UNIVERSIDAD SAN PEDRO - CHIMBOTE

ESCUELA DE INGENIERIA INFORMATICA Y SISTEMAS

INVESTIGACION INFORMATIVA

"DESARROLLO DE UN SISTEMA CRIPTOGRAFICO USANDO RSA PARA EL CONTROL DE ACCESO DE LOS TRABAJADORESDE LA EMPRESA HAYDUK S.A.C CHIMBOTE, 2016"

Autores:

- Olano León Linkon Alexander.
- Laredo Meza Paris Antonio.
- Tume Naquiche Alexander Estevan.

Chimbote, 09 de octubre del 2016.

RESUMEN

Desde hace más de 2000 años, la criptografía ha caminado de la mano del hombre, y desde las campañas romanas hasta la Segunda Guerra Mundial, se ha encargado de determinar los vencedores y los vencidos. Poder disponer de un sistema que permita enviar un mensaje que solo pudiera ser leído por el destinatario objetivo ha sido y sigue siendo una necesidad crucial. La ciencia de la criptografía presente múltiples problemas, pero por ser un sistema destinado a usarse por unos pocos, siempre se han podido paliar con soluciones rudimentarias y poco creativas. Sin embargo, el mundo en el que vivimos hoy, la "Era de la Información", lleva todos estos problemas a una nueva dimensión, y por tanto requiere soluciones innovadoras y revolucionarias en campos tan modernos como la informática, y tan antiguos como las matemáticas.

El propósito de este proyecto es implementar una serie de herramientas que permitan los trabajadores de la empresa HAYDUK S.A.C. Chimbote, y así obteniendo los beneficios de la criptografía RSA, pudiendo enviar información cifrada con el resguardo y seguridad total de sus datos personales en el proceso del (área de control de acceso) en sus áreas de trabajo en su sistema informático de reconocimiento facial del control de acceso en los trabajadores de la empresa HAYDUK S.A.C. Chimbote, 2016.

Para el desarrollo del proyecto se utilizaremos API basados en la realización de la criptografía RSA, así como también emplearemos el lenguaje java para desarrollarlo y así como otras herramientas que optimicen el tiempo de desarrollo del proyecto y con el logro del objetivo a cumplirlo.

Con la implementación del API de Criptografía en el sistema experto se busca brindar el resguardo y seguridad de los datos de cada trabajador dentro de la empresa HAYDUK S.A.C. Chimbote para así restringir el acceso a posibles entidades secundarias no autorizadas, con el fin de lograr y obtener un mejor manejo administrativo de datos en el proceso del control de acceso de los trabajadores en la empresa HAYDUK S.A.C.

ABSTRACT

For over 2000 years, cryptography has walked hand man, and from the Roman campaigns until World War II, has been commissioned to determine the winners and losers. Able to have a system that allows only send a message that could be read by the recipient objective has been and remains a crucial need. The science of cryptography present many problems, but being a system to be used by a few, have always been able to overcome with rudimentary and not very creative solutions. However, the world in which we live today, the "Information Age" takes all these issues into a new dimension, and thus requires innovative and revolutionary solutions in such modern fields such as computer science, and as old as mathematics .

The purpose of this project is to implement a series of tools that allow workers the company HAYDUK S.A.C. Chimbote, and thus obtaining the benefits of RSA cryptography, and can send encrypted information receipt and complete security of their personal data in the process (area access control) in their work areas in the computer system of facial recognition access control workers HAYDUK SAC company Chimbote, 2016.

For the development of project-based use API performing the RSA cryptography, and also we will use the Java language to develop and as well as other tools that optimize the development time of the project and the achievement of the objective to comply.

With Crypto API implementation of the expert system aims to provide the safety and security of the data of each employee within the company HAYDUK S.A.C. Chimbote order to restrict access to potential secondary unauthorized entities, in order to achieve and get a better administration of data in the access control process of workers in the company HAYDUK S.A.C.

INTRODUCCION

Hoy en día las comunicaciones a través de canales abiertos (teléfono, bluetooth, VolP, Internet…) están a la orden del día. Desgraciadamente, existen muchas maneras en las que alguien interesado podría acceder a ellas. Muchas de estas comunicaciones, además contienen información valiosa, como datos bancarios, movimientos industriales, información personal. En resumen, información que en manos de las personas equivocadas puede ocasionar muchos problemas. Internet ofrece muchas maneras de proteger estos datos, pero muy pocas son capaces de detener a un intruso con el conocimiento o la dedicación necesaria.

Este proyecto pretende implementar una serie de herramientas que permitan a los trabajadores de la empresa obtener los beneficios de la criptografía RSA, pudiendo enviar información de sus datos al momento de acceder a cada área de trabajo mediante un sistema experto ya existente en dicha empresa. La principal ventaja de esta implementación es que pone al alcance de los programadores una tecnología que tiene una base matemática que en ocasiones resulta compleja de comprender. Gracias a ella, las matemáticas quedan ocultas al programador, que puede comunicar sus procesos de forma transparente, sin ser necesariamente consciente de como esa encriptación está sucediendo.

PROBLEMA

Planteamiento del problema

La administración del control de acceso de los trabajadores en una empresa es muy importante ya que permite a los jefes de áreas gestionar bienes o servicios para cada empleado.

El proceso de control de acceso es realizado por un software capaz de registrar los datos de cada trabajador.

Se concluye que la empresa HAYDUK S.A.C. ubicada en la ciudad de Chimbote existen dificultades y problemas en el proceso del control de acceso de sus trabajadores debido a que los datos de cada empleado quedan expuestos por la falta de seguridad en cuanto al resguardo de información de los datos personales de estos.

Formulación del problema

¿Cómo desarrollar un sistema criptográfico empleando RSA en el control de acceso de los trabajadores de la empresa HAYDUK S.A.C. de apoyo en la administración y la protección de los datos de cada empleado en la empresa HAYDUK S.A.C. Chimbote?

Antecedentes

David Kahn(1974) “Historiador estadounidense, periodista y escritor. Se ha dedicado casi exclusivamente a escribir acerca de la historia de la criptografía, de la inteligencia militar y de temas relacionados. Fue nombrado como doctor(DPhil) por la Universidad de Oxford en el área de Historia Moderna de Alemania.

Dr Jorge Ramió Aguirre (2000), Coordinador de la Red Telemática Iberoamericana de Criptografía y Seguridad de la Información (CriptoRed). También profesor de la Universidad Politécnica de Madrid, su intención es establecer un flujo de cooperación con todos los países de Iberoamérica en materia de seguridad informática.

Jeimy Cano (2006), "Facilitación y ampliación de un mejor método para atrapar a los hackers" Imparte cátedras relacionadas con delitos informáticos y computación forense, moderador de la lista seguridad informática de la ACIS.

Sergio de los Santos, "Ni los antivirus ni los cortafuegos protegen ya contra criminales informáticos (Hakers"), refiriéndose a la Rusian Businnes Network, una empresa de SanPertersburgo que vende servicios web para distribución de código maligno y phishing.

Marco Referencial

Internet es, hoy por hoy, un medio extremadamente inseguro. El hecho de que la mayoría de las redes que lo componen sean Ethernet o inalámbricas supone que siempre que un mensaje es emitido, este es distribuido a multitud de máquinas en su camino hasta el receptor. En general, estas máquinas están preparadas para ignorar los mensajes que no las incluyan como destinatarios, pero es peligrosamente sencillo configurar un ordenador para recuperar estos mensajes.

A continuación, veremos algunos de los sistemas criptográficos más empleados hoy en día. Se tratarán los medios más populares hoy en día sobre los que se basa la criptografía.

En primer lugar, veremos el protocolo TCP/IP, el más extendido en Internet por el momento, y sobre el que se basan la mayoría de las comunicaciones, así como sus características de cara a proteger la información.

Además, se explicará con detalle el algoritmo de cifrado RSA, aportándose la notación y explicaciones necesarias para comprender su funcionamiento, así como el de las aplicaciones desarrolladas en este proyecto.

Por otra parte, se describirán PGP y SSL, dos de las implementaciones criptográficas más extendidas hoy en día, y veremos que de hecho se basan en principios similares a la criptografía RSA, o incluso hacen uso de ella.

Por último, nos adentraremos en un presente que se diría que es ficticio, y en las posibilidades que nos brinda de cara a un futuro que ya podría estar aquí. Veremos cómo la llegada de la criptografía cuántica, hasta hace unos meses sólo una teoría, comienza a dar sus frutos, y a mostrarnos que la criptografía perfecta puede, de hecho, existir.

TCP/IP

El protocolo preferido en Internet, TCP/IP, ha ido evolucionando desde su inicio hasta convertirse en un protocolo con un compromiso bastante eficiente entre fiabilidad y latencia. IP se encarga de distribuir los datos por la red, y TCP aporta los matices de fiabilidad necesarios (puesto que se asegura de que los paquetes sean correctos, no se pierdan, y si se pierden vuelvan a ser transmitidos).

Desgraciadamente, este protocolo viaja sin cifrar, lo cual significa que cualquiera que se encuentre en alguna de las redes atravesadas por un mensaje puede acceder a su contenido. El envío de mensajes a través de TCP/IP parece, por tanto, una opción pobre a la hora de buscar privacidad en las comunicaciones, si bien por ser el protocolo más común en Internet, tendrá que servir de base para las comunicaciones que realicemos.

RSA

Ya hemos hablado en la Introducción Histórica de la evolución de la criptografía RSA. Aquí se detalla su funcionamiento, así como la notación que utilizaremos de ahora en adelante para referirnos a los diversos elementos que intervienen en ella.

PGP

PGP (las siglas de 'Pretty Good Privacy', o 'privacidad bastante buena') es otro estándar criptográfico creado por Philip Zimmermann, y que como RSA tiene por función el cifrado de mensajes o textos. Está comenzando a ser bastante popular debido en parte a sus implementaciones en código abierto, como OpenPGP.

Algunas de sus mayores ventajas son la posibilidad de cifrar archivos en un ordenador además de comunicaciones, o el uso de un algoritmo de compresión antes del cifrado, para reducir el tamaño del mensaje o texto (ver referencias W01 y W02).

SSL

SSL (Secure Sockets Layer) es un estándar de seguridad que permite el envío de mensajes privados entre nodos de una red. En general, su proceso consta de tres fases.

En la primera fase se decide qué algoritmo de encriptación se empleará para la comunicación (recordemos que SSL, al igual que PGP son estándares criptográficos, mientras que RSA es realmente un algoritmo). La implementación actual ofrece las siguientes opciones. En criptografía de clave pública están disponibles los algoritmos RSA, Diffie-Hellman (ambos descritos anteriormente), DSA y Fortezza. Además nos permitirá elegir algoritmos de otras categorías como el cifrado simétrico, o una serie de funciones hash. En la segunda fase se intercambian las claves, y en la tercera se procede al intercambio de mensajes cifrados.

La característica principal de SSL es que nos permite crear túneles seguros de comunicación hasta el punto en que una red completa pueda estar tunelada, dando lugar a una Red Privada Virtual, o VPN (ver referencia W01).

Criptografía Cuántica

Parece que nos encontramos en una época dorada de la criptografía, en la que si nos esforzamos un poco podemos tener una privacidad prácticamente total en nuestras comunicaciones a través de canales abiertos. Según Zimmerman, "Todos los ordenadores del mundo trabajando en paralelo tardarían 12 millones de veces la edad del Universo en descifrar un mensaje cifrado correctamente con PGP". Sin embargo, la historia nos demuestra que los sistemas criptográficos suelen tener algún fallo escondido que las termina haciendo vulnerables. Por tanto, debemos mantener siempre un ojo en los descubrimientos presentes y futuros (ver referencia L01).

La manera más fácil de descifrar mensajes correctamente cifrados es hacer uso de un 'atajo', o un 'hack' (haciendo uso del auténtico significado del término, que es descubrir cómo funciona algo para poder modificar alguna de sus características para obtener un mejor rendimiento) que se aproveche de alguna de las facetas no matemáticas de la encriptación. Un virus, troyano, puerta trasera… instalado en el ordenador de Alice haría que todos los mensajes cifrados que le lleguen puedan ser leídos por un intruso.

Sin embargo, eso no es una solución elegante (aunque sí resulte eficaz), de hecho, ni siquiera está en el campo del criptoanálisis (ciencia que se dedica a descifrar los mensajes cifrados mediante criptografía). Un criptoanalista intentaría en primer lugar buscar un error en el algoritmo (como ocurrió en el Implementación de una API Java de Criptografía RSA caso de Enigma, o en el de la más reciente encriptación WEP).

Desgraciadamente, el problema de factorización (obtener los factores de un número) sigue sin haber sido resuelto, hasta el punto que hay matemáticos que sostienen que seguramente no tenga solución. Quedaría aún una tercera manera para intentar romper RSA, que es contemplada en estos momentos la piedra angular de la criptografía (los documentos y comunicaciones más secretos del mundo siguen siendo cifrados con ella).

Si ocurriera una revolución tecnológica equivalente al nacimiento del ordenador, y que aumente la potencia de cálculo en la medida en que el ordenador lo hizo, sería concebible que un ataque de fuerza bruta sobre un mensaje cifrado con RSA pudiera obtener la solución en un margen de tiempo más cómodo, de horas o incluso minutos. Aquí entra en juego la cuántica. Un ordenador cuántico es a un superordenador actual lo que éste es a un ábaco estropeado. Sería capaz de realizar operaciones tan complejas en tan poco tiempo que desestabilizaría el concepto de privacidad. Un gobierno que pudiera contar con él tendría total control de las comunicaciones en el mundo.

Población y Muestra

Universo:

Trabajadores de la empresa HAYDUK S.A.C, Chimbote, 2016.

Población:

Trabajador de cada área de trabajo dentro de la empresa.

Muestra:

30 Trabajadores.

Variable:

Cuantitativa: Datos personales de cada trabajador.

Instrumentos

- ✓ Encuestas.
- ✓ Formularios.
- ✓ Opiniones.
- ✓ Recolección de Información (Gestor de base de datos)

Objetivos

Objetivos General:

Mejorar el control de acceso de los trabajadores de la empresa HAYDUK S.A.C. en cuanto al resguardo, seguridad y protección de los datos personales de cada empleado por medio del desarrollo de un sistema criptográfico usando RSA.

Objetivos Específicos:

- Cifrar el usuario de cada empleado.
- Mejorar la estabilidad del trabajo administrativo.
- El aporte de nuevas herramientas de seguridad y protección.
- Conocimientos previos de criptografía RSA.