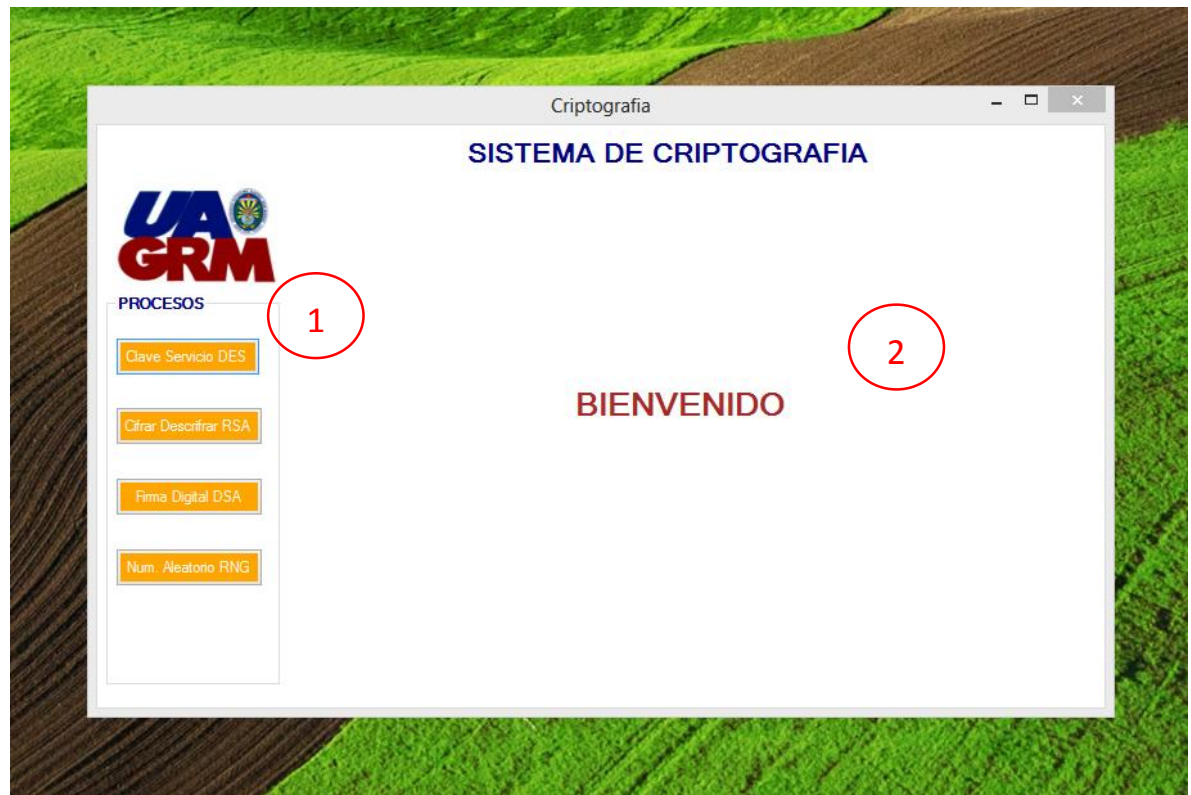


MANUAL DE USUARIO

SISTEMA DE CRIPTOGRAFIA

1. Pantalla Inicial



- 1) Área de procesos.- Son los botones que permiten realizar 4 tareas:
- 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.

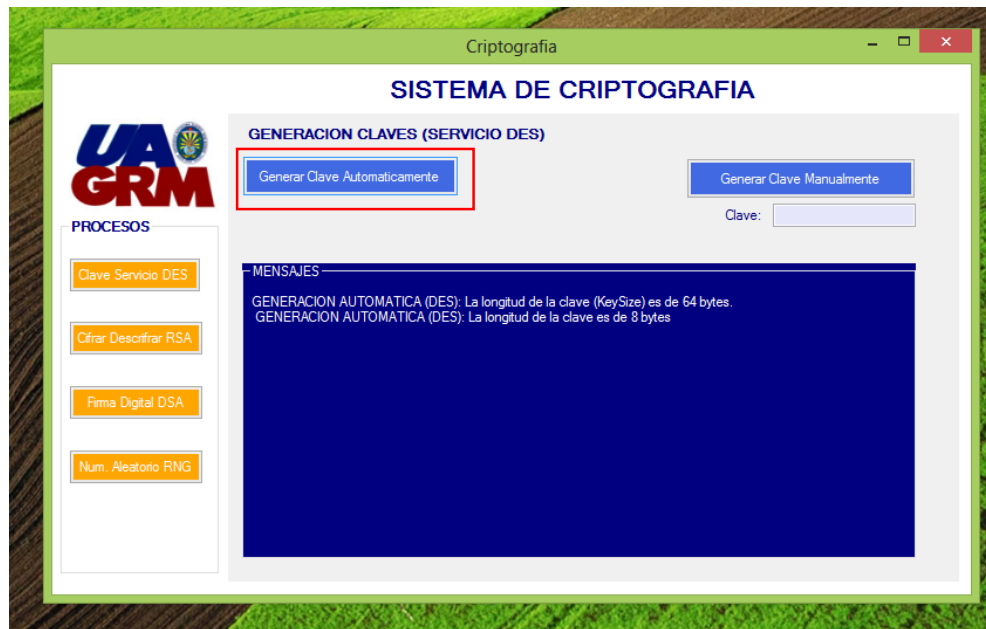
- 2) Área de Realización de Proceso.- Es la parte del sistema donde se realizara cada proceso seleccionado.

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 Automaticamente:



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.

```

MENSAJES
GENERAR CLAVE (RSA): Se genero el fichero "llave_privada.xml".
Clave Privada XML (RSA):
<RSAKeyValue><Modulus>shLBXdHWQI7xW+ocyrVukTkOBbICQI/hvLAhIB/LI8I6Zf9Tb
UqytrqetUCoFj1ZdaQSL+vw3gkN4LVaXqGQyNH8M1Fq8ZJiEq1la0jBkrlpkT8yqUL6IU6o
0JzOixBchyGb8cXdZSTsYv1Ee6jPiwmhypzuQ6+WpHRS4S0PKc=</Modulus><Exponen
t>AQAB</Exponent><P>6DYz93mRX5vJA1w+t/b6RuO7/7bQfvkr97s8xTESyKLi2GMue
5X1AOsn0LRjmRh8WhwZojYfZV49OLKOIWLQ==</P><Q>woYIDpoCd08OFKUj5g6NS
apADQ1qHvEfzTHywHEcb7sh2hoUFJUGAps3WrgbRc4K2tqydZe4gCj2oF9kU6FWow==<
/Q><DP>UqjgzMpQjmkH5r4IIHtS4jLpLZMV7aYyoe3bzxIN7q/U8IQz+rhBs6cB0FA2UtAy8
T1NLAKu9d1cZkfi1I/rQ==</DP><DQ>OyDtiLe1wjBslkfVpDbz6WJnK4UMN2YjhtX9tRNs
0mWuj45XxxNXGNz+wZ1e816rTXHA0mgEozhErSMWYN0Qw==</DQ><InverseQ>LuR
AD7BeAX3AD+EtD0E4IIU2bMzDI90TiomYCOQB1+KcgZ9wmsaMhp8QAmrgIfCcZ2THs
vcRSUJnnMiHjCzqjA==</InverseQ><D>il+EGxJLJlezGfTP3XxJGGQZBghiUoVELxgk8i9c
vFTtwv1nrlbu/fP8nv00XRJKsOfa6tpOob5NiallyG3CydRoNyCyEQSrk0zZ8SVMV86TJe/
GNAjSkXSR4VXc1Pv/L3bIRFzvQa/61K2S9DNIIQXBO/V0CCFH504ek4GEYk=</D></RS
AKeyValue>
Se escribio clave privada en "llave_privada.xml"
GENERAR CLAVE (RSA): Se genero el fichero "llave_publica.xml".
Clave Pública XML (RSA):
<RSAKeyValue><Modulus>shLBXdHWQI7xW+ocyrVukTkOBbICQI/hvLAhIB/LI8I6Zf9Tb
UqytrqetUCoFj1ZdaQSL+vw3gkN4LVaXqGQyNH8M1Fq8ZJiEq1la0jBkrlpkT8yqUL6IU6o
0JzOixBchyGb8cXdZSTsYv1Ee6jPiwmhypzuQ6+WpHRS4S0PKc=</Modulus><Exponen
t>AQAB</Exponent></RSAKeyValue>
Se escribio clave pública en "llave_publica.xml"

```

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

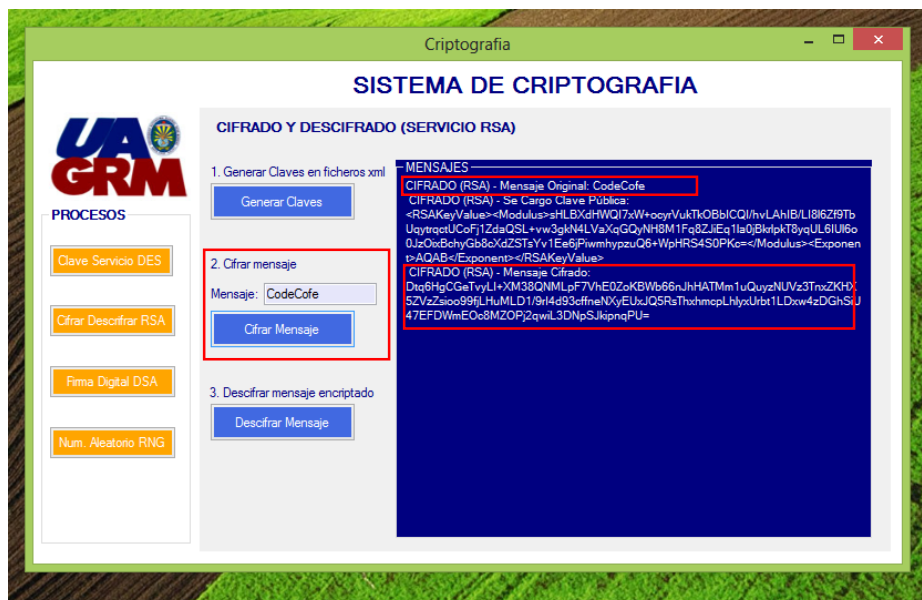
...\\Uagrm.Criptografia\\Uagrm.Criptografia.Cliente\\bin\\Debug

ño 2013 > Projects > Uagrm.Criptografia > Uagrm.Criptografia.Cliente > bin > Debug

Nombre	Fecha de modifica...	Tipo	Tamaño
llave_privada.xml	25/06/2015 14:44	Archivo XML	1 KB
llave_publica.xml	25/06/2015 14:44	Archivo XML	1 KB
Uagrm.Criptografia.Cliente.exe	25/06/2015 14:10	Aplicación	31 KB
Uagrm.Criptografia.Cliente.exe.config	24/06/2015 16:34	Archivo CONFIG	1 KB
Uagrm.Criptografia.Cliente.pdb	25/06/2015 14:10	Program Debug D...	56 KB
Uagrm.Criptografia.Cliente.vshost.exe	25/06/2015 14:24	Aplicación	24 KB
Uagrm.Criptografia.Cliente.vshost.exe.co...	24/06/2015 16:34	Archivo CONFIG	1 KB
Uagrm.Criptografia.Cliente.vshost.exe.m...	02/06/2012 15:34	Archivo MANIFEST	1 KB
Uagrm.Criptografia.Servicio.dll	25/06/2015 12:23	Extensión de la apl...	12 KB
Uagrm.Criptografia.Servicio.pdb	25/06/2015 12:23	Program Debug D...	28 KB

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.



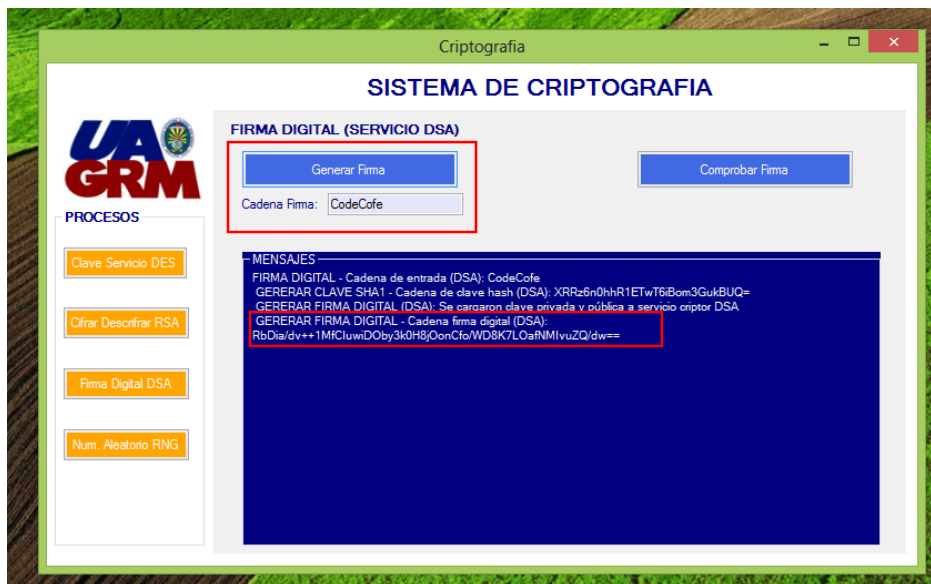
- 3) Descifrar mensaje encriptado.- Este proceso realiza una operación inversa obtiene el mensaje cifrado que se muestra en el 3 cuadro seleccionado de la anterior imagen, y lo convierte a mensaje original. Nota: Para este proceso se carga la clave privada desde el fichero al servicio de criptación de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



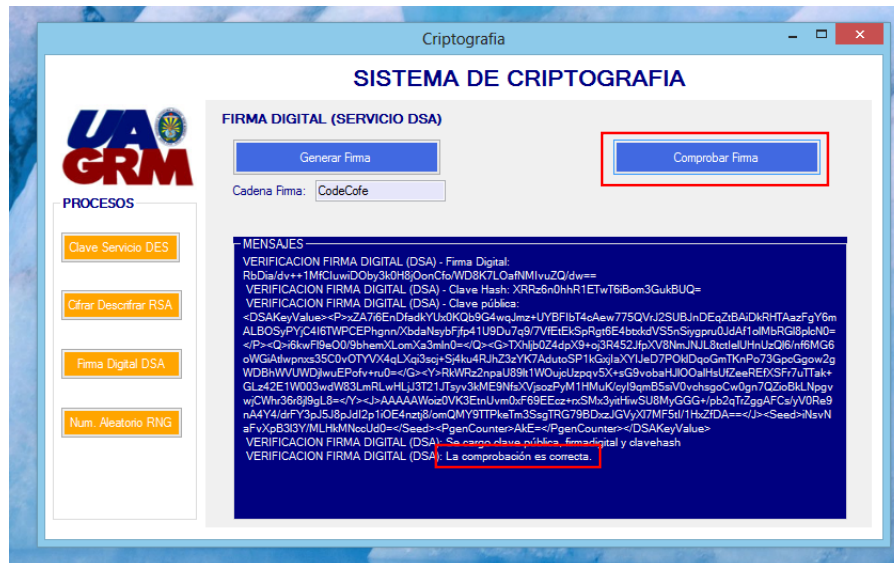
4. Proceso – Firma Digital DSA



- 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.

