Inter*net* Electronic Journal*

Nanociencia et Moletrónica

Julio 2009, Vol. 7, N°1, pp. 1323-1332

Algoritmo EPAR para Encriptación de Información en un Sistema Multiagentes

J. C. Ramírez Vargas, M. Salcedo Haro, B. E. Sanchez Rinza

Facultad de Ciencias de la Computación
Benemérita Universidad Autónoma de Puebla
Puebla 72000, **México**
jcramirezmx@gmail.com, miri_salcedo, brinza@hotmail.com

recibido: 15 de Marzo 2009 revisado: 29 de Marzo 2009 publicado: 31 de Julio de 2009

Citation of the article:
J. C. Ramírez Vargas, M. Salcedo Haro, B. E. Sanchez Rinza, Algoritmo EPAR para Encriptación de Información en un Sistema Multiagentes, Internet Electrón. J. Nanocs. Moletrón. 2009, Vol. 7, N° 1., pp 1323-1332

Algoritmo EPAR para Encriptación de Información en un Sistema Multiagentes

J. C. Ramírez Vargas, M. Salcedo Haro, B. E. Sanchez Rinza

Facultad de Ciencias de la Computación
Benemérita Universidad Autónoma de Puebla
Puebla 72000, **México**
jcramirezmx@gmail.com, miri_salcedo, brinza@hotmail.com

recibido: 15 de Marzo 2009 revisado: 29 de Marzo 2009 publicado: 31 de Julio de 2009

Internet Electron. J. Nanoc. Moletrón. 2009, Vol. 7, No.1,pp.1323-1332

Resumen
En un sistema multiagente como lo es un mercado electrónico donde la privacidad de los datos entre vendedores y compradores es un aspecto sumamente importante, el encriptamiento de la información es uno de los recursos que se pueden utilizar de forma que solo el receptor de dicha información pueda entenderla y por tanto, hacer uso de ella con plena autorización del emisor. EPAR es un algoritmo que ofrece una opción mas para encriptar la información en estos casos. Consta de dos partes, una de ellas es el cifrado por palabra con un algoritmo basado en principios matemáticos, y la otra es una revoltura de letras que utiliza técnicas matriciales y una llave que debe ser previamente conocida por ambos agentes (comprador y vendedor).

Abstract
In a multiagent system as it is an electronic marketplace where data privacy between sellers and buyers is a very important aspect, the encryption of information is a resource that can be used so that only the recipient of such information may understand and therefore use it with full authority of the issuer. EPAR is an algorithm that provides an option to encrypt the information in these cases. It consists of two parts, one is the word with a cipher algorithm based on mathematical principles, and the other is a letter revoltura matrix and employs a key that must be previously known by both agents (buyer and seller).

1. Introducción

El tema del pago en redes abiertas ha adquirido una gran relevancia en los últimos años debido al creciente desarrollo del comercio electrónico. Los sistemas de pago electrónicos deben proporcionar la infraestructura necesaria para facilitar el pago en las transacciones realizadas a través de la red Internet. Son tan importantes y necesarios que, de no llegar a soluciones satisfactorias, el desarrollo del comercio electrónico se podría ver seriamente frenado [1].
La criptografía es un elemento indispensable para proporcionar seguridad a las transacciones electrónicas, es esencial para proporcionar seguridad e intimidad en comercio electrónico y en e-business.
Sin usar la Criptografía es difícil crear la confianza que la gente y las empresas necesitan para hacer negocios y para realizar sus actividades de forma electrónica. Con el uso de la Criptografía:

a) Los individuos y los consumidores pueden realizar con seguridad sus operaciones financieras y comunicarse entre sí a través del web.
b) Las empresas pueden transmitir por Internet sus programas, músicas, informes y otras formas de propiedad intelectual minimizando los riesgos de una extendida piratería.
c) Las empresas pueden proteger su información en Internet, con la confianza de que esa información está protegida de ojos fisgones.
d) Las empresas pueden desarrollar productos de forma más rápida pues equipos de ingenieros de todo el mundo pueden colaborar en su diseño en tiempo real mediante redes seguras de alta velocidad [2].

Este documento se concentra en la privacidad de la información al hacer sus transacciones por Internet.
Los agentes son el recurso computacional mas utilizado actualmente para realizar dicho comercio electrónico, sobre todo con el surgimiento del m-commerce o comercio móvil, en cual el uso de agentes móviles facilita su realización, quedando como único problema el de la seguridad, privacidad e integridad de los datos que intercambian entre ellos. Y es en este punto, donde la criptografía toma gran importancia.
A lo largo de la historia se han empleado distintos sistemas de cifrado, siendo los tres principales: el de *transposición*, el de *sustitución,* y el de *ocultación*.
El primero de ellos consiste en colocar un fragmento cifrado en un lugar previamente conocido por el destinatario. Comprende todos los métodos que modifican el orden natural bien de las letras, de las silabas o de las palabras en un texto, trastocándolas o formando anagramas con ellas. Entre otros métodos de transposición se pueden citar: escítalo, alteración, Richelieu, telégrafo, enrejado, tabla, Soudart, etc. Por lo general, se emplea cuando los textos a cifrar no son muy extensos.
El sistema de sustitución consiste en reemplazar alguna letra del alfabeto por uno o más signos convenidos por los corresponsales. Engloba los métodos basados en sustituir los elementos del texto normal (letras, sílabas, palabras o frases), por una representación distinta a la original, que puede ser literal, numérica o estenográfica, es decir, figurativa. Algunos ejemplos de métodos de sustitución son: alfabeto Morse,

masónico, César, Guyot, Porta, Cechetti, benedictino, Tritemio, Hirsh, Jean, Collange, Beaufort, Jefferson, Lord Bacon, silábico, Ivry, tabla numeral, Fleissner, Bazeries, etc.
En el sistema de ocultación se incluyen aquellos procedimientos en los que el remitente transmite el contenido del mensaje de forma oculta o disfrazada. En consecuencia, este sistema abarca todas las argucias y artimañas empleadas a lo largo de la historia para conseguir que un criptograma sea leído únicamente por el destinatario, impidiendo su comprensión a quien no le ha sido empleado [3].
El algoritmo EPAR expuesto en el presente artículo, utiliza un método de sustitución por palabra DP y un método de transposición con llave privada TM. Es por esto que para su comprensión, es necesario mencionar las siguientes definiciones matemáticas.
Un *número primo absoluto o simple* es el que sólo es divisible por sí mismo y la unidad [4].
Teorema fundamental de la aritmética. Todo entero n ≥2 se escribe de manera única (excepto el orden de los factores) de la siguiente forma:

$$n = p_1^{\alpha 1} \ldots p_n^{\alpha n}. \qquad (1)$$

en donde los p_i son números primos distintos y los α_i son números naturales no nulos. Esta descomposición se llama la descomposición de n en factores primos absolutos [5].
El la sección 2 del presente artículo se describe el funcionamiento del mercado electrónico, así como el comportamiento de los agentes que interactúan en él, en la sección 3 se expone el análisis y diseño del algoritmo EPAR y se explican los dos algoritmos que lo conforman, en la sección 4 se muestra la implementación del algoritmo en el mercado, y por último en la sección 5 se dan algunas conclusiones y el posible trabajo futuro acerca de este.

2. Funcionamiento del Mercado

El objetivo de este trabajo es implementar una versión muy simple de un mercado automatizado en tiempo real. Un mercado es un recinto en el que continuamente se compra y vende productos o valores, es decir, cualquier cosa a la que se le pueda dar un precio. El precio de los bienes intercambiados fluctúa según la oferta y la demanda.
El mercado se encarga de gestionar las operaciones de compra y venta buscando automáticamente el precio más favorable y cumpliendo ciertas reglas de juego limpio (p/e, no se hacen distinciones personales, se atienden primero las solicitudes más viejas, etc).
El sistema recoge muchas de las reglas de funcionamiento de los auténticos mercados de valores (bolsas). Es un mercado muy sencillo en el que se intercambian 3 productos, p/e, naranjas, jitomate y limón. El mercado contiene dos operaciones: comprar y vender. Una persona interesada en comprar un producto lanzara al mercado una orden de compra, con unos parámetros determinados (cantidad y precio máximo a pagar). Por su parte, los vendedores comunicaran al mercado órdenes de venta, a la espera de que lleguen compradores. El mercado se encarga de “emparejar” cada orden de compra con la orden de venta que mejor encaje con sus condiciones. Una orden (compra o venta)

queda almacenada en el mercado hasta que éste la consigue ejecutar, es decir, emparejarla con una orden complementaria y ejecutar la transacción.
En esta versión simplificada supondremos que las órdenes de compra o venta son siempre por la misma cantidad de producto: 1 kilogramo.
El mercado esta controlado por un agente mercado, el cual esta encargado de iniciar el servicio mercado, así como de enviar avisos de apertura o cierre del mercado a los demás agentes que participan en el.
Así mismo existen agentes vendedores los cuales son los encargados de realizar las ventas de productos a los compradores existentes.
En este sentido puede verse al MOA como un sistema multiagente ya que se tienen a varios agentes interactuando entre si, para conseguir sus metas individuales, con una meta común global que consiste en el buen funcionamiento del mercado.

3. Algoritmo EPAR

El algoritmo EPAR está dividido en dos partes: la sustitución por palabras y la transposición de caracteres.
La sustitución por palabras (algoritmo DP), está basada en el Teorema Fundamental de la Aritmética ilustrado en la formula (1). Debido a que la descomposición en números primos de un número es cada vez mas complicada a medida de que este número crece, lo primero que se hace es ordenar por orden de aparición, de mayor a menor, las letras. Una vez en este orden se le asigna un número primo consecutivo a cada una de ellas, es decir, a la letra ‘e’ le correspondería el 2, a la letra ‘a’ el 3 y así consecutivamente. Tomamos una palabra del texto original, por ejemplo, ‘hola’, se sustituye cada letra por su número primo y se multiplican. El resultado de esta multiplicación se escribe seguido de un asterisco ‘&’ y un número que indica el orden de las letras.
Para hacer la transposición (algoritmo TM) de caracteres (en este caso números) se usa una llave privada de 13 posiciones. Con esta llave (ordenada) se forma una matriz con 13 columnas, la cual es llenada con los caracteres del texto a transponer de forma horizontal. Se desordena la llave y a su vez todo el contenido de la matriz. Por ultimo, se escribe el contenido de la matriz de forma vertical en el texto transpuesto[1].
Los algoritmos para descifrar el texto, TMI y DPI, después de haber aplicado estos dos algoritmos son deducibles. Para el algoritmo TMI solo se tiene que formar la matriz ahora con la llave desordenada, llenar la matriz de forma vertical con las letras del texto cifrado. Se orden la llave y a su vez todo el contenido de la matriz. Se va sacando de forma horizontal los datos de la matriz, lo cual nos va dar el texto ordenado.
Ahora, para el algoritmo DPI, se identifica por palabra el número compuesto y el número de orden. Se descompone el número compuesto en números primos, se mapean estos números primos a sus correspondientes letras y posteriormente se ordenan de acuerdo al número de orden.
La única forma de obtener el texto original a partir del texto cifrado es conociendo la llave, y aplicando estrictamente en ese orden, el algoritmo TMI y DPI.

[1] Si existe algún carácter de salto de línea, permanece en la misma posición que en el texto original.

4. Implementación del Sistema

El sistema se desarrolló sobre la plataforma JADE (Java Agent DEvelopment Framework), que es un sistema de software totalmente implementado en el lenguaje JAVA. Simplifica la implementación de sistemas multi-agentes a través de un “middle-ware” que cumple con las especificaciones de la FIPA y contiene un conjunto de herramientas gráficas que soportan las fases de depurado y despliegue. La plataforma del agente puede ser distribuida a través de máquinas (que no necesariamente comparten el mismo sistema operativo) y la configuración puede ser controlada vía una interfaz gráfica remota.

4.1 Agentes en JADE

Un agente esta basado en "behaviours" o comportamientos, estos representan una tarea que un agente puede realizar.

Los comportamientos se pueden agrupar en tres grandes grupos:

i. Comportamientos one-shot: Comportamientos que se ejecutan de manera casi instantánea, y solamente una vez.

ii. Comportamientos cíclicos: Comportamientos que nunca son sacados del conjunto de comportamientos del agente y cuyo método action() siempre ejecuta el mismo código; por lo tanto, nunca finalizan.

iii. Comportamientos genéricos: El código que se ejecuta en ellos depende del status del agente, y eventualmente finalizan su ejecución.

Para la implementación de alguno de estos tipos de comportamientos sólo basta con heredar de la clase jade.core.behaviours.Behaviour, y para lograr que un agente ejecute la tarea implementada por un objeto behaviour, es suficiente con agregar el comportamiento al agente por medio del método addBehaviour() de la clase Agent. Los comportamientos pueden ser agregados en cualquier momento, cuando un agente inicia (en el método setup()) o dentro de otros comportamientos [6]. Toda clase que herede de la clase behaviour, debe implementar el método action() que es donde se incluye el código de las acciones correspondientes.

Cada una de las tareas de los agentes que conforman el sistema son implementadas en base a algunos de los tipos de comportamientos previamente citados.

4.2 Algoritmo EPAR

La implementación del algoritmo EPAR se puede dividir en 2 partes: la sustitución por palabra (DP), y la transposición de las letras (TP).

El algoritmo para la DP es el siguiente:

1. Obtener la primera letra de la palabra.
2. Sustituir esta letra por su número primo correspondiente y guardarlo en un arreglo llamado ‘primos’.
3. Verificar la siguiente letra a cifrar:

a. Si es una letra, obtenerla y regresar al paso 3.
b. Si es un espacio (ya acabó la palabra),
    i. Ordenar el arreglo ‘primos’
    ii. Multiplicar todos estos números primos
    iii. Escribir este resultado, seguido de ‘&’ (amperson), seguido del orden de la palabra basado en el arreglo ‘primos’.
4. Obtener la siguiente palabra del texto original y regresar al paso 2.

Este procedimiento se repite hasta que todas las letras del texto original estén cifradas[2].

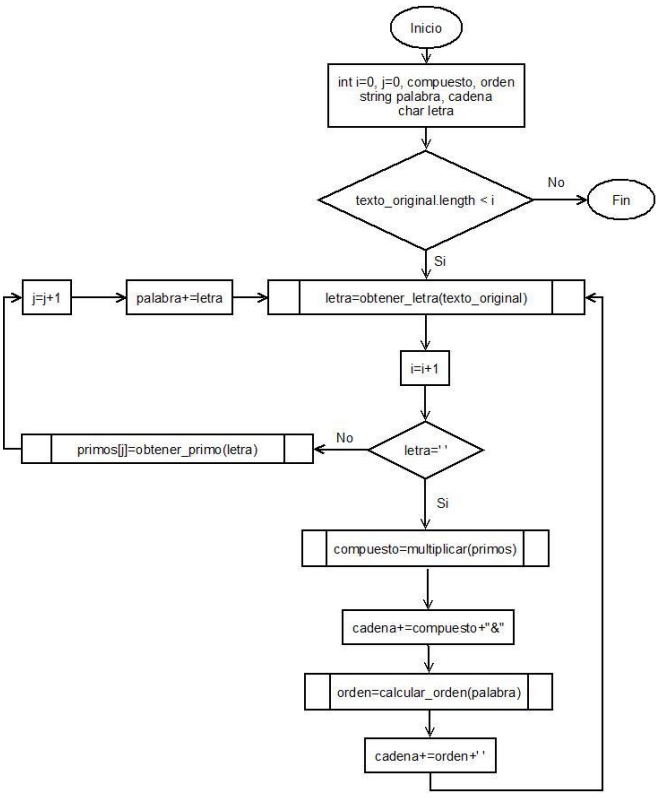

Diagrama 1. Diagrama de flujo del algoritmo DP.

El algoritmo para la transposición de las letras TM, es el siguiente:

1. Guardar en un arreglo el orden de las trece posiciones, es decir, la llave.
2. Crear una matriz de 13 columnas
3. Obtener el primer carácter del texto cifrado con la DP[3].
4. Colocar este carácter en la posición (0,0) de la matriz.
5. Obtiene el siguiente carácter del texto cifrado con la DP.

[2] En este procedimiento solo de cifran letras y números, conservando espacios y otros caracteres especiales.
[3] Si este carácter es un salto de línea, se guarda la posición de éste en un arreglo de saltos de línea, para posteriormente ubicarlos en la misma posición original.

6. Colocar este carácter en la siguiente posición de manera horizontal, de la matriz y regresar al paso 5, hasta que todos los caracteres del texto original se encuentren en la matriz.
7. Transponer las columnas de la matriz según el orden de la llave.
8. Obtener los caracteres de forma vertical de esta matriz transpuesta, y agregarlos a la variable cadena de salida que contendrá el texto cifrado.

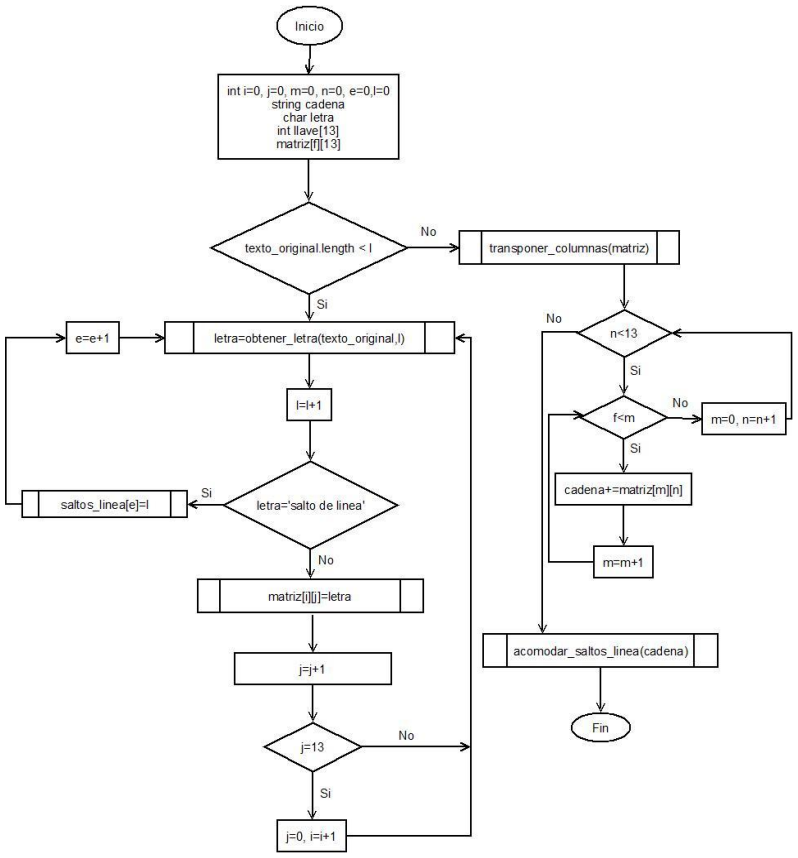

Diagrama 2. Diagrama de flujo del algoritmo para la transposición de letras.

El algoritmo de descifrado DPI es el siguiente:

1. Obtener el primer numero del texto hasta el separador '&'.
2. Realizar factorizacion de este numero en numeros primos
    a. Dividir el numero entre los primos
    b. Si el modulo es cero se guarda ese primo en un arreglo de primos
    c. el numero es el resultado de la division por ese primo
    d. se repite desde a. hasta que el resultado sea 1
3. Leer el orden despues del '&'.
4. Reordenar el arreglo de primos obtenido en 2 en base al orden obtenido en 3
5. Mapear el arreglo de primos en base a las letras originales
6. Insertar el arreglo en la salida hacia el texto original
7. Si no ha terminado el texto repetir desde 1.

El algoritmo de descifrado para la transposición de las letras TMI, es el siguiente:

1. Guardar en un arreglo el orden de las trece posiciones, es decir, la llave.
2. Crear una matriz de 13 columnas
3. Obtener el primer carácter del texto cifrado.
4. Colocar este carácter en la posición (0,0) de la matriz.
5. Obtiene el siguiente carácter del texto cifrado.
6. Colocar este carácter en la siguiente posición de manera.

5. Conclusiones y trabajo futuro

El algoritmo EPAR es una opción mas para el cifrado de mensajes, que logra mediante la combinación de dos algoritmos, el manejo de información de una forma más segura.
El algoritmo es mejorable en cuanto a nivel seguridad, ya que si la llave privada es descubierta se puede descifrar el algoritmo TM. Y en cuanto al algoritmo DP es mejorable si se encontrara la forma de que no se extendiera tanto la longitud del texto cifrado. Sin embargo, representa un recurso más para conservar la privacidad e integridad de los datos en los mercados electrónicos.

Referencias

[1] Huguet i Rotger, L.; Ferrer Gomila, J.L.: Aplicaciones Criptográficas en Entornos Económicos. Protocolos Criptográficos y Seguridad en Redes. Servicio de Publicaciones de la Universidad de Cantabria (2003).
[2] Cohen, W.; Reno, J.; Lew, J.; Daley, W.: Preserving America's Privacy and Security in the Next Century: a Strategy for America in Cyberspace. NOVATICA, (1999).
[3] Galende, J.: Sistemas Criptográficos empleados en Hispanoamérica. Revista Complutense de Historia de América. (2000).
[4] Baldor, A.: Aritmética. Ed. Cultural Centroamericana, Guatemala (1974).
[5] Fúster, A.; De la Guía, D.; Hernández, L.: Técnicas Criptográficas de Protección de Datos. Alfaomega, 2da. Edición (2001).
[6] Caire, G.; JADE Programming-Tutorial-for-beginners, JADE Documentation, p 8, 2003.
http://galeon.hispavista.com/lasinterredes/cifrado1.htm