SEGURIDAD EN REDES. DISEÑO E IMPLEMENTACIÓN DE UN CIFRADOR DE DATOS POR MEDIO DE DES TRIPLE.

RESUMEN
El propósito de este proyecto es diseñar e implementar una función lógica que permita representar el funcionamiento del algoritmo de cifrado de datos DES TRIPLE (TDES). El diseño de esta función lógica se llevará a cabo utilizando el lenguaje VHDL que es un lenguaje de descripción de hardware y, la implementación se hará sobre un dispositivo lógico programable (PLD) de muy alta escala de integración (VLSI) como lo son las FPGA.

Este proyecto se encuentra contemplado dentro de la línea de REDES Y COMUNICACIONES del grupo de investigación Sirius de Ingeniería de Sistemas y Computación.

PALABRAS CLAVES: DES TRIPLE, VHDL, PLD, FPGA.

ANA MARIA LÓPEZ ECHEVERRY
Ingeniera Electricista
Docente Programa Ingeniería de Sistemas y Computación.
Universidad Tecnológica de Pereira
anamayi@utp.edu.co

DIEGO FERNANDO ROJAS RINCÓN
Aspirante a Ingeniero de Sistemas y Computación.
diefer@utp.edu.co

ABSTRACT
The aim of this Project is to represent the cipher algorithm TDES of data trough the design and implementation of a logical function. The design of the logical function will be done with the very high description language VHDL, that is a language of description of hardware, and the implementation will be done in a programmable logical device (PLD) of high level scale of integration (VLSI) as are the FPGA´s.

The Project is framed in the line of research of communications and networks of the Research Group Sirius, that belongs to the program of Engineering Systems.

KEYWORDS: TDES, VHDL, PLD, FPGA.

1. INTRODUCCIÓN

Las redes de computadores han sido uno de los grandes adelantos hechos por el ser humano en el campo de las comunicaciones ya que permiten el envío de información de un lugar a otro de manera rápida, sin importar la distancia que se encuentren separados.

La seguridad que la red le pueda ofrecer a sus usuarios es un punto importante ya que ¿a quien le gustaría que la información que esta enviando sea vista por una persona no autorizada? Por la red se pueden enviar desde simples cartas familiares hasta documentos de negociaciones importantes de empresas; sin importar el documento que sea enviado la red debe estar en la capacidad de brindar la seguridad necesaria para que este llegue a su destino sin ningún tipo de alteraciones y sin haber sido visto por personas no autorizadas.

Ahora surge otra pregunta ¿existen personas que se dediquen a tratar de vulnerar la seguridad de una red? La respuesta es SI, se les llama HACKERS ó piratas informáticos. Algunas de estas personas solo lo hacen por diversión, por demostrar sus grandes habilidades y conocimientos en el campo de la informática. Pero otros lo hacen con el fin de apoderarse de la información que se esta transmitiendo, bien sea para modificarla o para hacer uso de esta para bien propio.

2. ESQUEMA GENERAL DEL ALGORITMO DES

DES (Standard de cifrado de datos) tiene como entradas, para su funcionamiento, un dato y una clave de 64 bits cada uno.

Al inicio y final del algoritmo se aplican dos permutaciones al dato que poseen la característica particular, que una es la inversa de la otra. Luego de la aplicación de la primera permutación el dato es pasado por dieciséis rondas de cifrado en las cuales se hace necesaria la utilización de unas subclaves que son obtenidas a partir de la clave que se ingresa al inicio del algoritmo, en total son dieciséis subclaves una para cada ronda. Al terminar el total de las rondas de cifrado se aplica la ultima permutación y de esta manera se obtiene un dato cifrado por medio del algoritmo DES.

Fecha de Recepción: 31 Agosto de 2006
Fecha de Aceptación: 27 Febrero de 2007

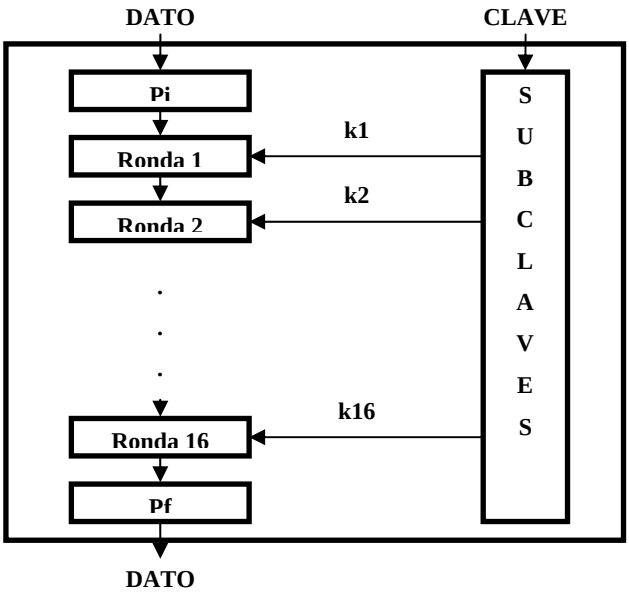

Figura 1. Esquema general del algoritmo des.

3. SIMULACION DE DES TRIPLE

DES TRIPLE es aplicar tres veces el algoritmo DES en un orden especifico. Primero se cifra el dato con una clave, el resultado de esto es descifrado con otra clave y por ultimo el resultado del descifrado es cifrado nuevamente. La clave que se emplea en este último paso puede ser la primera clave utilizada o puede ser una nueva clave.

Para el desarrollo de la función lógica que simula el funcionamiento de DES TRIPLE se utilizo un lenguaje de descripción de hardware como es VHDL.

3.1 Simulación de DES TRIPLE con 3 claves iguales.

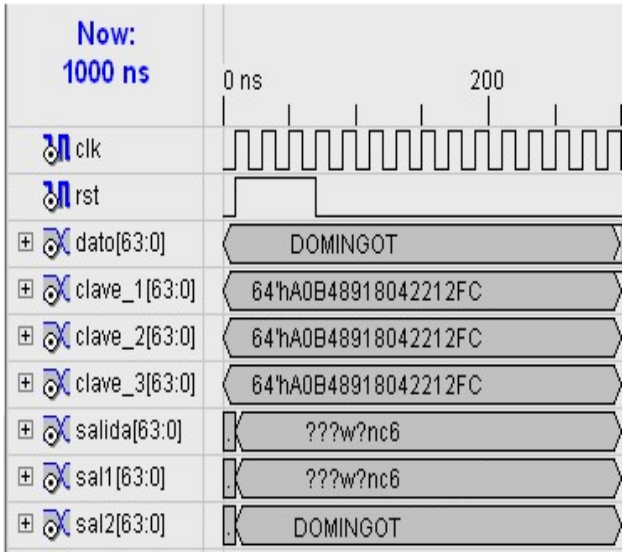

Figura 2. Simulación de DES TRIPLE con 3 claves iguales.

El propósito de realizar la simulación con las tres claves iguales es poder demostrar que la función esta funcionando correctamente.

La figura 3.1 muestra el resultado de esta simulación, en esta se pueden ver los siguientes datos:

Clk: reloj de la función, se encarga de la sincronización de los procesos durante la ejecución de la función.

Rst: reset, reinicia todas las variables que intervienen en la aplicación de la función.

Dato: texto que se desea cifrar.

Clave_1, clave_2 y clave_3: claves usadas para la aplicación de cada ronda del algoritmo DES.

Salida: resultado final de la aplicación de DES TRIPLE al dato.

Sal1: resultado de la primera aplicación del algoritmo DES (cifrado).

Sal2: resultado de la segunda aplicación del algoritmo DES (descifrado).

En DES se utiliza la misma clave y el mismo algoritmo tanto para cifrar como para descifrar, lo único que debe hacerse es invertir el orden de aplicación de las subclaves.

Si se observa el resultado de la simulación se tiene que existen datos iguales, por ejemplo **dato** y **sal2**, **salida** y **sal1**, esto debido al hecho de estar aplicando la función lógica con las tres claves iguales. La primera aplicación del algoritmo DES tiene como entradas a **dato** y **clave_1** y el resultado obtenido es **sal1**. Para la segunda aplicación de DES las entradas son **sal1** y **clave_2** y la salida es **sal2**, en este punto se puede observar que **dato** y **sal2** son iguales y esto es porque se esta utilizando la misma clave para cifrar y descifrar. Para la tercera aplicación de DES las entradas son **sal2** y **clave_3** y el resultado es **salida** que también es el resultado final de la función lógica, aquí se puede ver que salida y sal1 son iguales y esto se debe ha que las entradas en la primera y ultima aplicación de DES son iguales por lo tanto los resultados deben ser iguales.

Aunque el aplicar la función lógica con las tres claves iguales es de gran ayuda para comprobar que esta se encuentra funcionando correctamente, en la practica no sirve de nada porque es como si solo estuviera aplicando una vez el algoritmo DES.

3.1 Simulación de DES TRIPLE con 3 claves diferentes.

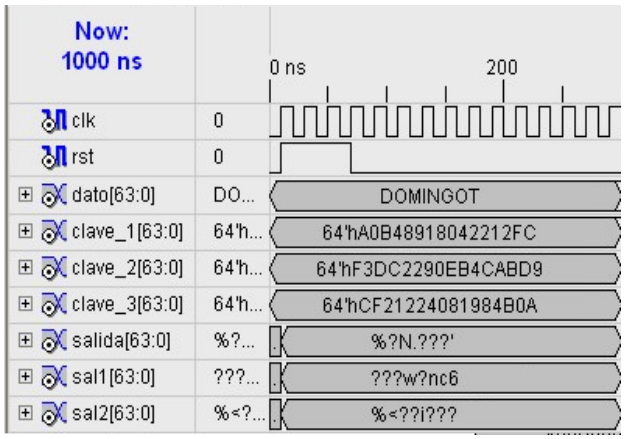

Figura 3. Simulación de DES TRIPLE con 3 claves diferentes.

En la figura 3 se puede observar el resultado de la simulación de la función lógica aplicándola con tres claves diferentes, lo cual corresponde al caso practico ideal ya que la longitud de la clave es de 192 bits lo que brinda mayor seguridad. En este caso se puede observar que no hay datos iguales debido a que cada aplicación del algoritmo DES se esta realizando con claves distintas. Es de anotar que el resultado final **salida** es el dato que viajará a través de los medios de comunicación, garantizando que incluso si se presenta un análisis de tráfico, esta información no tendrá ningún valor para quien realice el ataque, ya que solamente el dispositivo final de la información estará en capacidad de ejecutar el algoritmo de manera inversa para obtener el dato original.

4. CONCLUSIONES Y RECOMENDACIONES

Se pudo establecer que la criptografía es una herramienta fuerte que permite el mejoramiento de la seguridad en las redes.

Permite la manipulación de datos a nivel de cada uno de sus bits, permitiendo esto un desarrollo más simple de la función lógica que simula el algoritmo DES TRIPLE.

Se adquirió un nivel de conocimiento en el lenguaje de descripción de hardware (VHDL) tal que permitió el desarrollo de una función lógica de buen desempeño en la simulación del algoritmo de cifrado.

Este proyecto servirá de base para el desarrollo de un dispositivo de cifrado que permitirá brindarle a la región un producto con el cual se podrá mejorar la seguridad de las redes de transmisión de datos.

Se avanzó en el manejo de la herramienta Xilinx ISE, lo cual permitió el desarrollo de la función lógica sobre la cual se pudieron realizar las simulaciones de funcionamiento durante todas las etapas del proyecto.

Se logró dar un paso importante en el desarrollo de la tecnología de cifrado que permitirá mejorar los niveles de seguridad en la transmisión de datos a través de una red.

Se logró obtener un conocimiento tal del funcionamiento del algoritmo DES que permitirá que las nuevas generaciones de estudiantes logren alcanzar un nivel más alto en los desarrollos que se realicen acerca de seguridad en redes.

La función lógica resultante requiere el uso de un dispositivo lógico programable con mejores características, razón por la cual se recomienda realizar la implementación en una FPGA Spartan 3E xc3s1200e con el propósito de obtener un producto terminado.

El grupo de investigación Sirius le dará continuidad al presente proyecto con el objetivo de llegar a un desarrollo optimizado de la función lógica, con el propósito de que esta pueda ser implementada en una tarjeta FPGA cuyo costo permita ofrecer un prototipo de un producto (cifrador – descifrador) económico y eficiente.

5. BIBLIOGRAFÍA

[1]. FLOYD, thomas l. Dispositivos electrónicos. Editorial Limusa S.A de C.V., México, 1996.

[2]. FLOYD, thomas l. Fundamentos de electrónica digital. Editorial Limusa S.A de C.V., México, 2001.

[3]. LUCENA LÓPEZ, Manuel José. Criptografía y seguridad en computadores.

[4]. LUIS, terés y otros. VHDL Lenguaje estándar de diseño electrónico. McGraw Hill / Interamericana de España, S.A.U, España, 1997.

[5]. STALLINGS, William. Comunicaciones y redes de computadores. Prentice-Hall Inc, España, 1997.

[6]. Hackers. Secretos y soluciones para la seguridad en redes. McGraw Hill

[7]. Manual de seguridad en redes. Coordinación de Emergencia en Redes Teleinformáticas de la Administración Pública Argentina.