MANUAL DE USARIO
SISTEMA DE CRIPTOGRAFIA

CODECOFE

Celular: +591 72483556
Skype: jlrodriguez.codecofe
www.codecofe.com
contact@codecofe.com

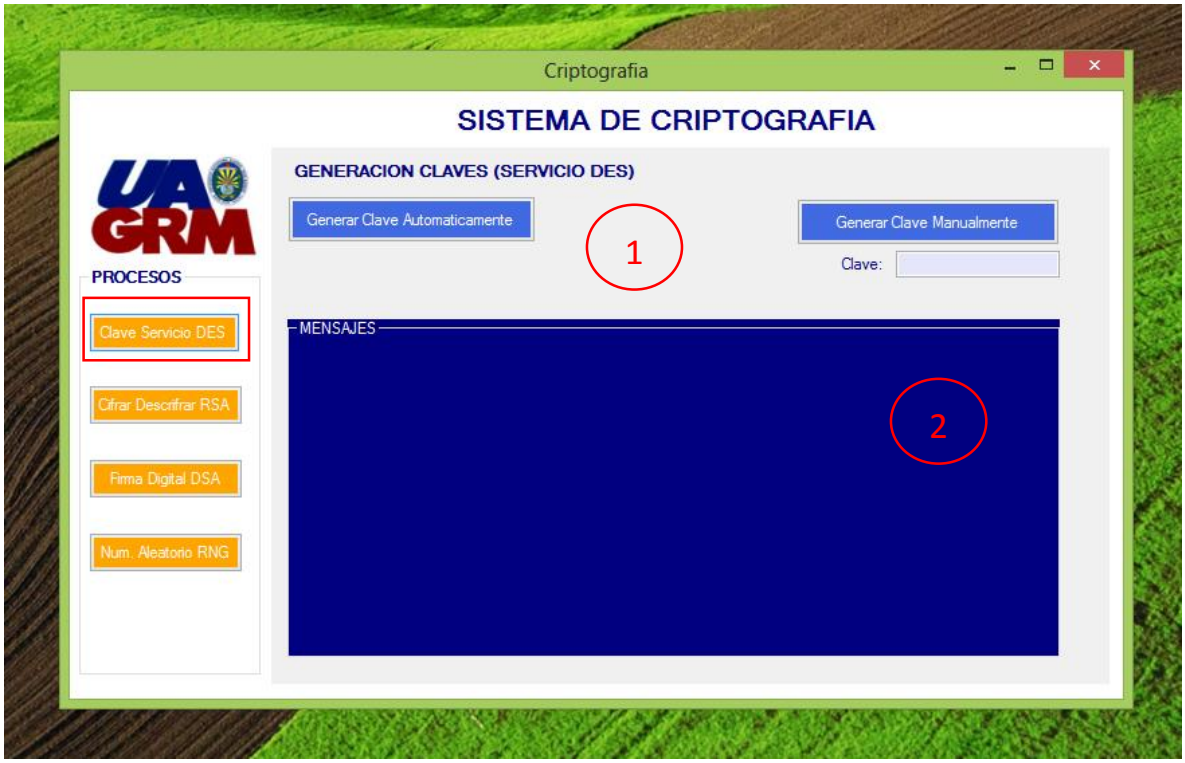
1. Pantalla Inicial

1) Área de procesos.- Son los botones que permiten realizar 4 tares:
   - Generación de Clave por Servicio Encriptación DES.
   - Generación de Calves y ficheros xml por Servicio Encriptación RSA.
   - Generación y Comprobación de firma digital por Servicio Encriptador DSA.
   - Generación de Números Aleatorios por Servicio Encriptador ENG.

Nota: Los servicios que se menciona son propios de framework de.NET `RSACryptoServiceProvider`, `DESCryptoServiceProvider`, `DSACryptoServiceProvider`, `RNGCryptoServiceProvider` que se utilizan para criptografía.

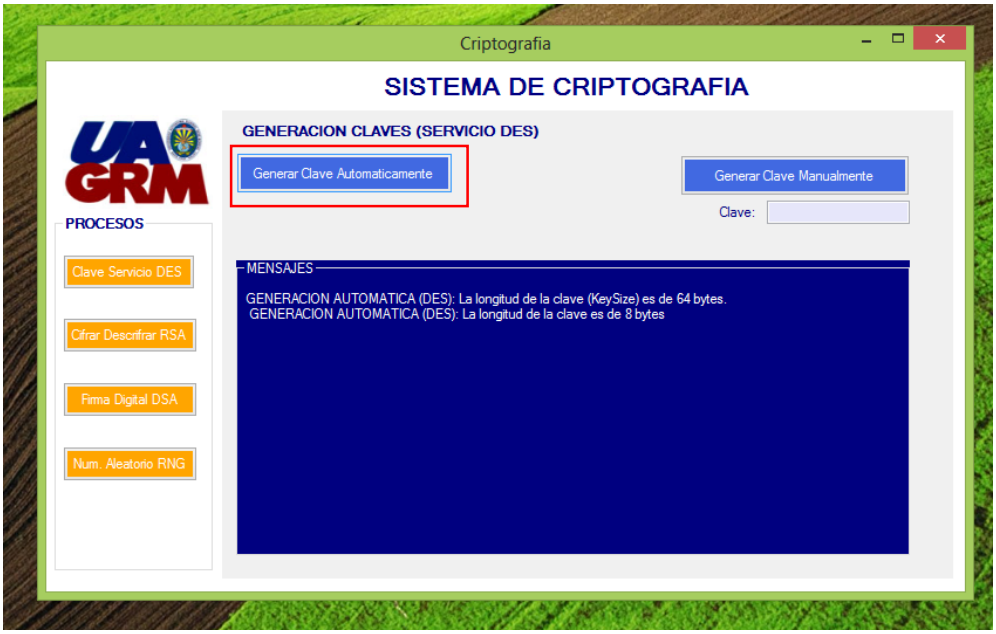
2) Área de Realización de Proceso.- Es la parte del sistema donde se realizara cada proceso seleccionado.

2. Proceso – Clave Servicio DES

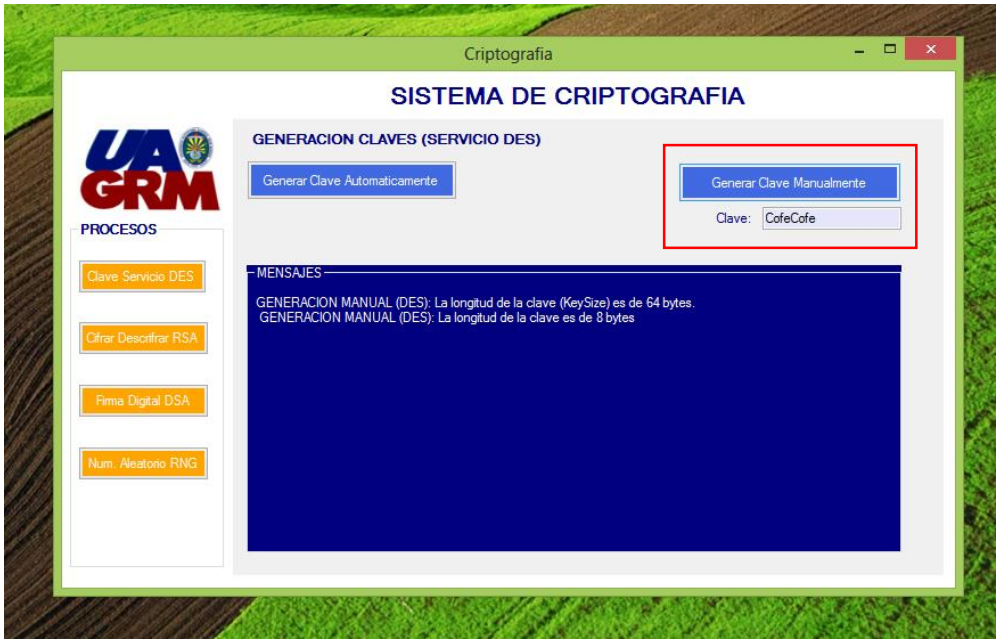


1) Área de Botonera.- Contiene los controles de entrada como ser caja de texto para la entrada de datos y botones para ejecutar el proceso, en algún proceso los botones de color azul con texto blanco se mostrara opaco es porque ese proceso requiere un proceso previo o mejor dicho está bloqueado.
2) Área de mensajería.- Es la parte del sistema que muestra los mensajes de cada proceso.

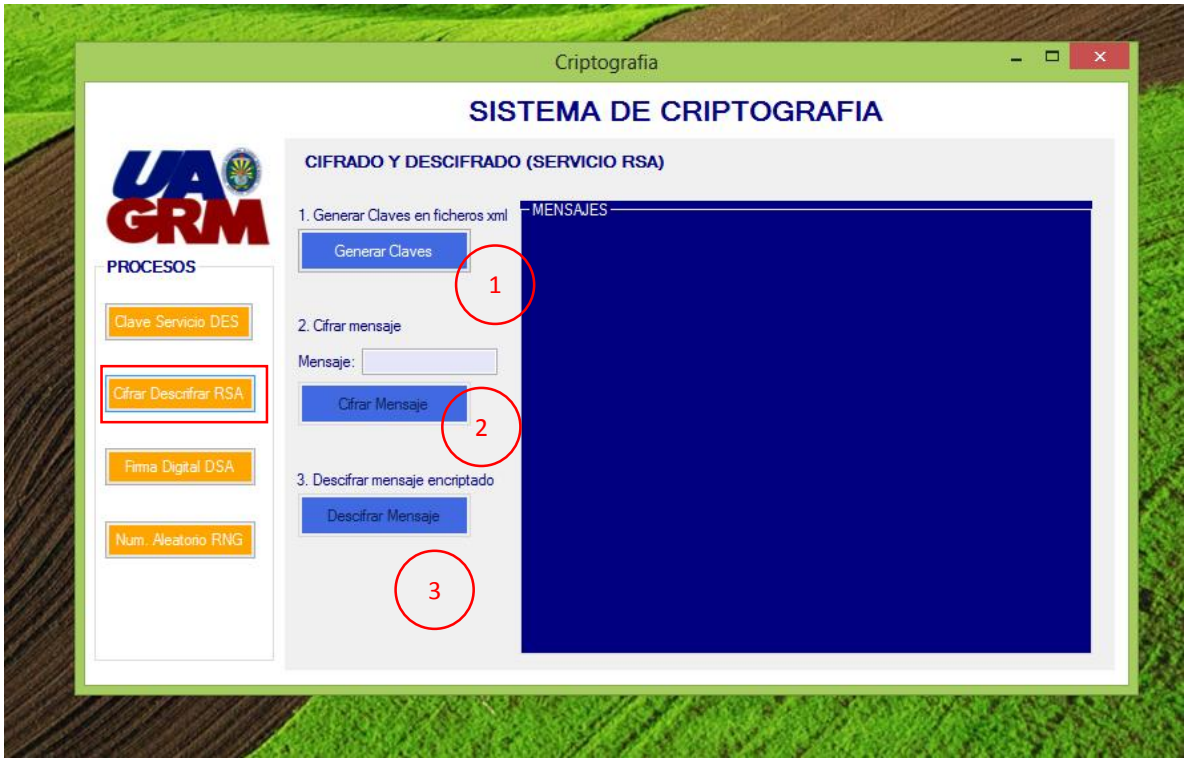
SubProceso Generacion Clave Automaricamente:



Subproceso Generación Clave Manualmente:



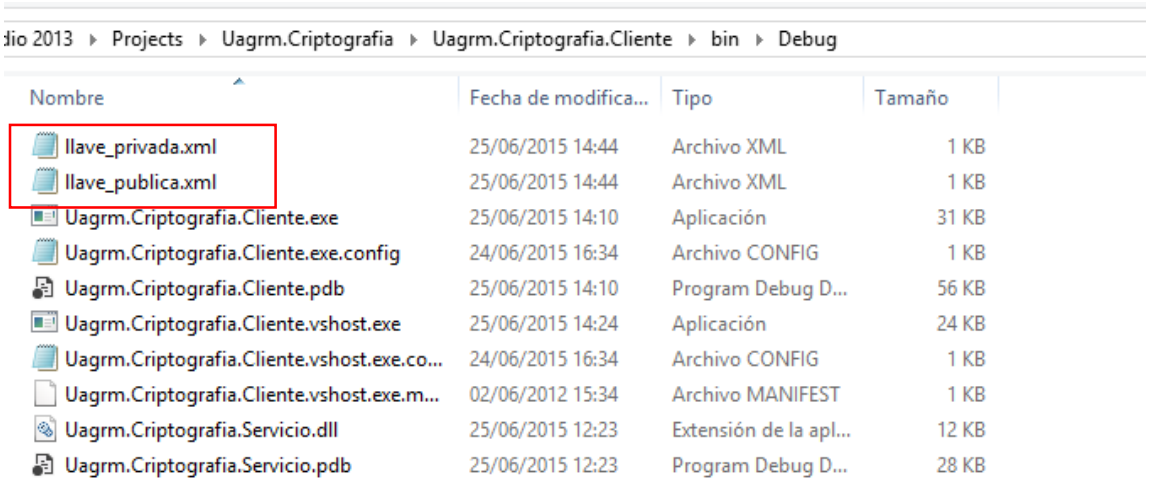
3. Proceso – Cifrar Descifrar RSA



1) Generar Claves.- Asigna parámetros de inicio de Servicio Criptográfico de RSA, crea ficheros de claves llave_privada.xml y llave_publica.xml y después escribe en los ficheros las claves.

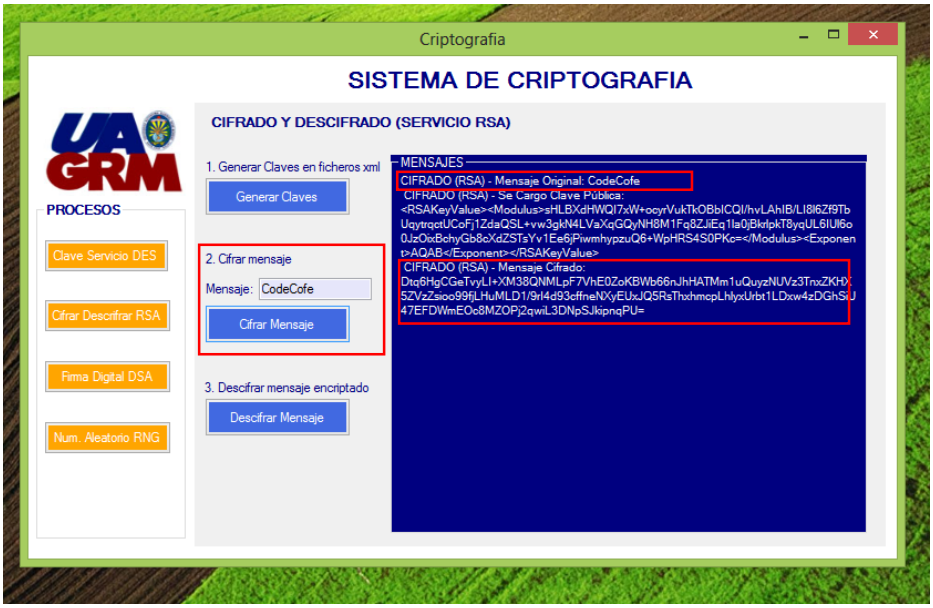
Para verificar la creación de estos ficheros puede dirigirse a la siguiente ruta:

…\Uagrm.Criptografia\Uagrm.Criptografia.Cliente\bin\Debug



Si abre los ficheros podrá observar las claves generadas.

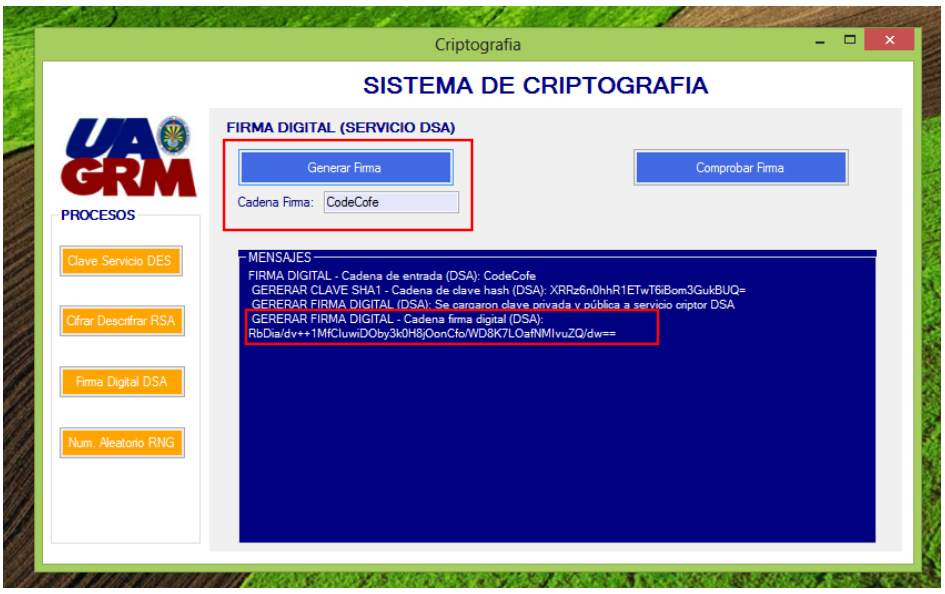
2) Cifrar Mensaje.- Es necesario introducir un dato en la caja de texto mensaje, de todas formas si no lo hace el sistema validara que es requerido. Presiona el botón correspondiente y se cifra el dato ingresado. Nota: Para este proceso solo es necesario cargar la clave pública desde el fichero al servicio de criptacion RSA.



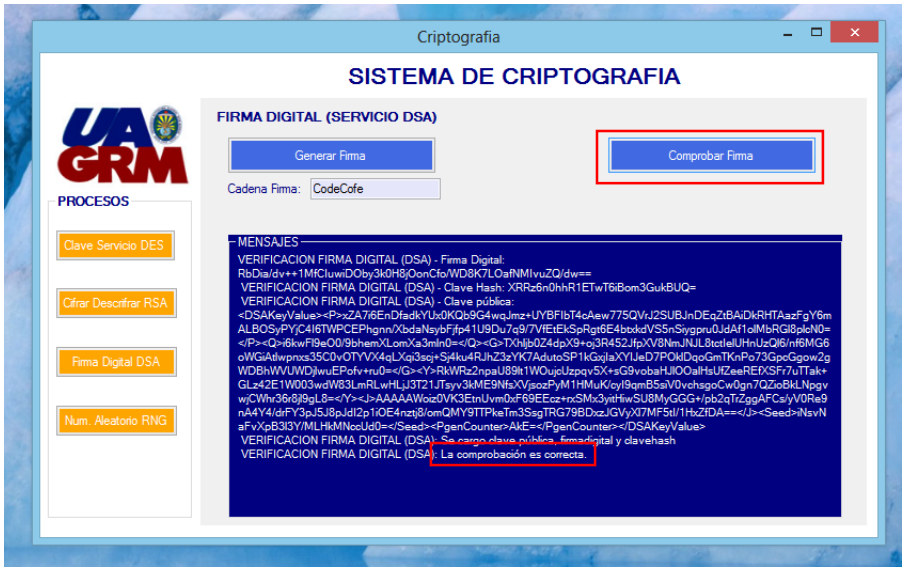
3) Descifrar mensaje encriptado.- Este proceso realiza una operación inversa obtiene el mensaje cifrado que se muestra en el 3 cuadro seleccionado de la anterior imagen, y lo convierte a mensaje original. Nota: Para este proceso se carga la clave privada desde el fichero al servicio de criptación de RSA.

4. Proceso – Firma Digital DSA

1) Generar Firma.- Es necesario ingresar un dato en la caja de texto cadena de firma este es la entrada para la firma digital, el panel nos muestra los subprocesos que se realizaron como es la generación de la clave HASH, carga de clave pública y privada y finalmente la cadena de firma digital.



2) Comprobar Firma.- Verifica si firma digital es correcta cargado la clave hash, clave pública y firma.



5. Proceso – Numero Aleatorio RNG

Este proceso genera n números aleatorios que permite realizar el servicio criptográfico RNG en base a un parámetro de entrada que indica la cantidad de números a generar.