Algoritmo de encriptación de archivo de texto plano

Algorithm of encriptación of file of plain text

Alejandro Junior Huahuala Chaupi*

http://dx.doi.org/10.21503/CienciayDesarrollo.2010.v11.08

RESUMEN

El presente proyecto es del tipo exploratorio y trata acerca de la implementación de un algoritmo de encriptación basado en el método de Hills y RSA, por el cual se leen las líneas de un archivo de texto plano, para luego ser codificado o decodificado según el proceder del usuario.

Trabajamos con el código ASCII para la aplicación del algoritmo, debido a que el algoritmo se basa en aritmética modular. Las características notables del algoritmo son:

- Facilidad de conversión de cualquier carácter que pertenezca al código ASCII.
- Uso de dos claves de conversión diferentes para el cifrado y descifrado.
- Uso de cifras numéricas grandes para la generación de las claves (de 101 a 99999).

Palabras clave: *aritmética modular, algoritmo de Euclides, algoritmo de Euclides extendido, algoritmo de potencia modular, criptograma, base modular.*

ABSTRACT

This project is exploratory and is about the implementation of an encryption algorithm based on the method of Hills and RSA. Reading the lines of a plain text file, then be encoded or decoded by the user to proceed.

We work with the ASCII code for the implementation of the algorithm, because the algorithm is based on modular arithmetic. Notable features of the algorithm are.

- Easy conversion of any character that belongs to the ASCII code.
- Using two different conversion keys for encryption and decryption.
- Using large numerical figures for the generation of keys (101 to 99999).

Key words: *arithmetic modulate, algorithm of Euclides, algorithm of extended Euclides, algorithm of power to modulate, cryptogram, base modulate.*

* Alumno de la Escuela Académico-Profesional de Ingeniería de Sistemas e Informática, Filial Arequipa.

DOI: http://dx.doi.org/10.21503/CienciayDesarrollo.2010.v11.08

INTRODUCCIÓN

La necesidad de protección de información va en aumento a la par con el desarrollo tecnológico; debido a esto se plantea formular nuevas alternativas de encriptación para ser aplicadas. Ningún algoritmo de encriptación es óptimo, pero según el grado de seguridad del algoritmo, el tiempo que tardaría descencriptar la información variaría entre 100 y 300 años. Y usando una supercomputadora, entre 5 y 10 días.

Trabajando con algoritmos de encriptación como Hill y RSA se unirán características de comportamiento para la generación de un algoritmo derivado que contenga su comportamiento.

Problema de la investigación

Debido a que el algoritmo trabaja con aritmética modular, el cálculo de números primos grandes o el cálculo de exponentes modulares enormes, consume muchos recursos del sistema y un lenguaje de programación como .NET, que no soporta grandes números.

Debido a esto, inicialmente el algoritmo trabajaba con números no muy grandes, lo que significaba que el nivel de seguridad no era lo suficientemente eficiente.

Por la misma razón, se aplicaron algoritmos matemáticos como el algoritmo de Euclides, el algoritmo de Euclides extendido y la potencia modular.

Objetivo de la investigación

Encriptar un archivo de texto plano usando los algoritmos de HILL y RSA.

Justificación e importancia

El proyecto es importante por la necesidad de seguridad de los documentos digitales de texto plano, lo cual beneficiará a los usuarios informáticos a mantener su información segura.

- **Importancia para la investigación.** Es importante porque de esta forma se aportará con conocimiento generado a través de la experiencia de la investigación, lo cual servirá de referencia para futuras investigaciones.

- **Importancia para la Sociedad.** El resultado de la investigación brindará nuevas opciones para el público, opciones de seguridad para los documentos digitales de texto plano.

MATERIAL Y MÉTODO

Descripción de la solución

Para tener una mejor idea de cómo se encripta y desencripta una palabra, a continuación tenemos las siguientes pruebas de escritorio:

Datos:

Base Modular:	33
Llave Pública:	3
Llave Privada:	7

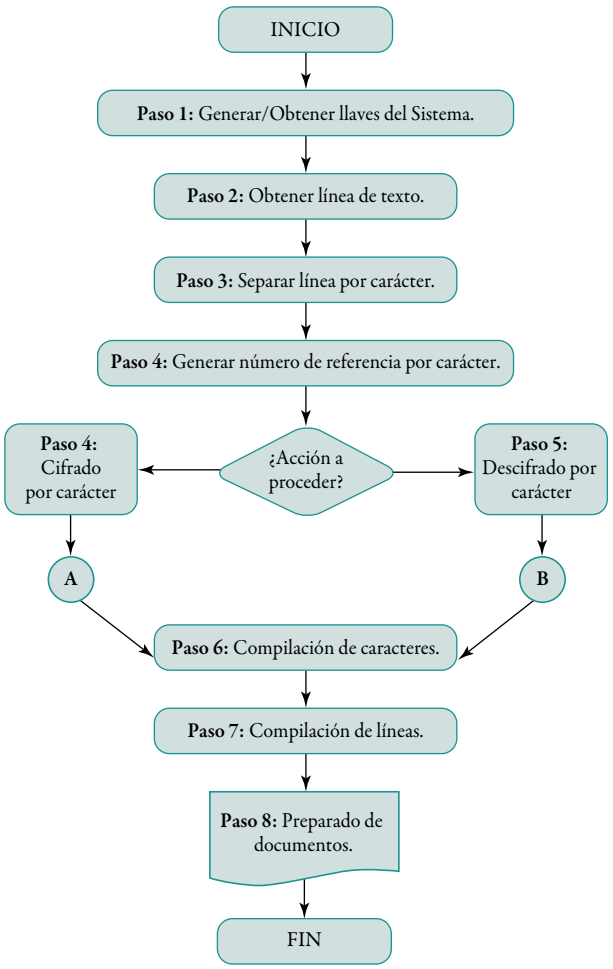
Encriptación:

SIMBÓLICO	NUMÉRICO	p^3	p^3 (mod 33)
C	05	125	26
A	01	1	01
S	19	6859	28
A	01	1	01

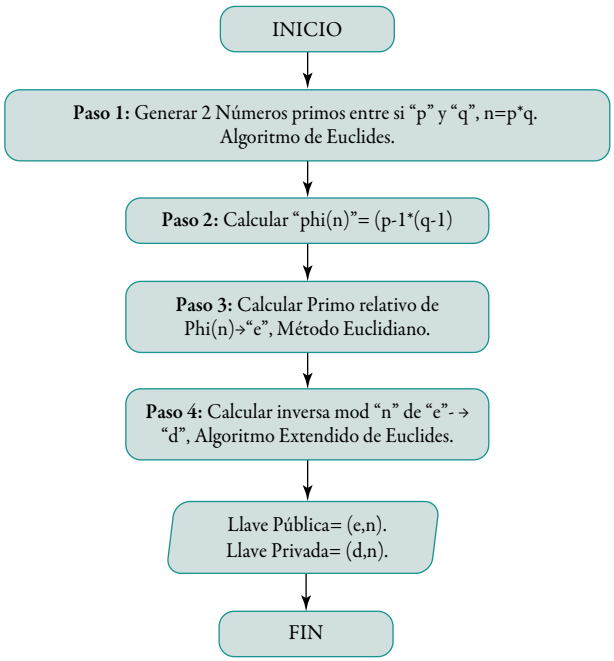
Desencriptación:

TEXTO CITADO (C)	C^7	C^7 (mod 33)	SIMBÓLICO
C	8031810176	5	C
A	1	1	A
S	13492928512	19	S
A	1	1	A

Algoritmo principal



Algoritmo de generación de claves



Requisitos funcionales:

- **Req 01**. Verificar archivo
- **Req 02**. El sistema debe cargar el texto del documento y empezar el cifrado.
- **Req0 3**. Al final del cifrado el sistema debe mostrar opciones de elegir llave generada por el sistema o generada manualmente.
- **Req 04**. En el caso del descifrado también se deben mostrar las opciones mencionadas en Req 03 (en caso de no contar con dichas opciones).
- **Req 05**. En el caso del descifrado, el sistema debe brindar también la opción de almacenar en cualquier tipo de archivo de texto plano como doc, txt e ini.

RESULTADOS

Se desarrolló un DLL el cual cuenta con la funcionalidad y el control de medida para el cifrado y descifrado de archivos de texto plano; esto con el fin de poder modificar y mejorar el algoritmo para aumentar su eficacia.

Se encontró también que solo se pueden encriptar archivos de texto plano sin formato, debido a que si presentara algún tipo de formato el resultado de descifrado generará errores de archivo.

CONCLUSIONES

- El Algoritmo RSA varía en su modalidad, pero la base en aritmética modular es inmodificable.
- La dll generada es reusable y puede ser mejorada, según los requerimientos.
- El tiempo de encriptación es más largo que el tiempo de desencriptación.

- El manejo de control de contraseñas es de vital importancia al momento de aplicar seguridad.

TRABAJOS FUTUROS

- Se recomienda realizar la complementación de una base de caracteres basada en álgebra lineal y el principio del CAOS o pseudo impredecible, para desplazar el código ASCII y aumentar el grado de seguridad.
- Se recomienda realizar empaquetamiento de archivos de texto plano cifrado, durante el proceso de cifrado o al final del proceso.

REFERENCIAS BIBLIOGRÁFICAS

1. Sergio Rajsbaum. *Publicaciones Preliminares* No. 632 (marzo 1999) Instituto de matemáticas UNAM. .
2. *http://www.programatium.com/asp/index.htm.*
3. *www.chilkad.com.*
4. *www.elguille.com*.
5. Universidad Tecnológica de Pereira. "Encriptación de señales binarias por medio de wavelets seudocaóticas". *Scientia Et Technica*, mayo, año/Vol. XIII, número 034. .
6. Carrillo, A. *Sincronización de caos con aplicación en enmascaramiento de señales*. Instituto de Física, Universidad de Antioquia.
7. *http://www.devjoker.com/asp/ver_contenidos.aspx?co_contenido=2*
8. *http://neo.lcc.uma.es/evirtual/cdd/tutorial/presentacion/ejmrsa.html*