Proyecto 2

RSA

Información del curso

Criptografía y Seguridad - Facultad de Ciencias, UNAM.

- Profesor: Criptografía y Seguridad
- Ayudante: Gerardo Rubén López Hernández
- Laboratorio: José Canek García Aguilar

Descripción de la práctica

Implementación el algoritmo de RSA para cifrar y descifrar un mensaje.

En el archivo de especificación de la prática viene todo explicado `doc.pdf`.

Entorno

- **`OS`**: Ubuntu 18.04.2 LTS o macOS Mojave 10.14.4
- **`Scala`**: Scala 2.12.8
- **`make`**: GNU Make 3.81

Instalación de Scala

Se puede instalar **Scala** de la página oficil o bien, usando **SDKMAN!** (el cual recomiendo porque facilita la instalación y ofrece varios beneficios). Si se opta por la segunda opción, a continuación se explicará como instalar **Scala** con **SDKMAN!**.

Instalación de SDKMAN!

```
$ curl -s "https://get.sdkman.io" | bash
```

Abre una nueva terminal y pon lo siguiente:

```
$ source "$HOME/.sdkman/bin/sdkman-init.sh"
```

Por último, para verificar que fue instalado satisfactoriamente, ejecutar el siguiente comando:

```
$ sdk version
```

Si la instalación fue satisfactoria se mostrará un mensaje como el siguiente:

sdkman 5.0.0+51

Si eres curioso puedes ver la página oficial y ver la parte de la instalación.

Instalación de Scala

Teclear lo siguiente:

```
$ sdk install scala 2.12.8
```

Verificar si la instalación fue exitosa:

```
$ scala -version
```

Si se instaló correctamente, deberá aparecer algo similar:

> Scala code runner version 2.12.8 – Copyright 2002-2018, LAMP/EPFL and Lightbend, Inc.

Ejecución del programa

Para facilitar la compilación, ejecución y limpieza del proyecto se optó por usar la herramienta llamada `make` con diferentes *targets*.

Para compillar es programa, se deberá tener situada una terminal en la raíz del proyecto y ejecutar:

```
$ make compile
```

Para la ejecución del programa:

```
$ make run
```

Para limpiar el proyecto se deberá ejectar el comando:

```
$ make clean
```

Comentarios

Los casos de prueba solo están yuxtapuestos en el código del `main`.

La ejecución del programa puede demorar como 5 segundos.

Se mostrará en la ejecución del programa todos los parámetros utilizados en el RSA.

Para la implementación del algoritmo se basó en lo visto en clase, código del laboratorio y la siguiente bibliografía.

- Alfred J. Menezes, Scott A. Vanstone, and Paul C. Van Oorschot. 1996. Handbook of Applied Cryptography (1st ed.). CRC Press, Inc., Boca Raton, FL, USA.

Integrante(s)

- Ángel Iván Gladín García - *angelgladin@ciencias.unam.mx*
- Nora Hilda Hernández Luna - *nora-hdz@ciencias.unam.mx*