDIRECCIONAL DE ENCRIPTACIÓN BASADO EN TLS, PHP Y JAVASCRIPT

WILMER HERNEY MUÑOZ GOMEZ
CARLOS REINALDO GARCIA NASTAR
EDILSON ANDRES ROSERO VELASQUEZ

Producción académica por líneas de investigación para optar al título de INGENIERO DE SISTEMAS

Director: EDGAR ARCINIEGAS ERAZO
Magister en Software Libre
Asesor: ALVARO ADRIAN IZQUIERDO GOMEZ
Especialista en Multimedia Educativa

INGENIERÍA DE SISTEMAS
FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS
INSTITUTO TECNOLÓGICO DEL PUTUMAYO
Mocoa, Junio 14 de 2017

Nota de aceptación

_____

_____

_____

_____

_____

Presidente del jurado

_____

Jurado

_____

Jurado

AGRADECIMIENTOS

Queremos hacer mención de agradecimiento a quienes fueron un apoyo importante directa e indirectamente para la elaboración de este proyecto de investigación, y por el que a su vez hoy optamos al título de Ingenieros de Sistemas.

Primeramente al Instituto Tecnológico del Putumayo y toda la comunidad educativa que lo conforma. Gracias a esta institución hemos tenido la oportunidad de formarnos como profesionales y además crecer como personas. Debido a la situación socioeconómica e histórica del Putumayo, el ITP puede ser la única posibilidad de acceder a la educación superior para muchos de nosotros los putumayenses, de ahí su importancia para nosotros y las futuras generaciones de la región.

Agradecemos en especial a los docentes Edgar Arciniegas Erazo y Álvaro Adrián Izquierdo Gómez, quienes son parte del Grupo de Investigación en Análisis, Diseño y Desarrollo de Software, GIADDS. Con quienes realizamos esta investigación y quienes fueron nuestros asesores y guías en este proceso de aprendizaje y desarrollo.

A nuestras familias, quienes siempre fueron, son y serán un apoyo moral y una motivación constante para superarnos a nosotros mismos y a los obstáculos que nos pone la vida tanto personal como profesional. Gracias a nuestras familias somos quienes somos, y hemos llegado hasta donde hemos llegado, y de una u otra manera son los precursores de que el día de hoy nos estemos formando como profesionales.

Finalmente, a todos los docentes quienes nos acompañaron directamente en nuestro proceso de aprendizaje y formación profesional en el ITP. De todos aprendimos mucho, en lo profesional y en lo personal. Nos hicieron ser conscientes de la importancia de la academia y la educación en nuestra región, nuestra sociedad, y nuestro país. Partimos de esta etapa de la vida, convencidos de que la educación y el saber son las mejores armas para combatir los problemas sociales de nuestro entorno, y la mejor alternativa para una mejor calidad de vida.

TABLA DE CONTENIDO

Contenido

RESUMEN

Algoritmo de encriptación bidireccional basado en TLS, PHP y Javascript

Wilmer Herney Muñoz Gomez

Carlos Reinaldo Garcia Nastar

Edilson Andres Rosero Velasquez

Instituto Tecnológico del Putumayo, Mocoa, Putumayo, Colombia

En este proyecto realizamos primeramente una investigación exhaustiva acerca de los protocolos de seguridad estándar ampliamente usados como OpenSSL, así como también de los algoritmos de encriptación o algoritmos hash como MD5, SHA, AES, etc. El objetivo de aprender acerca de estas tecnologías, fue conocer su funcionamiento, sus aciertos y fallas para obtener una retroalimentación de referencia que nos sirviera de base para la creación de nuestro algoritmo, y determinar lo que se haría, lo que no se haría y como se diferenciaría de estas tecnologías ya existentes. Posteriormente realizamos el algoritmo de encriptación del que concierne este proyecto, al cual denominamos ENIGMA. Este algoritmo fue desarrollado a manera de librería de seguridad para desarrollo web, de manera que se debe implementar tanto en el backend (servidor) como en el frontend (cliente).

El objetivo principal de crear este algoritmo de encriptación bidireccional, es el de ofrecer a los desarrolladores una librería que permita añadir una capa de cifrado adicional a las existentes en la actualidad. Que tuviera un funcionamiento diferente a los demás algoritmos de cifrado, y que tuviera diferente configuración en cada sistema de información en el que fuera implementado. Con la finalidad de fortalecer la seguridad de los sistemas de información web.

Para esto fue necesario desarrollar el algoritmo de manera colaborativa y realizando cambios a medida que la investigación lo requería. Por esta utilizamos el modelo de desarrollo en cascada, el cual nos permitió ir trabajando en cada una de las etapas del desarrollo de software, y si requeríamos volver a alguna etapa en particular lo hacíamos, dado que a medida que descubríamos nueva información o fallos teníamos que replantear el algoritmo y/o su funcionamiento. También utilizamos Git, el cual es un sistema de control de versiones que nos permitió trabajar de manera colaborativa y progresiva. Adicionalmente, utilizamos GitHub.com, el cual es una plataforma que usa y ofrece desarrollo colaborativo y se integra con Git, de manera que podíamos trabajar cada uno de manera independiente en su parte designada, y a través de GitHub uníamos el trabajo realizado sin necesidad siquiera de reunirnos de manera presencial.

El algoritmo lo denominamos ENIGMA, y es el resultado de la investigación realizada y de nuestros esfuerzos por desarrollar un algoritmo de funcionamiento diferente a los actuales. Es compatible con la mayoría de sistemas de información web, funciona en la capa de aplicación del modelo OSI, pero a su vez es transparente al usuario, en este caso el desarrollador.

Palabras clave: Algoritmo; Encriptación; Cliente-Servidor; PHP; Javascript.

---

1. INTRODUCCIÓN

Para formular una manera simple de entender el problema del que concierne este proyecto, a continuación planteamos una analogía y la contrastamos con el proceso real del que tratamos.

Imaginemos que un auto transporta una maleta con una gran cantidad de dinero en su interior, y supongamos que una persona quiere hurtar ese dinero, pues para lograrlo lo único que necesita obtener es esa maleta, ya que una vez que la obtenga, abrirla no será un problema. Exactamente así funciona la mayoría del tráfico de información en internet actualmente. La información viaja simplemente empaquetada a través de las redes de datos, y basta con que algún atacante, a través de los muchos métodos existentes, capture los paquetes de datos para obtener la información que contienen.

Ahora bien, siguiendo con la analogía, imaginemos que ahora, aparte del dinero se deben transportar documentos privados muy importantes en los autos, y se necesita que si alguien logra robar las maletas no puedan acceder a los documentos privados que transporta. Para esto se decide que los autos lleven el dinero y los documentos en una caja fuerte, sin embargo, como se necesita que en todos los lugares de origen y destino sepan cómo asegurar la caja fuerte y como abrirla, se contrata una sola empresa que las fabrique, de esta manera tendrán un tipo de caja fuerte estándar, y en todos los puntos de origen y destino sabrán manipularla, y si acaso contratan otra empresa para que también suministre cajas fuertes, las tendrán que fabricar siguiendo el mismo estándar para no generar mayores inconvenientes en los puntos de origen y destino.

Dada esta situación, el ladrón se dedica día y noche a estudiar cómo funcionan estas cajas fuertes, ya que como todas siguen un estándar y funcionan más o menos igual, si logra abrir una podrá seguir robando y abriendo cuantas quiera. Pues bien, la situación que acabamos de describir es cómo funciona el cifrado de las comunicaciones en las redes de datos actuales, a través de protocolos de cifrado como el SSL (Secure Socket Layer) o el más actual TLS (Transport Layer Security), los cuales encriptan todos los datos que viajan por la red, de tal forma que si alguien captura dichos datos no podrá ver la información que contienen. Sin embargo, al igual que en la analogía, para evitar problemas de compatibilidad se establecieron ciertos estándares que todos los fabricantes de dispositivos deben seguir para poder intercomunicar los equipos y componentes de una red. Esto significa que alrededor del mundo hay muchos cibercriminales que están constantemente buscando vulnerabilidades a estos protocolos, ya que si logran encontrar una falla la pueden explotar en casi todo internet. Y de hecho es lo que

ha sucedido históricamente, siempre que se encuentra una manera de vulnerar estos protocolos, siempre y cuando salga a la luz pública, se deben aplicar parches o actualizaciones a estos protocolos para devolverles la seguridad de los mismos. Esto, repetimos, cuando las vulnerabilidades se hacen públicas, ya que cuando no se dan a conocer el atacante puede aprovecharlas el tiempo que quiera, que es justo lo que sucedió en el caso HEARTBLEED conocido en el año 2014, el cual fue un bug que la NSA (National Security Agency) aprovechó durante aproximadamente dos años para realizar espionaje.

Finalmente, para terminar la analogía, imaginemos que como última medida se toma la decisión de llevar dentro de las cajas fuertes otras cajas fuertes con el dinero y los documentos, sólo que estas cajas fuertes internas no son estándar, y que en cada envió de un origen a un destino se envía una caja fuerte de tipo diferente. Es decir, irán las cajas fuerte estándar y dentro de ellas cajas fuertes distintas, personalizadas, lo que hará muy difícil la tarea del ladrón de acceder al contenido, ya que primero que todo no seguirán un estándar común, y por otro lado si abre una no significa que pueda abrir otra, por el diferente funcionamiento de cada una.

Esto es a grandes rasgos lo que se pretende con ENIGMA, que sea un algoritmo de encriptación para que la información que va encriptada en los protocolos estándar vaya también con una encriptación adicional, que al no ser un estándar conocido, y al ser una encriptación dinámica en cada implementación, garantizará la seguridad e integralidad de la información.

ENIGMA, al ser una librería, se integrará con cualquier sistema de información web, para añadir una capa de cifrado adicional para la información de carácter privado que no debe ser vista por terceros, previniendo todos los problemas que esto podría conllevar. De esta manera tendremos un producto de software enfocado a la seguridad y a la integración con sistemas de información.

2. TÍTULO

ALGORITMO BIDIRECCIONAL DE ENCRIPTACIÓN BASADO EN TLS, PHP Y JAVASCRIPT.

3. DEFINCIÓN DEL PROBLEMA

- La información es un activo en cualquier entidad o institución actual, y de los más valiosos.
- De la privacidad depende mucho la percepción y opinión exterior, y de éstas a su vez depende la estabilidad de cualquier organización o entidad.
- Debido a cuestiones de compatibilidad y estandarización se usan prácticamente los mismos protocolos de seguridad a nivel mundial, y debido a esta exposición global sabemos hoy que estos protocolos no son infalibles.
- Los expertos en seguridad informática concuerdan en que se deben implementar todas las medidas y políticas de seguridad al alcance.
- Se suele recurrir a múltiples capas de cifrado de la información, pero de nuevo, se siguen usando uno sobre otro los mismos algoritmos estándar.
- Los protocolos estándar son de muy bajo nivel, por tanto se salen de nuestro control.

4. OBJETIVOS

4.1 OBJETIVO GENERAL

DESARROLLAR UN ALGORIMTO DE ENCRIPTACIÓN BIDIRECCIONAL EN ARQUITECTURA CLIENTE-SERVIDOR.

4.2 OBJETIVOS ESPECÍFICOS

- Recolectar y analizar información acerca de la encriptación de datos y comunicaciones a bajo nivel.
- Identificar todos los posibles usos y escenarios en los que se puede desempeñar este tipo de software (nuestro algoritmo).
- Determinar y aplicar las condiciones mínimas que debe cumplir el algoritmo para que sea compatible con la gran mayoría de sistemas de información web de la actualidad.
- Desarrollar el algoritmo con la capacidad de encriptar de manera diferente en cada software en que sea implementado.

5. JUSTIFICACIÓN

- El ITP es una institución que forma profesionales integrales, y la seguridad es un área fundamental en las TIC.
- La encriptación, la criptografía y el criptoanálisis son áreas muy interesantes en las cuales adentrarse para realizar investigación.
- Debemos estar en la capacidad de ofrecer una solución en seguridad, una capa de cifrado adicional ajena a los algoritmos y protocolos ampliamente conocidos y utilizados.
- Los sistemas de información web son los mas expuestos debido a su naturaleza en red y los diferentes tipos de clientes existentes.
- Los proyectos libres dan prestigio y reconocimiento a sus lugares de origen y desarrollo:
    - MySQL y JAVA (Sun Microsystems – Oracle).
    - PostgreSQL (Universidad de California en Berkeley).
    - Linux y Git (Linus Torvalds).

6. MARCO REFERENCIAL

Dentro de lo que es el desarrollo de software, las ramas más importantes y tenidas en cuenta a la hora de codificar son el software comercial, software educativo y software gubernamental entre otros, pero todos enfocados a los sistemas de información. Es muy poco común ver desarrollo de bajo nivel por ejemplo, enfocado a desarrollo de controladores, o de seguridad. Esto claramente por el factor económico y por la oferta-demanda implícitos en este tipo de software, ya que este tipo de software es poco comercial y/o los únicos interesados en desarrollar software de bajo nivel son las grandes marcas de tecnología, las cuales recuperan la inversión en estos desarrollos a través de la comercialización de sus productos insignia, los cuales si son comercialmente viables y muy rentables.

Por lo anterior en la región del Putumayo es nulo el desarrollo de este tipo de software, y aún en el país no conocemos una marca o empresa dedicada a ofrecer soluciones de seguridad propias. Ya que las empresas consultoras o asesoras en materia de seguridad informática, suelen implementar productos que si bien pueden ser costosos u otros también libres y gratuitos, son productos de grandes marcas tecnológicas conocidas en el área o son proyectos ampliamente usados de software libre, pero lo que prima es el reconocimiento del producto en el mercado tecnológico.

Por esta razón, dentro del marco teórico y estado del arte, recurrimos a consultar dichos productos, protocolos y conceptos que son ampliamente usados a nivel mundial, y que han definido las pautas a tener en cuenta siempre que algún fabricante requiere crear sus propios productos, y que por supuesto no podemos omitir en este proyecto de investigación, ya que nos ayuda a determinar en general nuestras debilidades, oportunidades, fortalezas y amenazas (DOFA) en este campo en el que nos queremos adentrar.

¿Qué es la encriptación?

Dados los nuevos métodos de investigación utilizados en la Informática Forense, el empleo de un método conocido como "encriptación" se ha vuelto muy usual.
La falta de seguridad que ofrece internet es una de las principales razones por los que esta técnica ha incrementado su presencia en la actualidad.

Por ejemplo, la encriptación para correos electrónicos es una técnica que lleva utilizándose varios años, y existen varios ejemplos de intervención de estas redes privadas que justifican su uso en los últimos años.
Uno de los casos más emblemáticos fue la filtración de lo que se ha venido a llamar el "Cablegate": una serie de documentos filtrados por el sitio WikiLeaks que revelan cientos de miles de informes sobre diferentes aspectos de la diplomacia norteamericana y que se enviaron a través de cables electrónicos a todo el mundo.

La principal preocupación de empresas y entidades gubernamentales es que lleguen los mensajes enviados, única y exclusivamente, a los receptores que ellos quieran. Por esta misma razón, existe una alta demanda para utilizar los diferentes programas de encriptación.

Por cifrado o encriptación, nos referimos al proceso de convertir información a una forma oculta o enmascarada para poder enviarla a través de canales potencialmente inseguros.
El proceso inverso es llamado desencriptación o descifrado.

Utilizando fuertes técnicas de encriptación, la información valiosa y sensible puede ser protegida contra criminales organizados, hackers o espías de fuerzas militares extranjeras. Sin embargo, al movernos dentro de la sociedad de la información, el valor de la criptografía se hace evidente en todos los días de la vida en determinadas áreas como la privacidad, confianza, pagos electrónicos y control de

acceso. De esta manera, el campo de la criptografía se ha ampliado desde las técnicas de encriptación clásicas hasta áreas como la autenticación, integridad de datos, y el no-repudio de la transferencia de datos.

La Criptografía es el arte o ciencia de técnicas matemáticas relacionadas con aspectos de la seguridad de los datos como:

- Confidencialidad o mantener secreto el contenido de la información de partes no autorizadas;
- Integridad de los datos, o detección de modificaciones no autorizadas de los datos;
- Autenticación o autentificación, o identificación del origen de las entidades o datos;
- No repudio, o prevenir que una entidad niegue una acción que ha realizado.

El Criptoanálisis es el estudio de métodos matemáticos que son utilizados en el intento de vencer las técnicas criptográficas.

La Criptología es el estudio de la criptografía y del criptoanálisis.

Algoritmos Criptográficos Básicos

El método de encriptación y desencriptación es llamado Cifrado. Algunos métodos criptográficos se basan en el anonimato de los algoritmos de encriptación; tales algoritmos son de interés histórico y no son adecuados para las necesidades del mundo real. En lugar de anonimato de los algoritmos por si solos, todos los algoritmos modernos basan su seguridad en la utilización de llaves; y un mensaje solo puede ser desencriptado si la llave utilizada para desencriptar coincide con la utilizada para encriptar.

Algoritmos Criptográficos Fuertes

Los buenos sistemas criptográficos deberían siempre ser diseñados para que sean tan difíciles de quebrar como sea posible. Es posible construir sistemas que no puedan ser rotos en la práctica (aunque esto usualmente no puede ser probado). Esto no incrementa significativamente el esfuerzo de implementación

del sistema; sin embargo, se requiere de cierto cuidado y experiencia. No hay excusa para que un diseñador de sistemas deje al sistema quebrantable. Cualquier mecanismo que pueda ser usado para sortear la seguridad debe hacerse explícito, documentado, y puesto en atención de los usuarios finales.

Criptoanálisis y Ataques a Criptosistemas

El criptoanálisis es el arte de descifrar comunicaciones encriptadas sin conocer las llaves correctas. Existen muchas técnicas criptoanalíticas. Algunas de las más importantes se describen a continuación:

- **Criptosistemas de Llave Pública:** Con la clave pública se puede cifrar mensajes, y descifrarlos con la clave privada. Así el propietario de la clave privada sería el único que podría descifrar los mensajes, pero cualquier persona que conozca la clave pública podría enviarlos en forma privada.
- **Criptosistemas de Llave Privada:** Los algoritmos de Llave Privada (o cifrado simétrico) usan la misma llave para la encriptación y desencriptación (o una es fácilmente derivable de la otra). Este es el acercamiento más sencillo a la encriptación de datos, es matemáticamente menos complicado que la criptografía de llave pública y ha sido usado por varios siglos.
- **Funciones Hash:** Las funciones Hash criptográficas son utilizadas en varios contextos, por ejemplo, para calcular el resumen del mensaje cuando se está haciendo una firma digital. Una función Hash comprime el bit de un mensaje a un valor Hash de tamaño fijo en cierto modo que distribuye el posible mensaje uniformemente en medio de los valores Hash posibles.
- **Generador de Números Aleatorios:** El generador de números aleatorios puede ser fácilmente roto y puede volverse el punto más débil de nuestro sistema criptográfico.

Encriptación de 40-bits y 128-bits

Existen varios niveles de encriptación, pero las combinaciones más comunes son 40-512 bits ("llave secreta-llave pública") y 128-1024 bits ("llave secreta-llave pública"). La versión 128-1024 bits es el tipo de encriptación más fuerte que existe en el mercado. Actualmente U.S.A prohíbe la exportación de productos con este tipo de tecnología, pero cabe mencionar que ya existen varios productos producidos en Europa con esta Tecnología que no poseen tales restricciones de exportación.

La gran mayoría de los sitios en internet utilizan la encriptación 40-512 bits, la encriptación 128-1024 bits es utilizada generalmente en transacciones de alto riesgo, como las bancarias.

¿Es segura la encriptación que existe hoy en día?

Depende quien la intente observar, aunque la información sea enviada encripatada, cualquier persona en Internet con entrenamiento mínimo puede interceptar esta información encriptada, sin embargo, para observarla requiere de su "llave privada".

Y es aquí donde depende quien intente observar esta información, considere que una computadora personal (PC) puede realizar millones de operaciones por segundo, debido a esto, no es tan ilusorio generar una "llave privada" a partir de cierta información interceptada ; las "llaves privadas" generalmente constan de 40-bits, en una PC es posible (aunque tardado) procesar estas 2^40 alternativas, ahora bien, si se tienen varios servidores en paralelo realizando trillones de operaciones por segundo probablemente sea posible procesar estas 2^40 alternativas en cuestión de minutos.

Lo anterior es una de la razones por las que U.S.A cuida con tanto recelo la exportación de encriptación de 128-bits, la cual es 3 veces más poderosa (2^128 alternativas) que la de 40-bits.

Públicamente se conoce que en los servidores más poderosos del mercado es posible descubrir una "llave privada" en cuestión de días de procesamiento. Esto obviamente detiene aquellas personas ("hackers") con servidores "comunes" y en este caso hasta oficinas de seguridad gubernamentales en "decriptar" información con este tipo de encriptación.

Protocolos Criptográficos y Estándares

La criptografía funciona en varios niveles. En un nivel se encuentran algoritmos tales como el cifrado de bloques simétrico y los algoritmos de llave pública. Construyendo sobre estos se obtienen protocolos, y construyendo sobre los protocolos se obtienen aflicciones (u otros protocolos).

No es suficiente estudiar la seguridad de los algoritmos de base solamente, como tampoco las debilidades en un protocolo o aplicación de más alto nivel se pueden traducir en cuan insegura es una aplicación o que tan bueno es el algoritmo criptográfico de base. Un ejemplo simple es un protocolo que filtra información sobre la clave usada para encriptar un canal de comunicaciones. Independientemente de cuan buenos sean los algoritmos de encripción, se vuelven inseguros si el protocolo de capa superior muestra información de las claves usadas en la encripción.

El análisis de los protocolos es generalmente difícil porque las aplicaciones que implementan dichos protocolos pueden conducir a problemas adicionales. De esa manera un buen protocolo no es suficiente, se debe tener una buena y robusta implantación.

A continuación se mencionan varios protocolos bien conocidos:

- **Domain Name Server Security (DNSSEC):** es el protocolo para servicios de distribución de nombres seguros. Está definido en RFC 3007 y RFC 3008.
- **Generic Security Services API (GSSAPI):** GSSAPI provee una interfase de autenticación, intercambio de claves y encripción para diferentes algoritmos de encripción y sistemas.

Está definido en RFC 2743.

- **Secure Socket Layer (SSL) / Transport Layer Security (TLS):** SSL es uno de los dos protocolos para conexiones WWW seguras (el otro es SHTTP). La seguridad WWW se ha vuelto importante con el incremento de información sensible, como números de tarjeta de crédito, que se transmite sobre Internet.

  SSL fue desarrollado originalmente por Nestscape en 1994 como un protocolo estándar libre. El borrador de la versión 3.0 se puede encontrar aquí. En 1996, el desarrollo de SSL se convirtió en responsabilidad de la Fuerza de Tareas de Ingenieros de la Internet (IETF, por sus siglas en ingles) y fue renombrado como TSL (Transport Layer Security – Capa de Transporte Seguro). De todas formas TLS 1.0 difiere muy poco de SSL 3.0. Las diferencias se describen en RFC 3546.

- **Secure Hypertext Transfer Protocol (SHTTP) - Protocolo de transferencia de Hipertexto seguro):** el protocolo de transferencia segura de hipertexto es otro que provee más seguridad a las transacciones WWW. Es mucho más flexible que SSL, pero debido a la posición dominante que tenía Netscape en el mercado SSL/TSL está en una posición muy fuerte. SHTTP está definido en RFC 2660.

- **Estándares de encripción de llave pública (PKCS):** estos estándares son desarrollados en RSA Data Security y definen las formas seguras de usar RSA. Los documentos sobre estándares de encripción de llave pública publicados por RSA Laboratories se encuentran disponibles en su sitio web.

- **IEEE P1363 - Especificaciones sobre el estándar criptográfico de llave pública:** es un (siguiendo con lo precedente) estándar criptográfico de clave pública. Consiste de varios algoritmos de llave pública para encripción y firma digital. Tiene un anexo en que se profundiza en todos los detalles necesarios para su implementación. Más información en su sitio web.

- **Publius Censor-Resistent Publishing Protocol - Protocolo resistente a censura:** es un sistema muy avanzado que permite a un grupo de autores y lectores compartir documentos en una serie de servidores web de forma tal que ninguno de ellos necesita revelar su identidad, se certifica la procedencia de los documentos según su autor (usando seudónimos), los documentos no pueden ser eliminados o modificados (censurados) a no ser que se comprometan muchos de los servidores involucrados. En su sitio web se puede

encontrar información técnica, software y vínculos a proyectos relacionados.

- **Secure Shell (Shell Seguro):** el protocolo SSH versión 2 es desarrollado por el Grupo de trabajo SecSh de la IETF. Es un protocolo muy versátil para las necesidades de Internet y es usado en el SSH Tectia software. Se lo utiliza para asegurar sesiones de Terminal y conexiones TCP arbitrarias. Se basa en su predecesor, SSH v.1 desarrollado por Tatu Ylönen. Las especificaciones del protocolo se pueden encontrar en el sitio web de la IETF.
- **IPSec:** mientras que los protocolos arriba mencionados operan en la capa de aplicación de Internet, permitiendo comunicaciones por canales seguros sobre una red insegura, IPSec intenta hacer a Internet una red segura en su esencia, el Protocolo de Internet (IP). El protocolo IPSec está definido en RFC 2401.

SSL 128 bits

Los Certificados SSL de 128 bits funcionan con Server Gated Cryptography (SGC), tecnología aplicada al cifrado de información con la capacidad más alta que alcanza 256 bits. Además, los Certificados SSL de 128 bits garantizan compatibilidad con el 99 por ciento de los browsers y la mayoría de los dispositivos móviles. Por estas características, ofrecen los mejores niveles de protección en operaciones electrónicas para Organizaciones, sitios web y casi todos los clientes o usuarios.

Los Certificados SSL de 128 bits verdaderos (con la ayuda de la tecnología SGC), representan un avance de la tecnología Secure Sockets Layer (SSL). La tecnología SSL, creada por Symantec™, salió al mercado en los años noventa y se especializa en establecer relaciones seguras en la web mediante el cifrado de información y la autentificación de las Organizaciones con la intervención de un Tercero de Confianza para validarlas.

La tecnología SSL funciona con un sistema de claves públicas y privadas para cifrar la conexión entre emisores y receptores de mensajes. Por ejemplo, un consumidor y un sitio web de comercio electrónico. Así, cuando el navegador del consumidor muestra en pantalla el sitio web protegido con SSL, se produce un "apretón de manos" entre los dos sistemas implicados que los autentifica.

En cada sesión, se utiliza una clave de cifrado única cuyo nivel de seguridad depende del número de bits, cuantos más bits tiene es más segura. Una vez establecida la conexión, ambas partes pueden iniciar transacciones con la certeza de que la comunicación se mantendrá íntegra y confidencial.

Este tipo de seguridad adquiere mayor importancia cuando se comparte información de carácter privado a través de Internet, una extranet o una intranet.

Por otro lado, dentro de los Certificados SSL existen los de Validación Extendida

(Extended Validation, EV) que ofrecen el estándar más alto de autentificación. En ellos, Symantec™, como Autoridad de Certificación realiza procesos exhaustivos para la validación de las Organizaciones.

Los Certificados SSL EV se distinguen por su confirmación visual de autenticidad del dominio web, mediante la barra de direcciones en color verde, para que los visitantes sepan que ese sitio no es una falsificación. Por ello, cada vez son más solicitados en portales que reciben numerosos clientes, protegiéndolos de las amenazas por internet, el auge del phishing y otras actividades fraudulentas dedicadas a robar datos personales.
Asimismo, para generar los Certificados SSL de Validación Extendida se requiere, forzosamente, usar llaves de 2048 bits. Esta capacidad de cifrado sólo es posible cuando se cuenta con el sistema Server Gated Cryptography (SGC).

La tecnología Server Gated Cryptography (SGC) permite activar un nivel mínimo de cifrado de 128 bits, independientemente de la eficacia de cifrado disponible en el navegador del usuario.
Con SGC el control de los niveles de cifrado queda en manos del servidor. Es decir, es independiente del navegador disponible en el sistema del usuario. Cuando se carece de SGC, el nivel de cifrado que se activa de forma predeterminada es el mínimo disponible en el servidor o en el navegador cliente.
En otras palabras, dado que los visitantes del sitio web no pueden determinar fácilmente la potencia de cifrado de una sesión específica, dependen del propietario del sitio web para que los proteja. Así, los certificados SSL de 128 bits permiten a casi todos los visitantes de un sitio web disfrutar del cifrado más potente que existe en el mercado.
De esta forma, los Certificados SSL de 128 bits con su sistema SGC de criptografía activada por servidor ofrecen protección más de un billón de billones de veces más potente porque puede calcular 288 veces más combinaciones que un cifrado de 40 bits.

Los Certificados SSL de 128 bits protegen al 99 por ciento de los visitantes en un sitio web. Entre ellos, usuarios con aplicaciones de navegadores y sistemas operativos como: versiones de exportación de Internet Explorer desde la 3.02 hasta la versión anterior a la 5.5; versiones de exportación de Netscape posteriores a la 4.02 y hasta la 4.72; sistemas Windows 2000 adquiridos antes de marzo de 2001 que no hayan descargado High Encryption Pack o Service Pack 2 de Microsoft y que utilicen Internet Explorer.

Sin embargo, es importante mencionar que las versiones de Internet Explorer anteriores a la 3.02 y de Netscape previas a la 4.02, no admiten cifrado de 128 bits con ningún tipo de Certificado SSL.

Por lo tanto, los Certificados SSL de 128 bits son recomendables para las Organizaciones que: aceptan tarjetas de crédito, débito o de compra; realizan pagos en línea, permiten el acceso en red a información bancaria o bursátil; transmiten electrónicamente registros sobre expedientes clínicos o de seguros; deben cumplir con normativas de seguridad y confidencialidad como oficinas gubernamentales; y para aquellas cuya reputación y prestigio dependen de la integridad y confidencialidad de su información.

Finalmente, Los Certificados SSL de 128 bits cuentan con todas las ventajas de los Certificados de Seguridad emitidos por Symantec™, proveedor líder de Certificados a nivel internacional.

7. DISEÑO METODOLÓGICO

Nuestra investigación tomará principalmente dos enfoques, primeramente la investigación técnica de todo lo relacionado con comunicación a bajo nivel en redes, algoritmos de encriptación, software existente, métodos existentes, técnicas de compatibilidad, etc. Y por otro lado, se realizará el desarrollo de la librería como tal, aplicando todo el conocimiento adquirido en la investigación previa, pero diseñando el algoritmo con un funcionamiento diferente a los algoritmos y protocolos estándar ya existentes.

En cuanto al desarrollo utilizaremos el modelo en cascada como metodología de desarrollo, debido a que nuestra investigación marcará el camino y las decisiones a tomar en el desarrollo del algoritmo y cualquier cambio que determinemos necesario por la investigación deberá aplicarse al desarrollo del algoritmo. Por supuesto pasando por las etapas del desarrollo de software las cuales también aplican para el desarrollo de esta librería:

- Análisis de requisitos del sistema.
- Diseño del sistema.
- Implementación del sistema.
- Pruebas.
- Mantenimiento y corrección.
- Documentación del sistema.

También utilizaremos el sistema de control de versiones Git, el cual es ideal para el desarrollo progresivo y colaborativo, es decir, que todos podamos desarrollar de manera independiente las partes necesarias para luego unir el trabajo realizado. Esto se complementa con el uso de la plataforma GitHub, la cual nos permitirá tener unificado el código realizado por todos los integrantes del grupo y tener un respaldo en la nube del mismo.

8. RESULTADOS

De esta investigación y desarrollo el resultado se puede clasificar en dos partes, la primera es la librería Enigma como tal, la cual se encuentra en un repositorio de GitHub lista para ser descargada e implementada, y la segunda es el sitio web del proyecto, en donde a su vez se encuentra la descripción de Enigma, la documentación o manual de usuario de la librería, y también artículos que hacen parte de la investigación que realizamos para desarrollar Enigma.

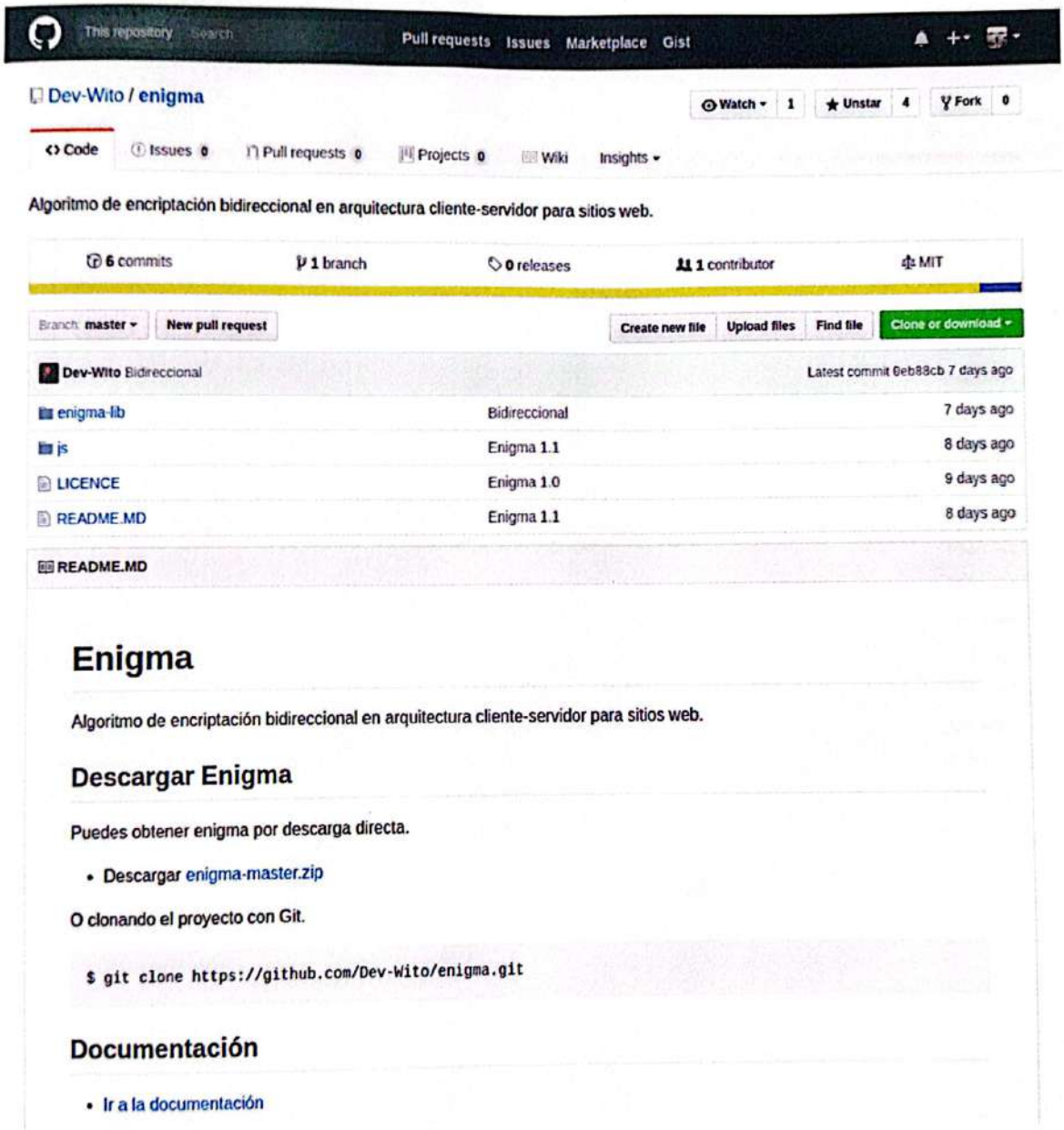
A continuación se explica y muestra en detalle cada uno.

8.1 ALGORITMO DE ENCRIPTACIÓN ENIGMA

El algoritmo o librería ENIGMA se encuentra en un repositorio de GitHub en la siguiente dirección:

- https://github.com/Dev-Wito/enigma

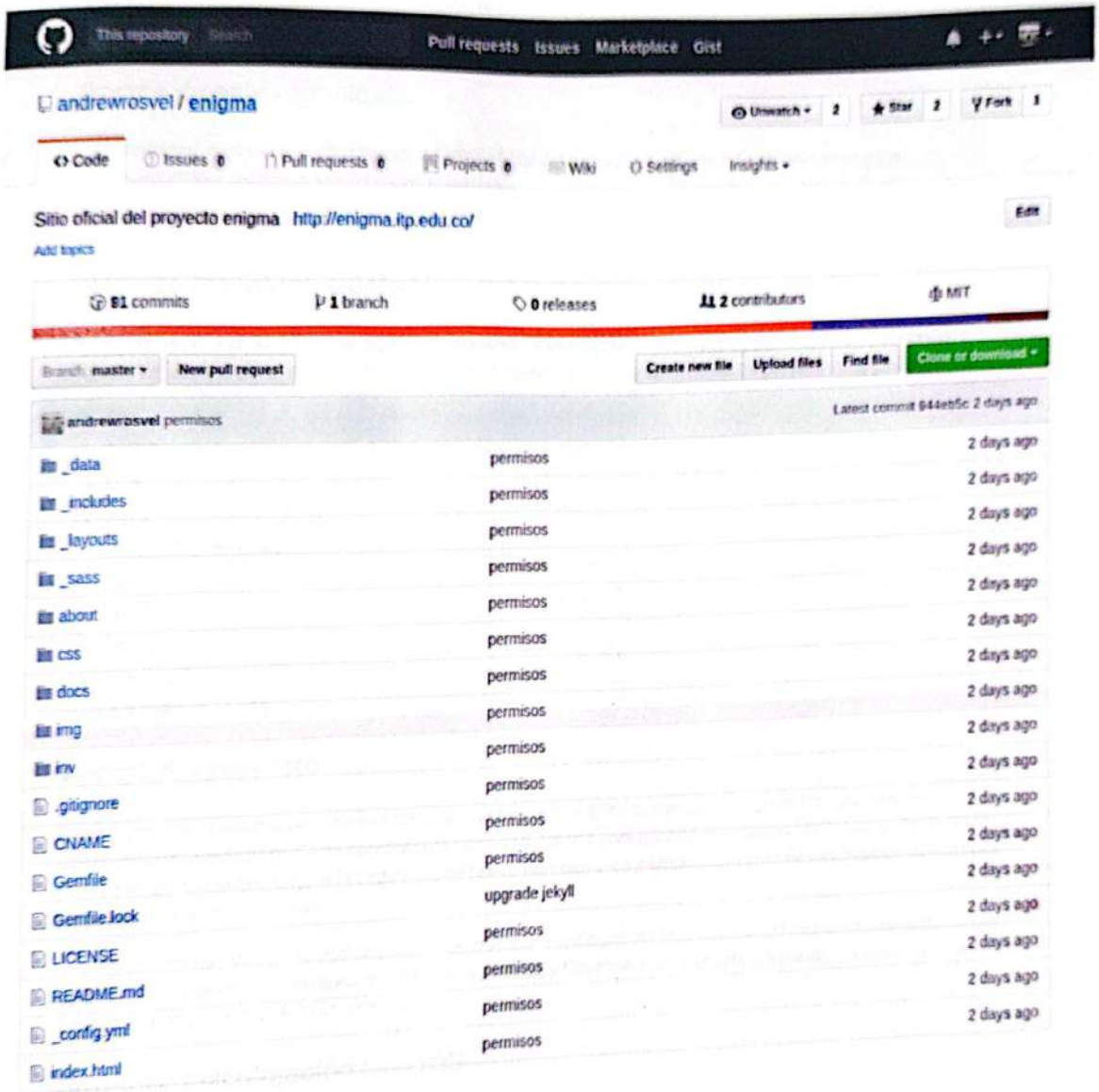
Aquí se encuentra únicamente la librería para descargar e implementar.



8.2 SITIO WEB DEL PROYECTO ENIGMA

Repositorio en GitHub del sitio web del proyecto, se encuentra en la dirección.

- https://github.com/andrewrosvel/enigma



Repositorio en GitHub del sitio web del proyecto.

README.md

enigma

Algoritmo bidireccional de encriptación en arquitectura cliente-servidor.

Acerca de este repositorio

Este repositorio contiene el **código fuente del sitio oficial del proyecto**, en el que a su vez se encuentra la **documentación e investigación** del proyecto enigma.

- Sitio oficial del proyecto

Stack de tecnologías del sitio

Para el desarrollo del sitio oficial del proyecto y su puesta en producción utilizamos el siguiente stack de tecnologías. Algunas las usamos por preferencia personal y otras simplemente porque son necesarias por parte de la plataforma GitHub.

- Git
- GitHub
- Ruby
- Jekyll
- Html, CSS y Javascript
- Sass
- Markdown
- jQuery
- Bootstrap 3
- Font Awesome Icons

Acerca del proyecto

Este proyecto es el resultado de una investigación realizada con el fin de desarrollar un algoritmo de encriptación bidireccional en arquitectura cliente-servidor para sitios web. No solo para generar investigación académica, sino también, **ofrecer un producto que mejore la seguridad de las comunicaciones y almacenamiento de información sensible** en los sistemas de información web.

Desarrollado por tres *estudiantes/investigadores* del Instituto Tecnológico del Putumayo sede Mocoa, Putumayo (Colombia). Integrantes del **Grupo de Investigación en Análisis, Diseño y Desarrollo de Software (GIADDS)**, y liderado por dos *docentes/investigadores* de la misma institución.

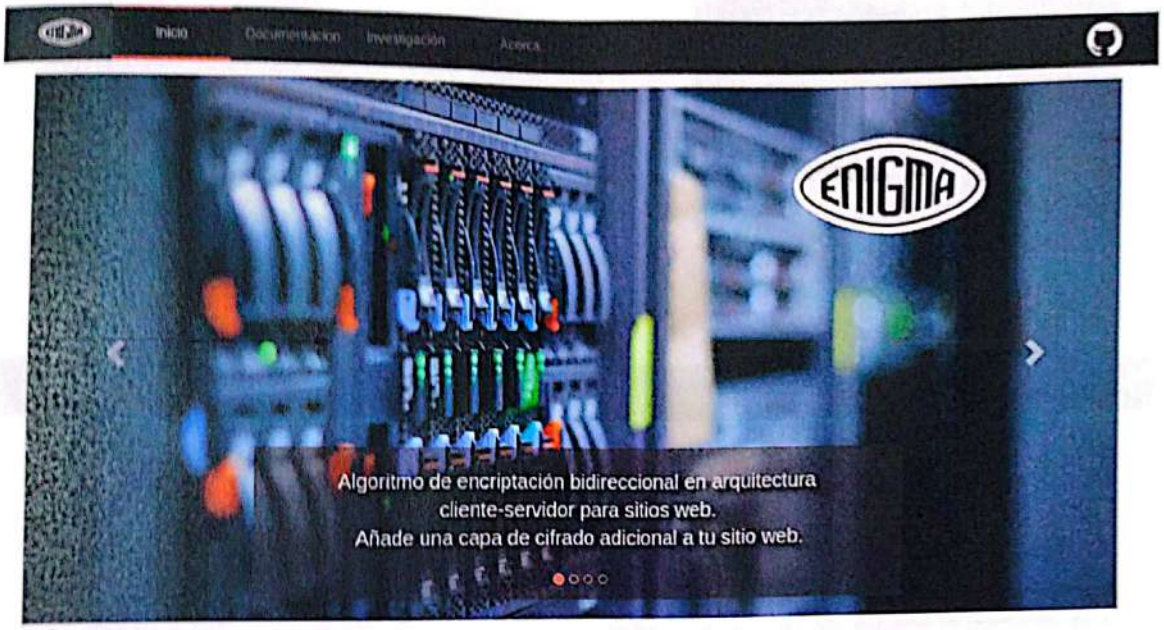
Grupo de Investigación GIADDS

- **Edgar Arciniegas Erazo** (Director GIADDS)
- **Alvaro Adrian Izquierdo Gomez** (Docente/Investigador)
- **Carlos Reinaldo Garcia Nastar** (Estudiante/Investigador)
- **Wilmer Herney Muñoz Gomez** (Estudiante/Investigador)
- **Edilson Andres Rosero Velasquez** (Estudiante/Investigador)

Sitio web del proyecto enigma, se encuentra en la dirección.

- http://enigma.itp.edu.co/

SITIO WEB ENIGMA – INICIO



SITIO WEB ENIGMA – INICIO

Enigma ¿Qué es?

Enigma es una librería de seguridad escrita en **php y javascript** para proyectos web. Añade una capa de cifrado adicional a las capas tradicionales de bajo nivel como **SSL/TLS**.

Incluso si no tienes implementado **https** en tu sitio (*que deberías tenerlo*), con enigma puedes cifrar la información sensible a la hora de enviarla y recibirla, usuarios, contraseñas, correos, etc.

Gran compatibilidad

No importa que framework o librerías ya estes utilizando, siempre y cuando tengas php en el backend, enigma se adaptará a tu proyecto.

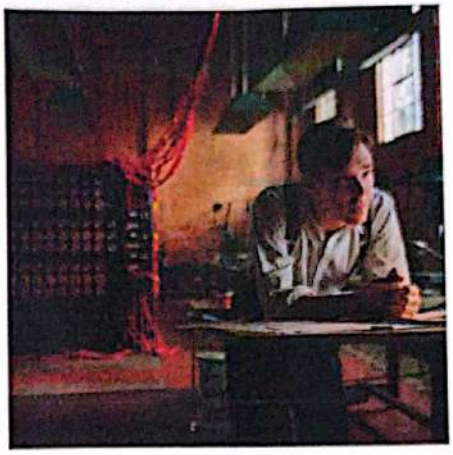
Enigma es semitransparente, sólo debes inicializarlo y esta listo, en lo demas es como si no estuviera allí, seguirás programando de la misma manera. Además es compatible con la gran mayoría de sitios de la actualidad debido al uso masivo de **php y javascript**.

Pronto estará disponible también para **javascript en el backend**, de manera que será compatible con **NodeJS**, el cual es un stack tecnológico que esta creciendo a pasos agigantados.

SITIO WEB ENIGMA – INICIO

El nombre ¿Por qué "enigma"?

El nombre de nuestro proyecto proviene de la película **The Imitation Game**, o en español, **El Código Enigma**, la cual a su vez se basa en la historia de cómo el matemático, científico y criptoanalista Alan Turing y un equipo de expertos, trabajó durante la segunda guerra mundial para lograr descifrar códigos de guerra encriptados con la máquina enigma.



Mavis Batey (1921 - 2013).

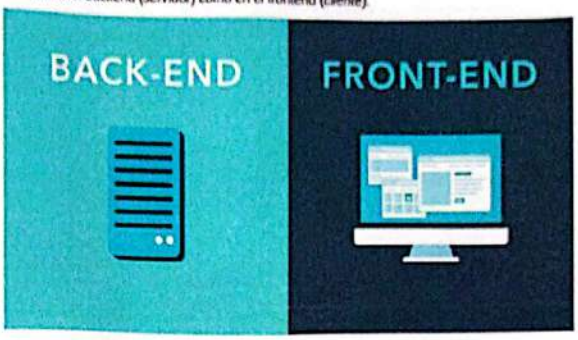
Mavis Batey fué una de las personas clave para romper el cifrado de la maquina enigma, ya que en 1941 fué la primer persona en descifrar un mensaje de dicha maquína, que hasta entonces se consideraba indescifrable.

SITIO WEB ENIGMA – INICIO

SITIO WEB ENIGMA – DOCUMENTACIÓN

Introducción

Enigma esta diseñado para funcionar en arquitectura **cliente-servidor**, por tanto su instalación consiste en importar los archivos necesarios de enigma tanto en el backend (servidor) como en el frontend (*cliente*).



Por ahora, enigma sólo funciona con **php** como lenguaje de programación en el backend y **javascript** en el frontend.
Esta es una fórmula casi estandar en la web actual, debido al uso masivo de php en el servidor y tecnologías javascript en el cliente.

Esto te garantiza una forma fácil de integrar enigma a cualquier proyecto con este stack de tecnologías, independientemente del framework o librerías que ya estes usando.

Descargar enigma

Puedes obtener enigma a través de una descarga directa.

- **Descargar** enigma-master.zip

O puedes clonar el proyecto con git.

```
$ git clone https://github.com/Dev-Wito/enigma.git
```

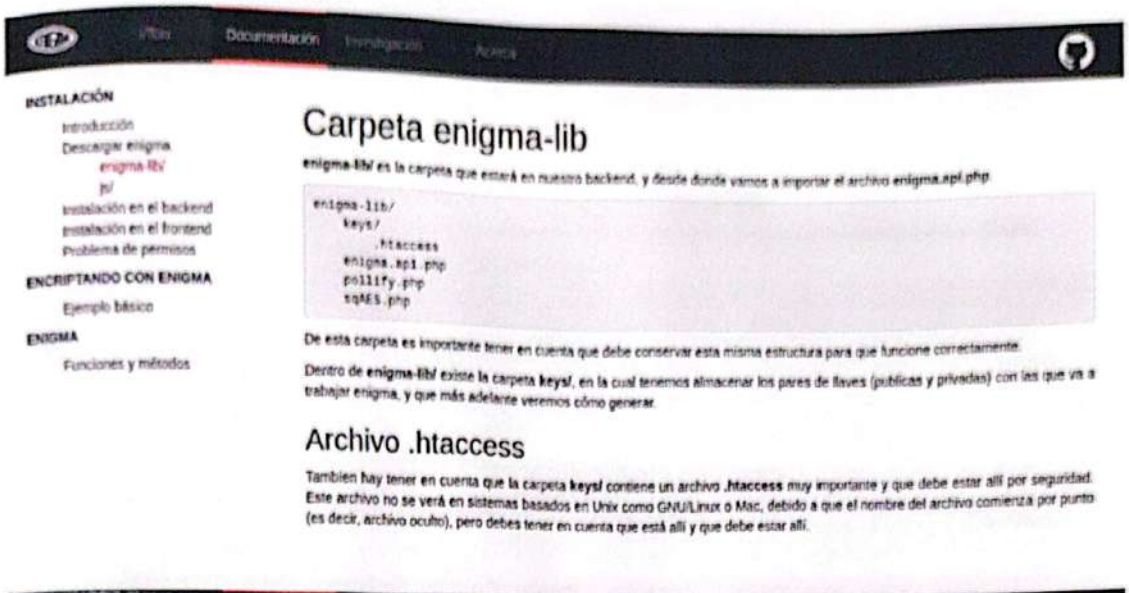
Estructura de carpetas

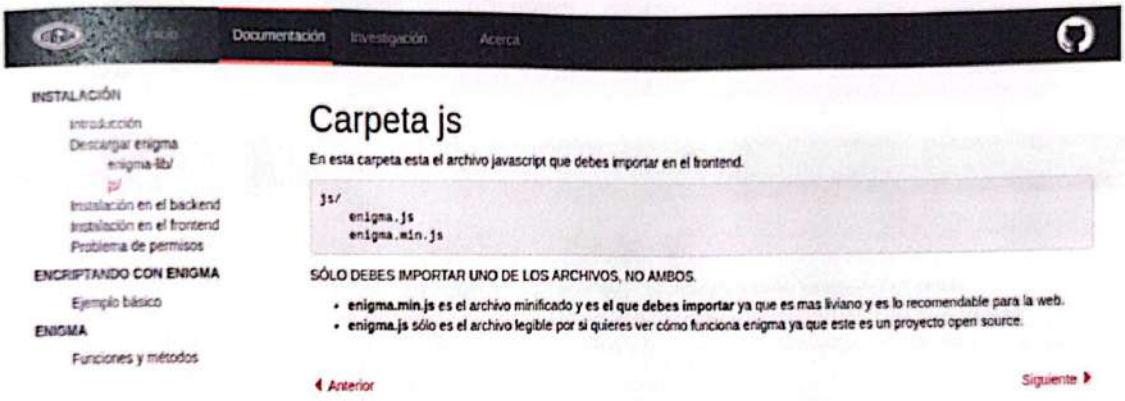
De cualquiera de las formas anteriores obtendrás una carpeta la cual tiene la siguiente estructura.

```
enigma-master/
    enigma-lib/
        keys/
            .htaccess
        enigma.api.php
        pollify.php
        sqAES.php
    js/
        enigma.js
        enigma.min.js
```

Donde **enigma-lib/** es la carpeta que irá en el backend. Y **js/** contiene el archivo javascript que irá en el frontend.

SITIO WEB ENIGMA – DOCUMENTACIÓN





Instalación en el backend

1. Implementar la carpeta enigma-lib

Debemos pegar la carpeta **enigma-lib/** según la estructura de nuestro proyecto y/o según el framework que estes utilizando.

A manera de un ejemplo sencillo quedaría así:

```
mi-proyecto/
    enigma-lib/
        keys/
            .htaccess
        enigma.api.php
        pollify.php
        xgAES.php
```

2. Generar el grupo de pares de llaves

Para que enigma cifre de manera segura y aleatoria, es necesario que tú generes un grupo de pares de llaves que enigma pueda utilizar. Para esto es necesario instalar OpenSSL y generar las llaves con los siguientes comandos *(y en este orden)* en la terminal.

Estos comandos aplican para sistemas de la familia unix como mac, gnu/linux o freebsd por ejemplo.

```
$ openssl genrsa -out priv.pem 2048
$ openssl rsa -pubout -in priv.pem -out pub.pem
```

Estos comandos nos van a generar **2 archivos, priv.pem y pub.pem**, es decir, la llave privada y la llave pública respectivamente. Esto es sólo nuestro primer par de llaves, las cuales debemos guardar en una carpeta y a su vez almacenarla en la carpeta **keys/**

Instalación en el frontend

IMPORTANTE: Enigma en el frontend require de **jQuery, en su versión mínima recomendada 1.12.4** o superior.

En el frontend sólo debes pegar el archivo **enigma.min.js** en la carpeta con tus otros archivos javascript, y luego importarlo.

Para continuar con el ejemplo anterior, he creado un archivo **index.html** el cual será nuestro archivo frontend, y en el que vamos a importar a **enigma.min.js**.

Por lo que la estructura del proyecto ahora sería así:

SITIO WEB ENIGMA – DOCUMENTACIÓN

Inicio Documentación Investigación Acerca

INSTALACIÓN
- Introducción
- Descargar enigma
  - enigma-lib/
  - js/
- Instalación en el backend
- Instalación en el frontend
- Problema de permisos

ENCRIPTANDO CON ENIGMA
- Ejemplo básico

ENIGMA
- Funciones y métodos

Problema de permisos

Si tu servidor es un sistema de la familia Unix, como **Mac** o **GNU/Linux**, es muy probable que enigma no funcione correctamente, y esto es porque hay que aplicarle los permisos correctos a los archivos y carpetas de tu proyecto. Hacer esta configuración es muy sencillo.

Primero deberías haber instalado enigma tanto en el **backend** como en el **frontend** según los pasos anteriores, **incluyendo haber creado los pares de llaves**.

Una vez hecho esto, abres la terminal o consola y vas hasta donde esta tu proyecto, especificamente a la raíz del proyecto, y una vez allí ejecutas los siguiente comandos.

```
$ find . -type d -exec chmod 755 {} \;
$ find . -type f -exec chmod 644 {} \;
```

Recuerda, los debes ejecutar en la raíz de tu proyecto. Por ejemplo así.

```
rosvel@k45vd: ~/mi-proyecto
rosvel@k45vd:~/mi-proyecto$ find . -type d -exec chmod 755 {} \;
rosvel@k45vd:~/mi-proyecto$ find . -type f -exec chmod 644 {} \;
rosvel@k45vd:~/mi-proyecto$
```

Estos comandos lo que hacen es asignar permisos **755** a las carpetas, y permisos **644** a los archivos, respectivamente. Que por cierto son los permisos estandar recomendados para la web.

Una vez hecha esta configuración no habrá inconvenientes.

Inicio Documentación Investigación Acerca

INSTALACIÓN
- Introducción
- Descargar enigma
  - enigma-lib/
  - js/
- Instalación en el backend
- Instalación en el frontend
- Problema de permisos

ENCRIPTANDO CON ENIGMA
- Ejemplo básico

ENIGMA
- Funciones y métodos

Ejemplo básico

A continuación vamos a continuar con el ejemplo básico que hemos venido trabajando en la instalación. En este ejemplo crearemos un formulario y lo enviaremos con enigma para ver su funcionamiento y cómo envía la información.

Repositorio de este ejemplo

En caso de que te pierdas en alguno de los pasos o no entiendas algo, he creado un repositorio con el ejemplo para que lo descargues.

- enigma-ejemplo-simple

O igualmente puedes clonarlo.

```
$ git clone https://github.com/andrewrosvel/enigma-ejemplo-simple.git
```

Archivo index.html

Primero que nada he creado un formulario sencillo con 3 campos, usuario, email y contraseña. He añadido algunas clases css de bootstrap para mejor visualización pero es un formulario muy sencillo.
Este formulario apunta al archivo **controlador.php**, y lo que devuelva este controlador lo veremos en un iframe al lado derecho.

```
<div class="container">
  <div class="row">
    <div class="col-md-6">
      <h3>Mi formulario</h3>

      <form id="mi-formulario" action="controlador.php" method="post" target="resultado">
        <div class="form-group">
          <input class="form-control" type="text" name="usuario" placeholder="usuario">
        </div>
```

SITIO WEB ENIGMA – DOCUMENTACIÓN

INSTALACIÓN

- Introducción
- Descargar enigma
  - enigma-lib/
  - js/
- Instalación en el backend
- Instalación en el frontend
- Problema de permisos

ENCRIPTANDO CON ENIGMA

- Ejemplo básico

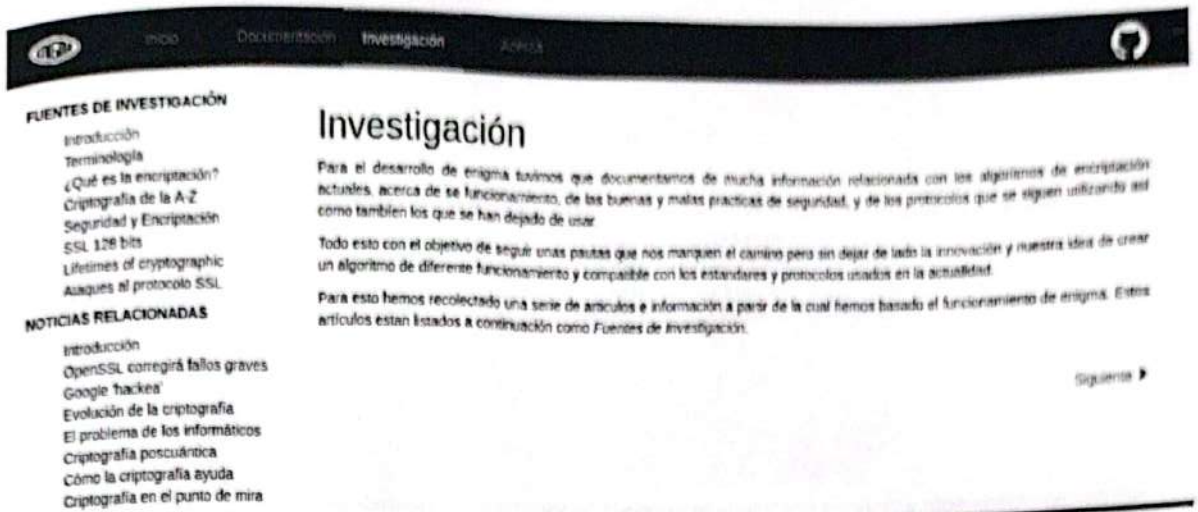
ENIGMA

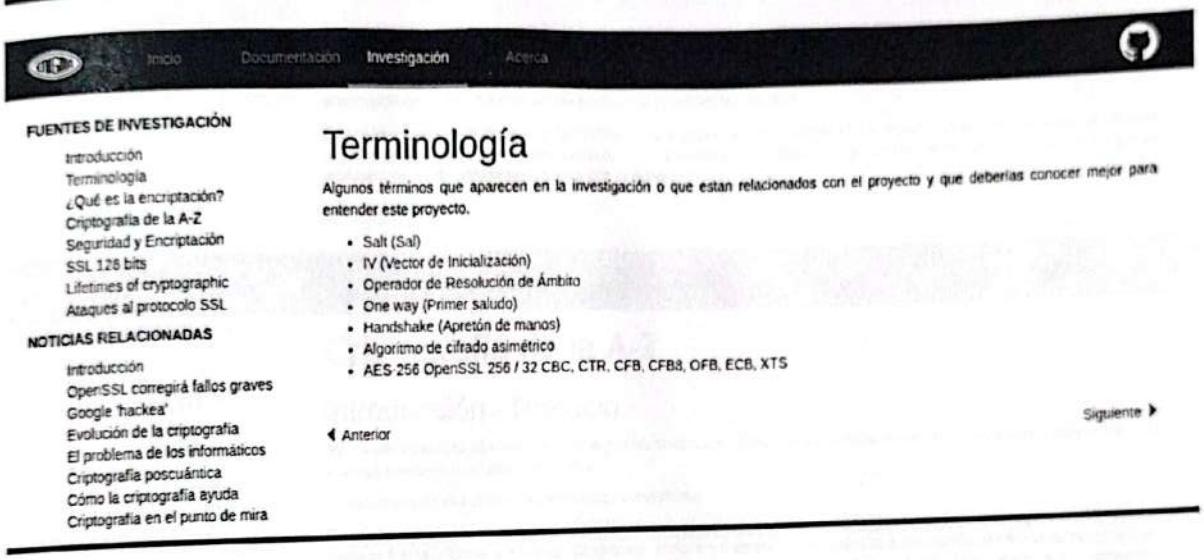
- Funciones y métodos

Funciones y métodos

Metodo	Parametros	Descripción
S.Enigma.authenticate	AESEncryptionKey[string], publicKeyURL[string], handshakeURL[string], success(AESEncryptionKey)[function], failure(AESEncryptionKey)[function]	Esta funcion es requerida antes de cualquier cifrado, optiene una llave publica del servidor y genera el handshake correspondiente. Su funcionamiento es: **1)** Cliente genera una clave (Cuando sea posible la ejecucion del evento mousemovement) **2)** El cliente solicita clave pública RSA desde servidor. **3)** El cliente cifra la contraseña con la clave pública RSA **4)** El servidor descifra la contraseña y la almacena en la sesión **5)** El servidor Cifra la contraseña con AES y la devuelve al Cliente

SITIO WEB ENIGMA – INVESTIGACIÓN





SITIO WEB ENIGMA – INVESTIGACIÓN

Inicio Documentación Investigación Acerca

FUENTES DE INVESTIGACIÓN

- Introducción
- Terminología
- ¿Qué es la encriptación?
- Criptografía de la A-Z
- Seguridad y Encriptación
- SSL 128 bits
- Lifetimes of cryptographic
- Ataques al protocolo SSL

NOTICIAS RELACIONADAS

- Introducción
- OpenSSL corregirá fallos graves
- Google 'hackea'
- Evolución de la criptografía
- El problema de los informáticos
- Criptografía poscuántica
- Cómo la criptografía ayuda
- Criptografía en el punto de mira

¿Qué es la encriptación?

Fecha: 28-dic-2010

Conoce cómo funciona uno de los principales métodos de seguridad utilizados en Internet que la misma WikiLeaks utiliza.

Dados los nuevos métodos de investigación utilizados en la *Informática Forense*, el empleo de un método conocido como "encriptación" se ha vuelto muy usual.

La falta de seguridad que ofrece Internet es una de las principales razones por los que esta técnica ha incrementado su presencia en la actualidad.

Por ejemplo, la **encriptación para correos electrónicos** es una técnica que lleva utilizándose varios años, y existen varios ejemplos de intervención de estas redes privadas que justifican su uso en los últimos años.

Uno de los casos más emblemáticos fue la filtración de lo que se ha venido a llamar el "Cablegate": una serie de **documentos filtrados por el sitio .WikiLeaks** que revelan cientos de miles de informes sobre diferentes aspectos de la diplomacia norteamericana y que se enviaron a través de cables electrónicos a todo el mundo.

Inicio Documentación Investigación Acerca

FUENTES DE INVESTIGACIÓN

- Introducción
- Terminología
- ¿Qué es la encriptación?
- Criptografía de la A-Z
- Seguridad y Encriptación
- SSL 128 bits
- Lifetimes of cryptographic
- Ataques al protocolo SSL

NOTICIAS RELACIONADAS

- Introducción
- OpenSSL corregirá fallos graves
- Google 'hackea'
- Evolución de la criptografía
- El problema de los informáticos
- Criptografía poscuántica
- Cómo la criptografía ayuda
- Criptografía en el punto de mira

Criptografía de la A-Z

Introducción - Prefacio

Por **cifrado o encriptación**, nos referimos al proceso de convertir información a una forma oculta o enmascarada para poder enviarla a través de canales potencialmente inseguros.

El proceso inverso es llamado **desencriptación o descifrado**.

tilizando fuertes técnicas de encriptación, la información valiosa y sensible puede ser protegida contra criminales organizados, hackers o espias de fuerzas militares extranjeras. Sin embargo, al movernos dentro de la sociedad de la información, el valor de la criptografía se hace evidente en todos los días de la vida en determinadas áreas como la privacidad, confianza, pagos electrónicos y control de acceso. De esta manera, el campo de la criptografía se ha ampliado desde las tecnicas de encriptación clásicas hasta áreas como la autenticación, integridad de datos, y el no-repudio de la transferencia de datos.

Terminología Básica

A continuación, se presentarán los conceptos básicos y los metodos principales de criptografía. Cualquier opinión y evaluación presentadas aquí son especulativas, y ni el autor, ni segu-info pueden hacerce responsable de su exactitud, aunque cada intento es realizado para asegurar que la información es tan correcta y actualizada como sea posible.

Supongamos que alguien quiere enviar un mensaje a un receptor, y quiere estar seguro de que nadie mas leea el mensaje.

Sin embargo, existe la posibilidad de que alguien mas abra el correo o escuche la comunicación electrónica.

En terminos criptográficos, el mensaje es llamado **Texto Plano o Texto Claro**. El proceso de codificación del mensaje de forma tal que se oculte su contenido de extraños o intrusos es llamado encriptación o cifrado. El mensaje encriptado es llamado **Texto Cifrado**. El proceso para obtener el texto plano desde el texto encriptado es llamado desencriptación, decodificación o descifrado. La encriptación y la desencriptación generalmente hacen uso de una **Llave**, y el método de codificación es tal que la desencriptación puede ser ejecutada solamente conociendo la llave.

SITIO WEB ENIGMA – INVESTIGACIÓN

FUENTES DE INVESTIGACIÓN

- Introducción
- Terminología
- ¿Qué es la encriptación?
- Criptografía de la A-Z
- Seguridad y Encriptación
- SSL 128 bits
- Lifetimes of cryptographic
- Ataques al protocolo SSL

NOTICIAS RELACIONADAS

- Introducción
- OpenSSL corregirá fallos graves
- Google 'hackea'
- Evolución de la criptografía
- El problema de los informáticos
- Criptografía poscuántica
- Cómo la criptografía ayuda
- Criptografía en el punto de mira

Seguridad y Encriptación

Con la aparición de Internet y la mayor importancia que se le va dando a la información día tras día , la tecnología que antes era utilizada sólo por la Militar o Gobiernos ha cobrado mayor importancia, pero... como funciona ?

Que es Encriptación?

Toda encriptación se encuentra basada en un Algoritmo, la función de este Algoritmo es básicamente codificar la información para que sea indescifrable a simple vista , de manera que una letra *"A"* pueda equivaler a *"5x5mBwE"* o bien a *"xQE9fq"*, el trabajo del algoritmo es precisamente determinar como será transformada la información de su estado original a otro que sea muy difícil de descifrar.

Una vez que la información arrive a su destino final, se aplica el algoritmo al contenido codificado *"5x5mBwE"* o bien a *"xQE9fq"* y resulta en la letra "A" o según sea el caso, en otra letra. Hoy en día los algoritmos de encriptación son ampliamente conocidos es por esto que para prevenir a otro usuario "no autorizado" descifrar información encriptada, el algoritmo utiliza lo que es denominado **llave (“key”)** para controlar la encriptación y decriptación de información. Algunos algoritmos son **DES** (algoritmo simétrico) AES que posiblemente suplantará a DES y uno de los más conocidos RSA (algoritmo asimétrico)

Que función tiene la llave (“key”)?

Existen dos tipos de llaves ("key's"), pero la de mayor uso en Internet es denominada "public key" o algoritmo asimétrico. El nombre "public" proviene de su funcionamiento: existe una llave pública que es dada a conocer a cualquier persona que así lo desee (todo Internet), esta llave pública es utilizada por los emisores de mensajes para encriptar información, sin embargo, existe otra llave (su pareja por llamarla de alguna manera) única que es conocida exclusivamente por el destinatario del mensaje, y es mediante esta llave única | secreta que el destinatario descifra ("decripta") los mensajes encriptados por el emisor.

Firmas Digitales (“Digital Signatures”)

FUENTES DE INVESTIGACIÓN

- Introducción
- Terminología
- ¿Qué es la encriptación?
- Criptografía de la A-Z
- Seguridad y Encriptación
- SSL 128 bits
- Lifetimes of cryptographic
- Ataques al protocolo SSL

NOTICIAS RELACIONADAS

- Introducción
- OpenSSL corregirá fallos graves
- Google 'hackea'
- Evolución de la criptografía
- El problema de los informáticos
- Criptografía poscuántica
- Cómo la criptografía ayuda
- Criptografía en el punto de mira

SSL 128 bits

Los **Certificados SSL de 128 bits** funcionan con Server Gated Cryptography (SGC), tecnología aplicada al cifrado de información con la capacidad más alta que alcanza 256 bits. Además, los Certificados SSL de 128 bits garantizan compatibilidad con el 99 por ciento de los browsers y la mayoría de los dispositivos móviles. Por estas características, ofrecen los mejores niveles de protección en operaciones electrónicas para Organizaciones, sitios web y casi todos los clientes o usuarios.

Los **Certificados SSL de 128 bits** verdaderos (con la ayuda de la tecnología SGC), representan un avance de la tecnología Secure Sockets Layer (SSL). La tecnología SSL, creada por Symantec™, salió al mercado en los años noventa y se especializa en establecer relaciones seguras en la web mediante el cifrado de información y la autentificación de las Organizaciones con la intervención de un Tercero de Confianza para validarlas.

La tecnología SSL funciona con un sistema de claves públicas y privadas para cifrar la conexión entre emisores y receptores de mensajes. Por ejemplo, un consumidor y un sitio web de comercio electrónico. Así, cuando el navegador del consumidor muestra en pantalla el sitio web protegido con SSL, se produce un "apretón de manos" entre los dos sistemas implicados que los autentifica.

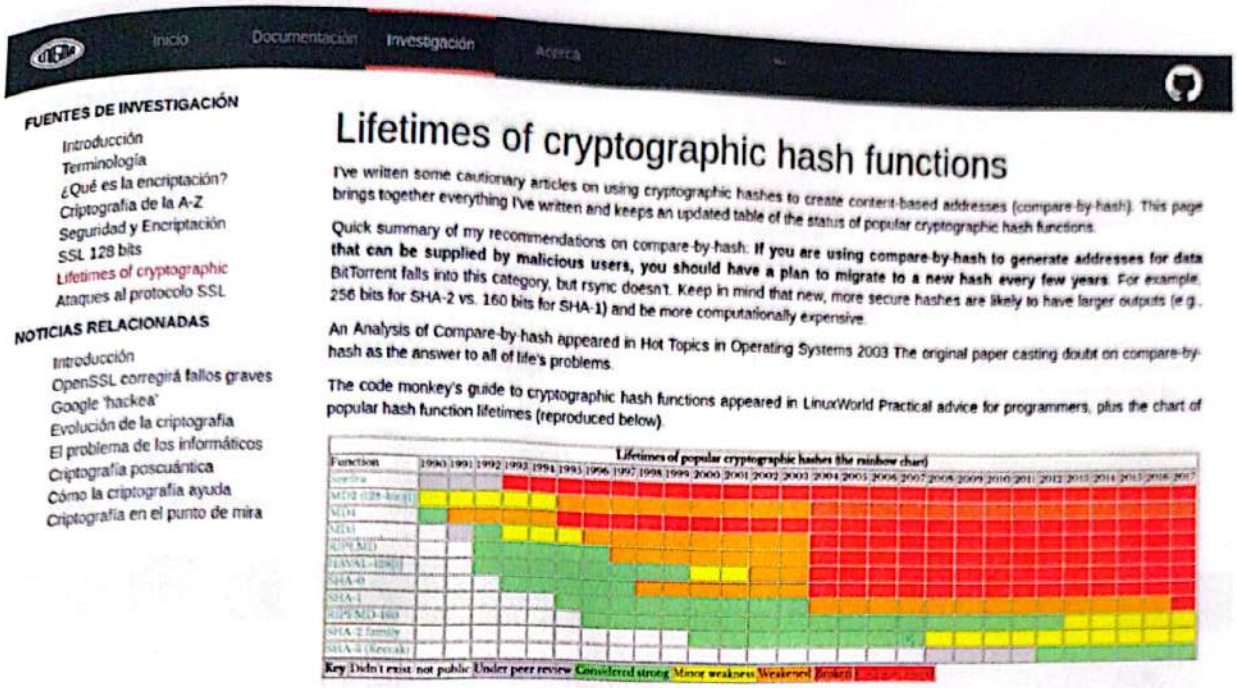
En cada sesión, se utiliza una clave de cifrado única cuyo nivel de seguridad depende del número de bits, cuantos más bits tiene es más segura. Una vez establecida la conexión, ambas partes pueden iniciar transacciones con la certeza de que la comunicación se mantendrá íntegra y confidencial.

Este tipo de seguridad adquiere mayor importancia cuando se comparte información de carácter privado a través de Internet, una extranet o una intranet.

Por otro lado, dentro de los Certificados SSL existen los de Validación Extendida (Extended Validation, EV) que ofrecen el estándar más alto de autentificación. En ellos, Symantec™, como Autoridad de Certificación realiza procesos exhaustivos para la validación de las Organizaciones.

Los Certificados SSL EV se distinguen por su confirmación visual de autenticidad del dominio web, mediante la barra de direcciones en color verde, para que los visitantes sepan que ese sitio no es una falsificación. Por ello, cada vez son más solicitados en portales que reciben numerosos clientes, protegiéndolos de las amenazas por Internet, el auge del phishing y otras actividades fraudulentas dedicadas a robar datos personales.

SITIO WEB ENIGMA – INVESTIGACIÓN



Seguridad del protocolo SSL (Secure Sockets Layer)

- SSL/TLS es seguro en su diseño teórico. Pero esto es una condición necesaria aunque no suficiente.
- La "seguridad real" del protocolo SSL tiene que ser matizada. Por ejemplo en su uso en la web va mucho más allá de la idea equivocada de que una página es segura si y solo si se muestra el famoso "candado amarillo".

SITIO WEB ENIGMA – INVESTIGACIÓN

Noticias relacionadas

Una de las razones principales por las que decidimos desarrollar un algoritmo de encriptación fué por las constantes noticias informáticas en los medios tecnológicos, en donde se da a conocer con mucha frecuencia que a X protocolo de seguridad o a X algoritmo de cifrado se le encontraron vulnerabilidades y/o que tiene huecos de seguridad.

Esto es porque en el mundo de la tecnología la seguridad siempre va detras de los fallos, casi siempre hay fallas ocultas en estas tecnologías hasta que alguien decide hacerlas públicas. Por esta razón es que enigma es una capa adicional a los protocolos ampliamente usados, para ofrecer protección cuando las capas de seguridad de bajo nivel fallan o no se han actualizado aún.

De ahí la importancia de las noticias relacionadas a esta temática de seguridad, y las cuales fueron una motivación y justificación para la realización de este proyecto. Por esta razón hemos recopilado unas noticias relacionadas directamente con los protocolos y algoritmos de seguridad de bajo nivel, que pueden a ayudar a vislumbrar la magnitud del problema al que se enfrenta la tecnología.

◀ Anterior

Siguiente ▶

Inicio Documentación Investigación Acerca

FUENTES DE INVESTIGACIÓN

Introducción
Terminología
¿Qué es la encriptación?
Criptografía de la A-Z
Seguridad y Encriptación
SSL 128 bits
Lifetimes of cryptographic
Ataques al protocolo SSL

NOTICIAS RELACIONADAS

Introducción
OpenSSL corregirá fallos graves
Google 'hackea'
Evolución de la criptografía
El problema de los informáticos
Criptografía poscuántica
Cómo la criptografía ayuda
Criptografía en el punto de mira

OpenSSL corregirá el próximo jueves varios fallos graves de seguridad.

Fecha: 8-nov-2016

Heartbleed es, sin duda, el peor fallo de seguridad al que se ha enfrentado Internet. Este fallo de seguridad en las librerías OpenSSL, librerías de cifrado más utilizadas en todo el mundo, permitía a los usuarios recuperar datos de la memoria de los servidores remotos con total facilidad. Aunque este fallo fue solucionado al poco de darse a conocer, esta librería sigue dejando ver, cada poco tiempo, nuevos fallos de seguridad.

SITIO WEB ENIGMA – INVESTIGACIÓN

Google 'hackea' una herramienta clave de seguridad en Internet que se consideraba indescifrable

Fecha: 24-feb-2017

La compañía ha logrado probar que una herramienta de seguridad usada por empresas en todo el mundo es vulnerable, y promete publicar el código para que otros realicen su 'hackeo'.

Evolución de la criptografía y sus ámbitos de aplicación durante la última década

La tecnología criptográfica surge como consecuencia de la necesidad de proteger la información en las comunicaciones para que ésta no sea interceptada por terceros. No es algo nuevo. Los espartanos ya utilizaban la "Escitala", un sistema de codificación para proteger sus mensajes secretos, o los Templarios, que inventaron la primera carta de crédito segura.

A través de cuatro bloques, que publicaremos sucesivamente, repasaremos la evolución y usabilidad de la criptografía en la última década tanto en el ámbito financiero, cuando la banca comienza a utilizar sistemas de cifrado obligado por la normativa, en el ámbito de la Administración, dado el desarrollo de la Sociedad Digital y la popularización del uso de Internet y en el ámbito en el que esta tecnología es utilizada por los ciudadanos, es decir, la llegada del DNI Electrónico.

Haciendo un breve repaso, podemos decir que los primeros usos de la criptografía, tal como hoy la entendemos, únicamente era utilizada en el mundo militar, diplomático y gubernamental, para más tarde trasladarse al entorno financiero, coincidiendo con la utilización del código PIN como elemento de autenticación en las tarjetas de crédito.

Es a partir del año 2000, con la popularización del uso de Internet, cuando las organizaciones públicas y privadas toman conciencia de los riesgos inherentes al uso de las nuevas tecnologías, pero, sobre todo, de la necesidad de mitigarlos, implantando para ello medidas y mecanismos de protección de la identidad y del contenido de la información.

Como consecuencia de ello, los sistemas de cifrado en general, y el cifrado asimétrico en particular, pasan a tener un papel relevante en el mundo empresarial como instrumento para proteger la información, las comunicaciones y la identidad empresarial. Asimismo, las Administraciones Publicas comienzan a hacer uso de los sistemas de cifrado y firma electrónica como herramienta de seguridad para el impulso de los trámites y relaciones telemáticas con los administrados.

Ya en el año 2002, se pone en marcha el proyecto "DNI Electrónico", un documento de identificación personal, basado en una tarjeta Chip criptográfica, que permite al ciudadano identificarse y autenticarse de manera segura.

SITIO WEB ENIGMA – INVESTIGACIÓN

Inicio Documentación Investigación Acerca

FUENTES DE INVESTIGACIÓN

- Introducción
- Terminología
- ¿Qué es la encriptación?
- Criptografía de la A-Z
- Seguridad y Encriptación
- SSL 128 bits
- Lifetimes of cryptographic
- Ataques al protocolo SSL

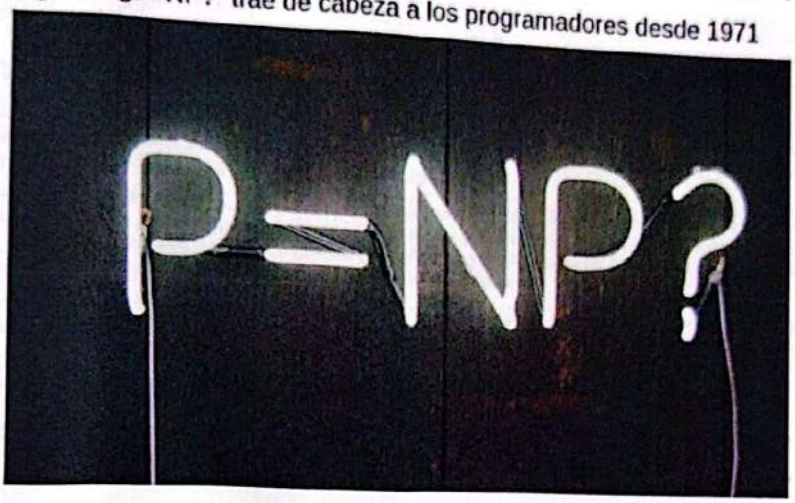
NOTICIAS RELACIONADAS

- Introducción
- OpenSSL corregirá fallos graves
- Google 'hackea'
- Evolución de la criptografía
- El problema de los informáticos
- Criptografía poscuántica
- Cómo la criptografía ayuda
- Criptografía en el punto de mira

El problema que los informáticos no han podido resolver en 45 años

La pregunta "¿P=NP?" trae de cabeza a los programadores desde 1971

Fecha: 22-may-2017



Inicio Documentación Investigación Acerca

FUENTES DE INVESTIGACIÓN

- Introducción
- Terminología
- ¿Qué es la encriptación?
- Criptografía de la A-Z
- Seguridad y Encriptación
- SSL 128 bits
- Lifetimes of cryptographic
- Ataques al protocolo SSL

NOTICIAS RELACIONADAS

- Introducción
- OpenSSL corregirá fallos graves
- Google 'hackea'
- Evolución de la criptografía
- El problema de los informáticos
- Criptografía poscuántica
- Cómo la criptografía ayuda
- Criptografía en el punto de mira

Criptografía poscuántica

¿Sabes qué? La criptografía es el tipo de tarea por la que los ordenadores cuánticos serán especialmente buenos.

La informática cuántica también podría ser la salvación o el fin para este nuevo mundo emergente. Como dijimos en nuestro boletín de seguridad de 2015, el modo en que existe la criptografía hoy en día terminará por desaparecer. La tesis que defiende que "la criptografía es uno de los muchos campos en que el conflicto antagonista continúa favoreciendo al defensor" será duramente refutada (por decir algo) hasta que se introduzcan unos algoritmos criptográficos poscuánticos efectivos.

Estos, a su vez, requerirán mucha más potencia informática de la que los ordenadores convencionales pueden otorgar. Pero, para salvación nuestra, la miniaturización y "comoditización" de los dispositivos cuánticos también es inminente, lo que significa que habrá más potencia informática disponible para defenderse de atacantes. Y el juego sin fin de "atacantes vs. defensores" continuará a un nuevo nivel.

Además de nuestro discurso sobre seguridad de información, tenemos esperanza en que los avances de la informática cuántica también lanzarán la realidad aumentada, la realidad virtual, la inteligencia artificial y otras aplicaciones que requieren muchos recursos.

En resumen: parece ser que los ordenadores cuánticos están llegando a ser una realidad. Todavía no puedes tocar uno, pero está bien ver que existen plataformas informáticas de ordenadores cuánticos que puedes comprobar con IBM o D-Wave. Dicha comprobación requiere cierto nivel de ingenio informático, por lo que la mayoría de la población mundial tendrá que esperar. Pero con más grandes invirtiendo en el esfuerzo, como Intel, IBM, Google y Microsoft, parece inevitable que veamos algún resultado práctico.

También hemos oído rumores de que Google quizá desvele un avance antes de finales de 2017, por lo que quizá no tengamos que esperar tanto.

FUENTE

Siguiente

Anterior

SITIO WEB ENIGMA – INVESTIGACIÓN

Inicio Documentación Investigación Acerca

FUENTES DE INVESTIGACIÓN

- Introducción
- Terminología
- ¿Qué es la encriptación?
- Criptografía de la A-Z
- Seguridad y Encriptación
- SSL 128 bits
- Lifetimes of cryptographic
- Ataques al protocolo SSL

NOTICIAS RELACIONADAS

- Introducción
- OpenSSL corregirá fallos graves
- Google 'hackea'
- Evolución de la criptografía
- El problema de los informáticos
- Criptografía poscuántica
- Cómo la criptografía ayuda
- Criptografía en el punto de mira

Cómo la criptografía en el DNS ayuda a reducir el abuso

Fecha: 9-abr-2015

En mi penúltima nota escribí acerca del Sender Policy Framework (SPF), que permite autorizar direcciones IP para el envío de email asociado a un nombre de dominio. Ahora me referiré al DomainKeys Identified Mail o DKIM, que es un estándar de Internet (ver RFC 4871) que permite reducir el spam, el phishing y otras cuantas formas de abuso.

Generalidades acerca de DKIM

Mientras que SPF es un servicio que permite determinar si una dirección IP está autorizada para enviar email asociado a un dominio, **DKIM permite determinar si el remitente del mensaje es en realidad quien él dice ser (autenticación) y si el mensaje fue alterado durante el tránsito del remitente al destinatario (integridad)**.

Funciona de manera sencilla, utilizando criptografía de llave pública: el remitente crea un par de llaves criptográficas, al igual que haría al usar PGP o GPG (llave pública y llave privada). Publica la llave pública como un registro de texto (o TXT record) en el archivo de zona de su dominio (vea al final de mi nota sobre SPF más información sobre archivos de zona y TXT records). Al enviar un mensaje, utiliza la llave privada para generar el hash (¿qué es un hash?) y firmarlo digitalmente.

Los servidores de correo utilizan la llave pública, que ha sido publicada como un recurso en el Sistema de Nombres de Dominio, para determinar si el mensaje es auténtico (enviado por quien se dice que lo envió) e íntegro (que permanezca inalterado desde su envío).

¿Cómo funciona DKIM en la práctica?

Esta imagen, que tomé prestada de mi colega Dave Piscitello -autor del blog securityskeptic.com y compañero de trabajo en la oficina- lo explica (la traducción al español es mía):

Inicio Documentación Investigación Acerca

FUENTES DE INVESTIGACIÓN

- Introducción
- Terminología
- ¿Qué es la encriptación?
- Criptografía de la A-Z
- Seguridad y Encriptación
- SSL 128 bits
- Lifetimes of cryptographic
- Ataques al protocolo SSL

NOTICIAS RELACIONADAS

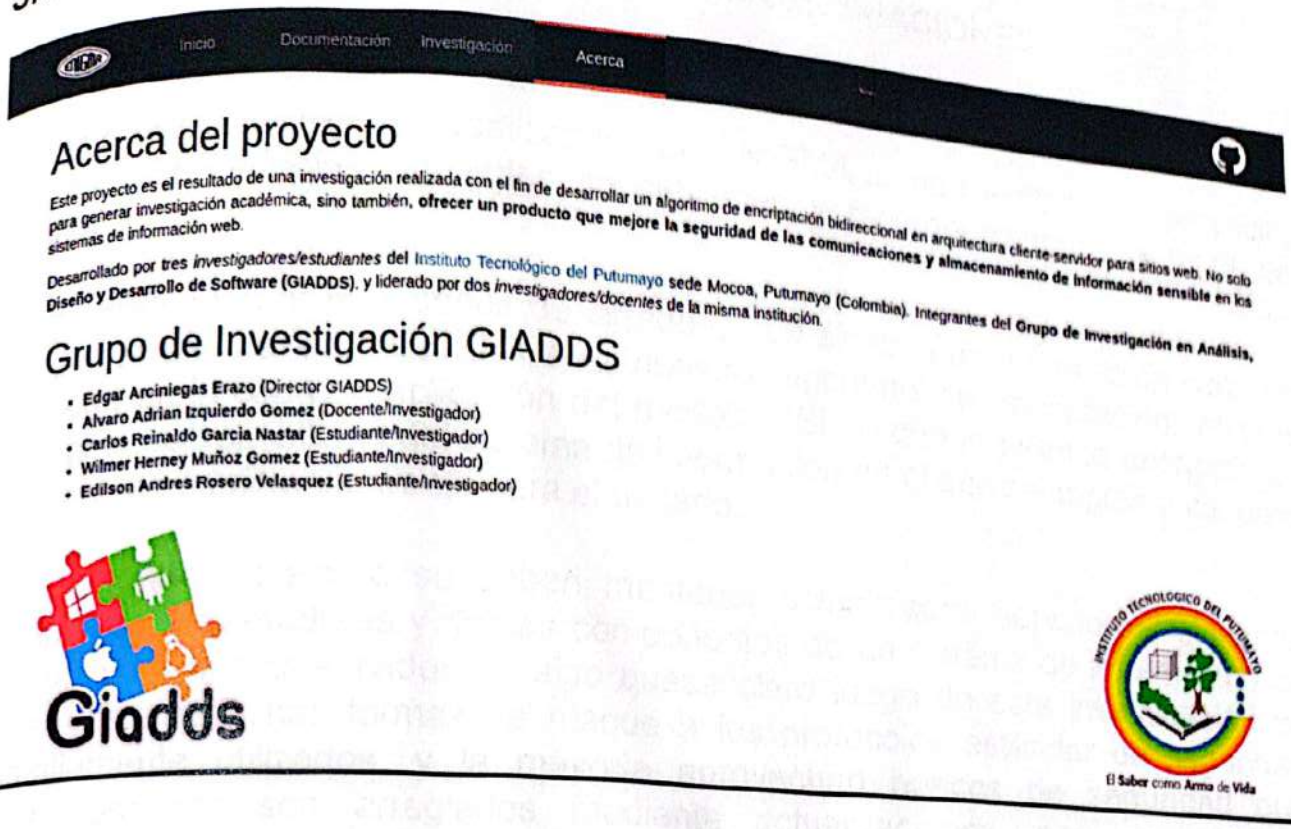
- Introducción
- OpenSSL corregirá fallos graves
- Google 'hackea'
- Evolución de la criptografía
- El problema de los informáticos
- Criptografía poscuántica
- Cómo la criptografía ayuda
- Criptografía en el punto de mira

Criptografía en el punto de mira

Fecha: 7-sep-2015

A principios del mes pasado, **un conflicto entre empresas de tecnología y administración en Estados Unidos detonó un debate** sobre si las compañías como Google y Apple deberían permitir a los usuarios que encripten su comunicación digital de tal manera que ni siquiera el FBI pueda descodificar la información. En otras palabras, el gobierno quiere que la encriptación sea más amigable para la policía.

SITIO WEB ENIGMA – ACERCA



9. CONCLUSIONES Y RECOMENDACIONES

A partir de la investigación realizada, y de ENIGMA como resultado del proyecto, hemos recopilado las siguientes conclusiones y recomendaciones a tener en cuenta.

Se pueden agregar más capas de cifrado en un sistema de información web, un claro ejemplo de esto es ENIGMA, nuestro algoritmo de encriptación, el cual funciona en la capa de aplicación del modelo OSI, lo que le permite encriptar sin afectar la compatibilidad del sistema de información en el que se implementa, pero a la vez, es semitransparente para el usuario.

Por seguridad, siempre se deben mantener actualizados servidores, sistemas operativos, navegadores y demás componentes de un sistema de información en arquitectura cliente-servidor. Si algo queda claro luego de esta investigación es que existen muchas formas de ataque a los protocolos estándar de seguridad ampliamente utilizados, y la mayoría aprovechan huecos de seguridad que posteriormente son arreglados mediante actualizaciones, pero que dichas actualizaciones muchas veces no son aplicadas por parte de los responsables.

Los algoritmos de encriptación y los protocolos de seguridad estándar no son garantía de seguridad. Como recomiendan los expertos en seguridad, el que un sistema sea seguro depende en gran medida de la cantidad de políticas de seguridad que se implementen tanto en los servidores como en los usuarios finales del sistema, y entre más políticas de seguridad se implementen más respaldo se tiene a la hora de mitigar las posibles fallas en alguno de los componentes, al menos mientras llegan las actualizaciones que parchan y corrigen dichos fallos.

No existe sistema 100% seguro. Por eso ENIGMA es una capa de cifrado adicional, y se recomienda utilizarlo de la mano del protocolo OpenSSL y las demás políticas de seguridad posibles. Siempre aplicando actualizaciones a todos los componentes del sistema de información.

Una vez que la computación cuántica sea asequible, los algoritmos de cifrado actuales quedarán obsoletos. Por lo que en su momento tendremos que utilizar nuevos mecanismos de cifrado y nuevos algoritmos que en la actualidad son sólo teoría, y que están pensados para ser inmunes a la computación cuántica.

Enigma actualmente funciona con php en el backend y javascript en el servidor, por lo que una recomendación a futuro es adaptar el algoritmo para funcionar con otros lenguajes de programación en el backend, como java, python, javascript, etc.

10. BIBLIOGRAFÍA

Jorge A. Monjarás. ¿Qué es la encriptación? Alto Nivel [en línea], 14 de mayo de 2017. Disponible en Internet: http://www.altonivel.com.mx/7581-que-es-la-encriptacion/

Cristian Borghello. Criptografía de la A-Z. Seguridad Informática [en línea], 14 de mayo de 2017. Disponible en Internet: http://www.segu-info.com.ar/proyectos/p1_criptografia.htm

Cristian Borghello. Protocolos Criptográficos y Estándares. Seguridad Informática [en línea], 14 de mayo de 2017. Disponible en Internet: http://www.segu-info.com.ar/proyectos/p1_protocolos-y-estandares.htm

Seguridad y Encriptación. Osmosis Latina [en línea], 14 de mayo de 2017. Disponible en Internet: https://www.osmosislatina.com/aplicaciones/seguridad.htm

SSL 128 bits. Certsuperior [en línea], 14 de mayo de 2017. Disponible en Internet: https://www.certsuperior.com/SSL128bits.aspx

Axpe. Criptografía en el punto de mira. Axpe Consulting [en línea], 14 de mayo de 2017. Disponible en Internet: http://www.axpe-blogs.com/noticias-tic/criptografia-en-el-punto-de-mira/

Carlos Alvarez. Cómo la criptografía en el DNS ayuda a reducir el abuso. EL TIEMPO [en línea], 14 de mayo de 2017. Disponible en Internet: http://blogs.eltiempo.com/el-lado-oscuro-de-internet/2015/04/09/dkimintro/

Sergey Lurye. Criptografía poscuántica. Blog Oficial de Kaspersky Lab [en línea], 14 de mayo de 2017. Disponible en Internet: https://blog.kaspersky.es/quantum-new-year/9931/

Valerie Aurora. Lifetimes of cryptographic hash functions. Valerie Aurora [en línea], 14 de mayo de 2017. Disponible en Internet: http://valerieaurora.org/hash.html