Instituto Tecnológico de Costa Rica

Área Académica de Ingeniería en Computadores

Programa de Licenciatura en Ingeniería en Computadores

Curso: CE-4301 Arquitectura de Computadores I

Especificación Proyecto Individual: Diseño e Implementación de un de un sistema de encriptación y desencriptación RSA empleando lenguaje ensamblador

Profesor:

Ronald García Fernández

Fecha de entrega: 08 de mayo, 2019

Semestre: I, 2019

Objetivo general

Mediante el desarrollo de este proyecto, el estudiante aplicará los conceptos de arquitectura de computadores en el diseño e implementación de una aplicación capaz de realizar encriptación y desencriptación RSA empleando un ISA específico.

Motivación

RSA (Rivest-Shamir-Adleman) es un sistema criptográfico de clave pública desarrollado en 1979 [1]. Es el primer algoritmo de este tipo y es válido tanto para encriptar como para firmar digitalmente.

De ahí la relevancia de entender en que consiste el algoritmo por lo que se le pide implementar una aplicación capaz de crear llaves, pública y privada capaz realizar la encriptación y desencriptación (ver figura 1) de un archivo de texto plano no muy extenso[1], la aplicación debe estar implementado en lenguaje ensamblador.

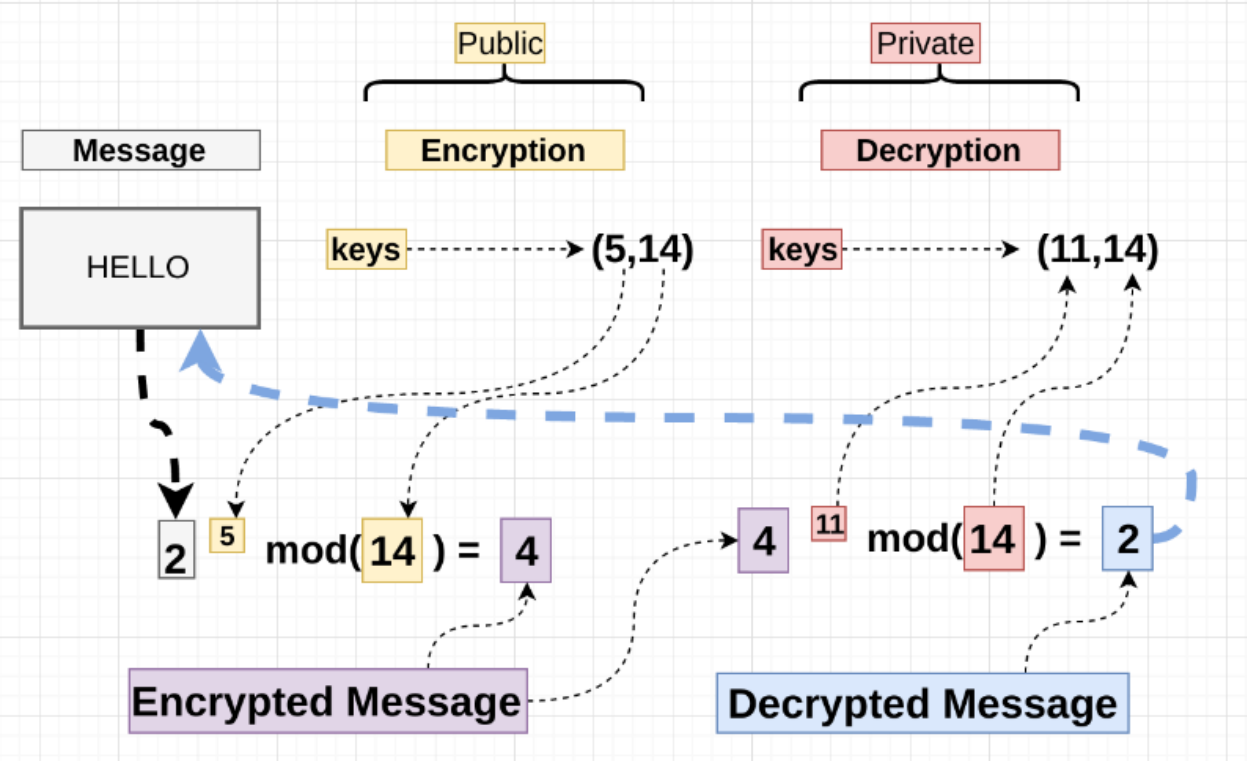

Figura 1. Diagrama básico del proceso de encriptación y desencriptación RSA [2].

[1] Parte de los objetivos del proyecto es determinar el tamaño adecuado del archivo y llaves de la aplicación

Requisitos generales de la aplicación

1- La aplicación debe permitir al usuario seleccionar el texto, y llaves que desea procesar.
2- La aplicación debe emplear el algoritmo RSA, no se aceptaran soluciones parciales u otros algoritmos.
3- La aplicación debe ser implementada **en su totalidad en lenguaje ensamblador** (asm).
4- La aplicación debe ser capaz de generar ambos procesos encriptación y desencriptación y permitir al usuario decidir qué operación desea realizar.

Entregables

Este proyecto está dividido en etapas cada una de ellas debe generar un entregable, los cuales no tienen valor de nota pero son necesarios para la evaluación del proyecto:

Fecha	Descripción Entregable
20-03-19	- Descripción del algoritmo RSA. - Modelo de referencia en el cual se implementa el algoritmo RSA en un leguaje de "alto" nivel. - Elección del ISA y plataforma de simulación/ejecución y justificación
05-04-19	- Justificación tamaños de llaves y archivos - Definición de forma de verificación de la aplicación - Avance de generación de llave
19-04-19	- Entrega de primer implementación de algoritmo junto con la descripción de las instrucciones de asm empleadas.
03-05-19	- Estrategia de evaluación de desempeño de los algoritmos (potencia, ciclos por instrucción, instrucciones empleadas, caché, etc)
08-05-19	- Entrega final de aplicación con códigos fuente, documentación relevante para el uso de la misma - Resumen de resultados sobre evaluación de desempeño

Evaluación

La evaluación del proyecto se da bajos los siguientes rubros:

- Presentación Funcional 100% (incluye documentación de uso, resultados, evaluación de desempeño)

Para que este proyecto sea evaluado deben entregarse todos los avances y la revisión será programada posteriormente a la fecha de entrega.

Referencias

[1] Rivest, Ronald & Shamir, Adi & M. Adleman, Leonard. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Commun. ACM. 21. 120-126. 10.1145/357980.358017.

[2] https://hackernoon.com/how-does-rsa-work-f44918df914b visitada el 28-02-2019.