

Manual de Usuario

Contenido:

1. Acceder a los algoritmos criptográficos	2
2. Algoritmos de clave simétrica	3
2.1. Generalidades	3
2.2. Cifrar	4
2.3. Descifrar	6
2.3.1. Descifrar un mensaje	6
2.3.2. Descifrar archivo binario	7
3. Algoritmos de clave asimétrica	9
3.1. Generalidades	9
3.2. Cifrar	10
3.3. Descifrar	12
3.3.1. Descifrar un mensaje	12
3.3.2. Descifrar archivo binario	13
4. Mensajes de Error	15

1. Acceder a los algoritmos criptográficos

Para utilizar los algoritmos criptográficos, puede acceder a ellos desde la pantalla de Inicio, haciendo click sobre la imagen del tipo de algoritmo correspondiente:



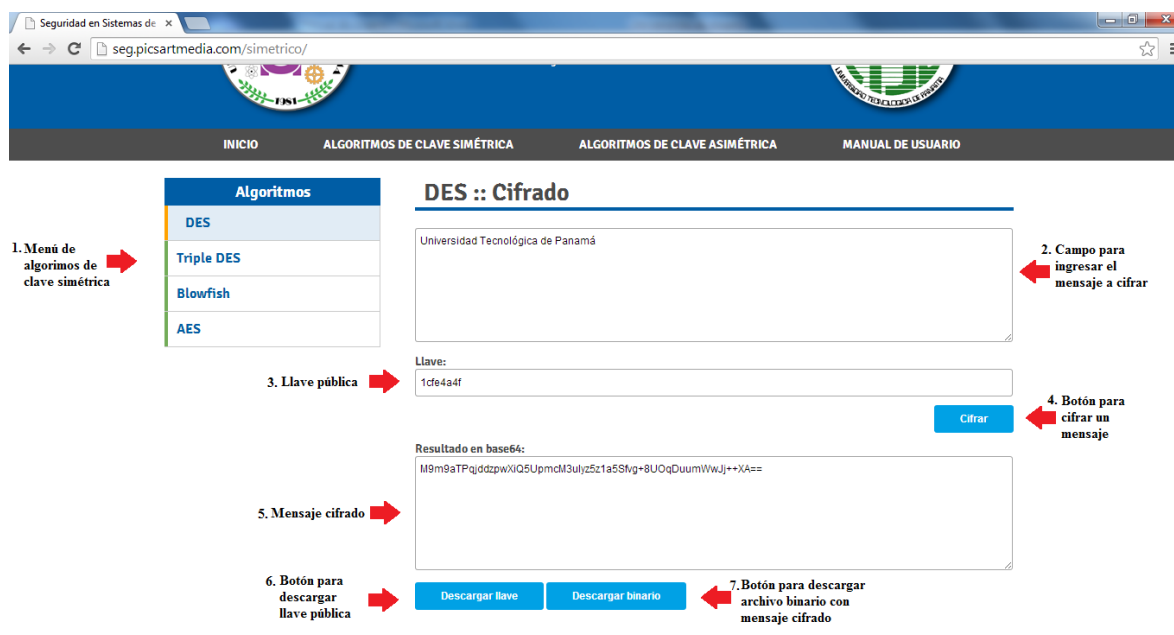
O a través del menú rápido:



2. Algoritmos de clave simétrica

2.1.Generalidades

A continuación se muestran los principales componentes de la pantalla de algoritmos de clave simétrica:



- 1- Menú de algoritmos de clave simétrica: desde este menú podrá visualizar y acceder a los distintos algoritmos de clave simétrica.
- 2- Campo para ingresar el mensaje a cifrar: en este campo deberá ingresar el mensaje que se requiera cifrar.
- 3- Llave pública: por defecto se muestra una llave pública, sin embargo esta puede ser modificada.
- 4- Botón “Cifrar”: al presionar este botón, se ejecuta el proceso que cifra el mensaje.
- 5- Mensaje cifrado: en este campo se muestra el mensaje cifrado.
- 6- Botón “Descargar llave”: con esta opción, puede descargar la llave pública para que el receptor del mensaje pueda descifrar el mismo.
- 7- Botón “Descargar binario”: permite descargar el archivo cifrado en binario.

2.2. Cifrar

Para cifrar un mensaje:

1. Escriba un mensaje en la caja de texto
2. Coloque una llave pública
3. Presione el botón “Cifrar”

The screenshot shows a web browser window with the URL `seg.picsartmedia.com/simetrico/`. The page has a blue header with the title 'Seguridad en Sistemas de Información Proyecto Semestral' and two logos: 'UNIVERSIDAD TECNOLÓGICA DE PANAMÁ' and 'INSTITUTO VENEZOLANO DE INVESTIGACIONES CIENTÍFICAS Y TECNOLÓGICAS'. Below the header is a navigation bar with links: 'INICIO', 'ALGORITMOS DE CLAVE SIMÉTRICA', 'ALGORITMOS DE CLAVE ASIMÉTRICA', and 'MANUAL DE USUARIO'. The main content area is titled 'Triple DES :: Cifrado'. On the left, there is a sidebar with a list of algorithms: 'DES', 'Triple DES' (highlighted), 'Blowfish', and 'AES'. The main area contains a large text input field with the placeholder text 'Universidad Tecnológica de Panamá'. Below this field is a label 'Llave:' followed by a text input field containing the value '1cfe4a4f5d52bb8717c3fd53'. At the bottom right of the main area is a blue button labeled 'Cifrar'. There are three numbered red circles (1, 2, 3) indicating the steps: 1. Enter the message, 2. Enter the key, 3. Click the 'Cifrar' button.

Nota: La llave pública por defecto es la que se muestra en la imagen, puede cambiarla cuando lo requiera.

El programa le indicará que la tarea se está ejecutando:

This screenshot shows the same web application as the previous one, but with a loading dialog box in the center. The dialog box is white with a black border and contains a circular loading spinner and the text 'Cargando. Por favor espere...'. The background of the web application is dimmed. The sidebar on the left still shows the list of algorithms, and the main area still shows the text input field and the 'Llave:' field with the same value. The 'Cifrar' button is still visible at the bottom right.

Se desplegará una caja de texto con el mensaje cifrado:

Seguridad en Sistemas de  Proyecto Semestral 

INICIO ALGORITMOS DE CLAVE SIMÉTRICA ALGORITMOS DE CLAVE ASIMÉTRICA MANUAL DE USUARIO

Algoritmos

- DES
- Triple DES**
- Blowfish
- AES

Triple DES :: Cifrado

Universidad Tecnológica de Panamá

Llave:
1cfe4a4f5d52bb8717c3fd53

Cifrar

Mensaje cifrado → Resultado en base64:
MVi0UJ66FXKcGOfqk1CTyhF93ScA3x2xd5MHV4DyWQlpvIM3AaA==

Descargar llave Descargar binario

Se le ofrece la opción de descargar el archivo cifrado al presionar el botón “Descargar binario” y descargar la llave pública al presionar el botón “Descargar llave”

Seguridad en Sistemas de  Proyecto Semestral 

INICIO ALGORITMOS DE CLAVE SIMÉTRICA ALGORITMOS DE CLAVE ASIMÉTRICA MANUAL DE USUARIO

Algoritmos

- DES
- Triple DES**
- Blowfish
- AES

Triple DES :: Cifrado

Universidad Tecnológica de Panamá

Llave:
1cfe4a4f5d52bb8717c3fd53

Cifrar

Resultado en base64:
MVi0UJ66FXKcGOfqk1CTyhF93ScA3x2xd5MHV4DyWQlpvIM3AaA==

Descargar llave pública → Descargar llave Descargar binario ← Descargar archivo en binario

De este modo, el mensaje sólo podrá ser leído por la persona que tenga la llave pública correcta para descifrar el archivo/texto cifrado.

2.3. Descifrar

2.3.1. Descifrar un mensaje

Para descifrar un mensaje debe:

1. Escoger la opción “Descifrar texto en base64”
2. Ingresar el texto cifrado
3. Colocar la llave pública
4. Presionar el botón de descifrar

The screenshot shows a web browser window with the URL `seg.picsartmedia.com/simetrico/`. The page has a blue header with the text "Seguridad en Sistemas de". Below the header, there is a section titled "Triple DES :: Descifrado". In this section, there are four numbered steps indicated by red circles: 1. A dropdown menu set to "Descifrar texto en base64". 2. A large text input field containing the base64-encoded string "MV00J96FXXG0f9qk1cThF938cA3x2d6MHV4DyW/Q/pVM3Aa==". 3. A key input field containing the string "1df4a4f5d52bb8717c3fd53". 4. A blue button labeled "Descifrar". Above the key input field, there is a "Llave:" label and the same key string. To the right of the key input field is a blue button labeled "Cifrar". At the bottom of the page, there is a blue footer with the text "Universidad Tecnológica de Panamá", "Profesor: Saulo Alzprá", and "Integrantes: ...".

El programa le indicará que la tarea se está procesando:

The screenshot shows the same web browser window as the previous one, but with a loading spinner overlay in the center. The spinner is a white circle with a black border and a black dot in the center. Below the spinner, the text "Cargando. Por favor espere..." is displayed. The background of the page is dark gray with a subtle grid pattern. The footer at the bottom of the page is also visible, showing the same text as in the previous screenshot.

El resultado se muestra como sigue:

The screenshot shows a web browser window with the URL `seg.picsartmedia.com/simetrico/`. At the top, there are two buttons: "Descargar llave" and "Descargar binario". Below these, the section is titled "Triple DES :: Descifrado". There is a dropdown menu labeled "Descifrar texto en base64". The main input field contains the base64 encoded string: `MVl0OJ66FXxcGOfqgk1cThhF83ScA3x2d6MHV4DvW/QlpVM3AaA==`. Below this is a field for the key, labeled "Llave:", containing the value `1cf4a4f5d52bb8717c3fd53`. A "Descifrar" button is to the right of the key field. The "Resultado:" field shows the decrypted text: "Universidad Tecnológica de Panamá". At the bottom, there is a file download bar showing "php-rsa.bin" and a link to "Mostrar todas las descargas..."

2.3.2. Descifrar archivo binario

Para descifrar un archivo binario debe:

1. Escoger la opción "Descifrar archivo binario"
2. Presionar el botón "Seleccionar archivo"
3. Colocar la llave pública
4. Presionar el botón de descifrar

This screenshot shows the same web interface as the previous one, but with annotations for the binary decryption process. On the left, a sidebar menu shows encryption options: DES, Triple DES (highlighted), Blowfish, and AES. The main section is titled "Triple DES :: Descifrado". It features a "Texto a cifrar" field. Below it is the "Llave:" field with the same key value. A "Cifrar" button is present. The "Triple DES :: Descifrado" section has a dropdown menu (1) set to "Descifrar archivo binario". Below this, the "Archivo binario a descifrar:" label is followed by a "Seleccionar archivo" button (2) and the filename "php-triple-des.bin". The "Llave:" field (3) contains the same key value. A "Descifrar" button (4) is at the bottom right of this section. The footer contains information about the Universidad Tecnológica de Panamá, the Faculty of Engineering and Computer Systems, the course "Licenciatura en Desarrollo de Software", the date "Julio, 2014", the professor "Saulo Alzprá", the group "Grupo: 1LS241", and the members: "Andrade, Óscar", "Estrada, Demetrio", and "Lau, Francisco".

El resultado se muestra como sigue:

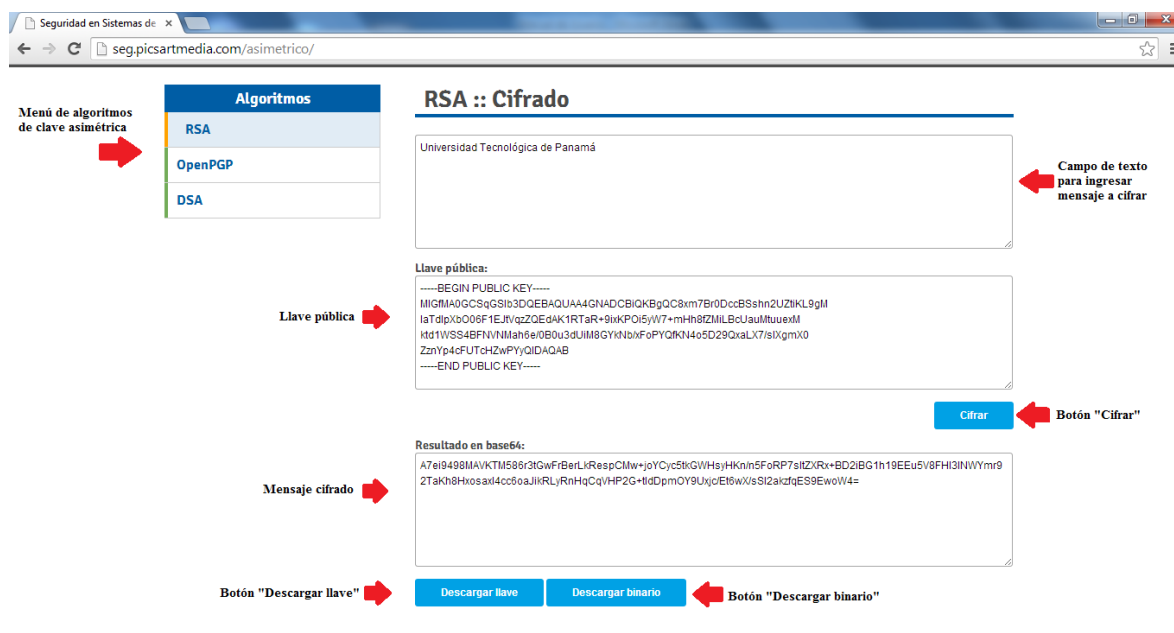
The screenshot shows a web browser window with the address bar displaying 'seg.picsartmedia.com/simetrico/'. The page has a light blue header and a white main content area. At the top, there is a 'Llave:' label followed by a text input field containing the hexadecimal string '1cfe4a4f5d52bb8717c3fd53'. To the right of this field is a blue button labeled 'Cifrar'. Below this, a section titled 'Triple DES :: Descifrado' is underlined. Under the title, there is a dropdown menu labeled 'Descifrar archivo binario' with a downward arrow. Below the dropdown is a label 'Archivo binario a descifrar:' followed by a file selection button labeled 'Seleccionar archivo' and the filename 'php-triple-des.bin'. Below this is another 'Llave:' label with a text input field containing the same hexadecimal string. To the right of this field is a blue button labeled 'Descifrar'. At the bottom, there is a 'Resultado:' label followed by a large text area containing the decrypted text 'Universidad Tecnológica de Panamá'.

Nota: La llave pública por defecto es la que se muestra en la imagen, puede cambiarla para descifrar mensajes que reciba de otras personas, utilizando el algoritmo correcto.

3. Algoritmos de clave asimétrica

3.1. Generalidades

A continuación se muestran los principales componentes de la pantalla de algoritmos de clave simétrica:

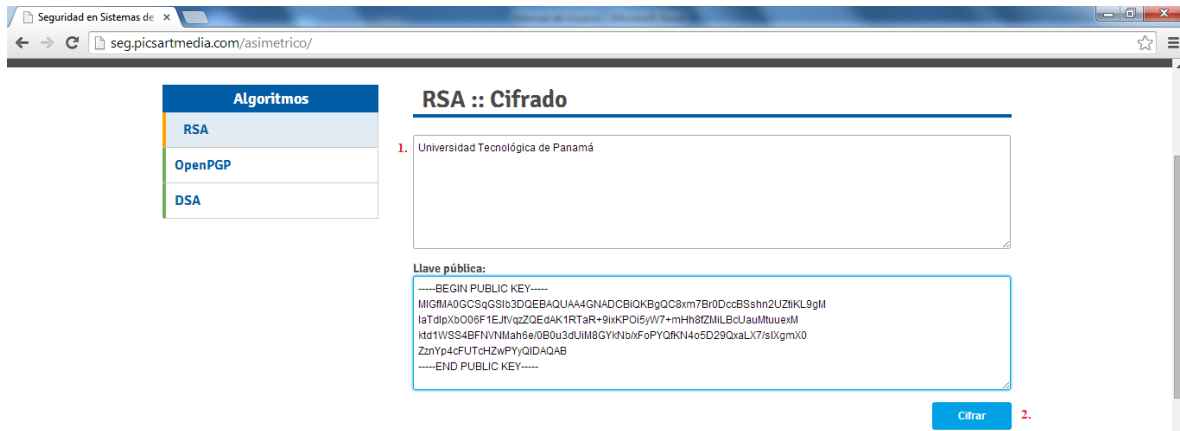


- 1- Menú de algoritmos de clave asimétrica: desde este menú podrá visualizar y acceder a los distintos algoritmos de clave asimétrica.
- 2- Campo de texto para ingresar el mensaje a cifrar: en este campo deberá ingresar el mensaje que se requiera cifrar.
- 3- Llave pública: la llave pública de los algoritmos asimétricos no se puede modificar, ya que la llave privada y pública forman un juego de llaves para cifrar y descifrar los mensajes.
- 4- Botón “Cifrar”: al presionar este botón, se ejecuta el proceso que cifra el mensaje.
- 5- Mensaje cifrado: en este campo se muestra el mensaje cifrado.
- 6- Botón “Descargar llave”: con esta opción, puede descargar la llave pública.
- 7- Botón “Descargar binario”: permite descargar el archivo cifrado en binario.

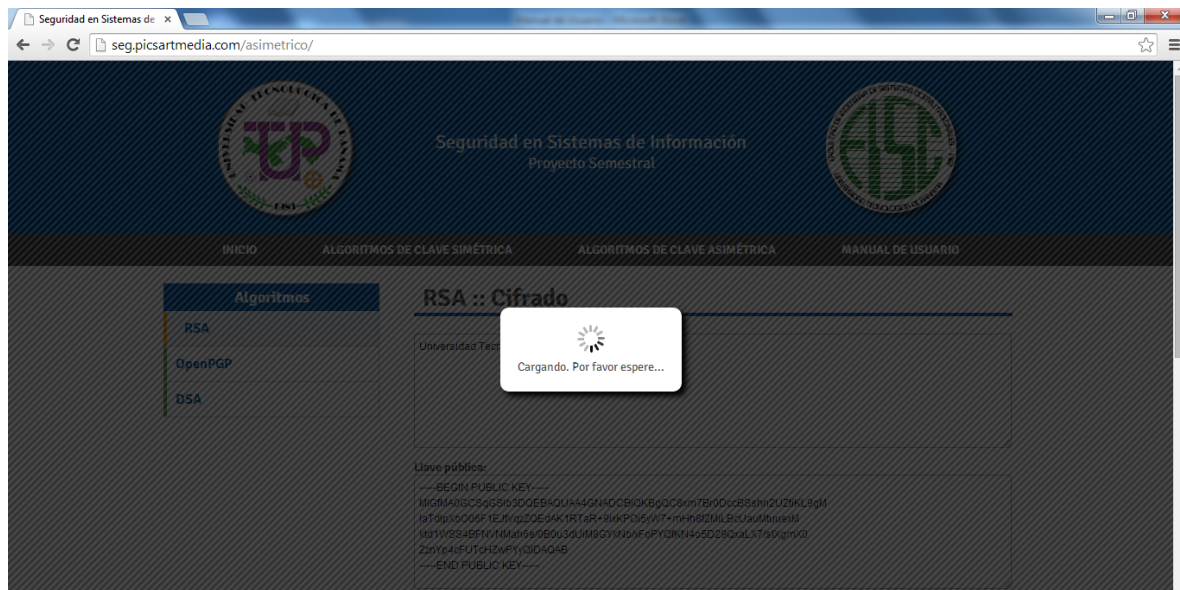
3.2. Cifrar

Para cifrar un mensaje:

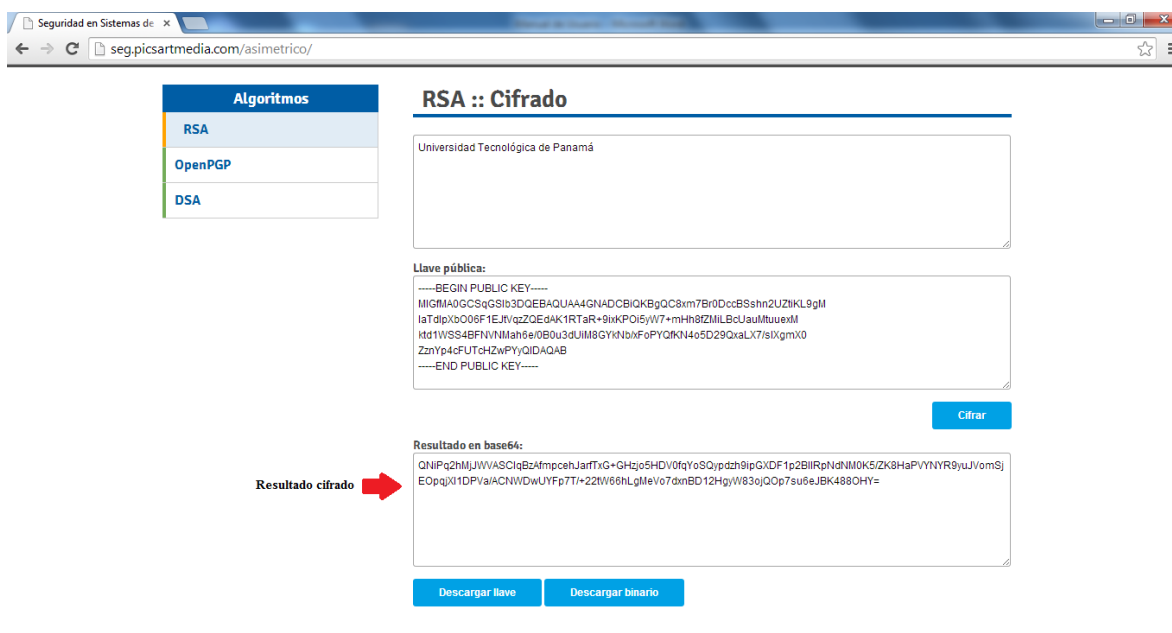
1. Escriba un mensaje en la caja de texto
2. Presione el botón “Cifrar”



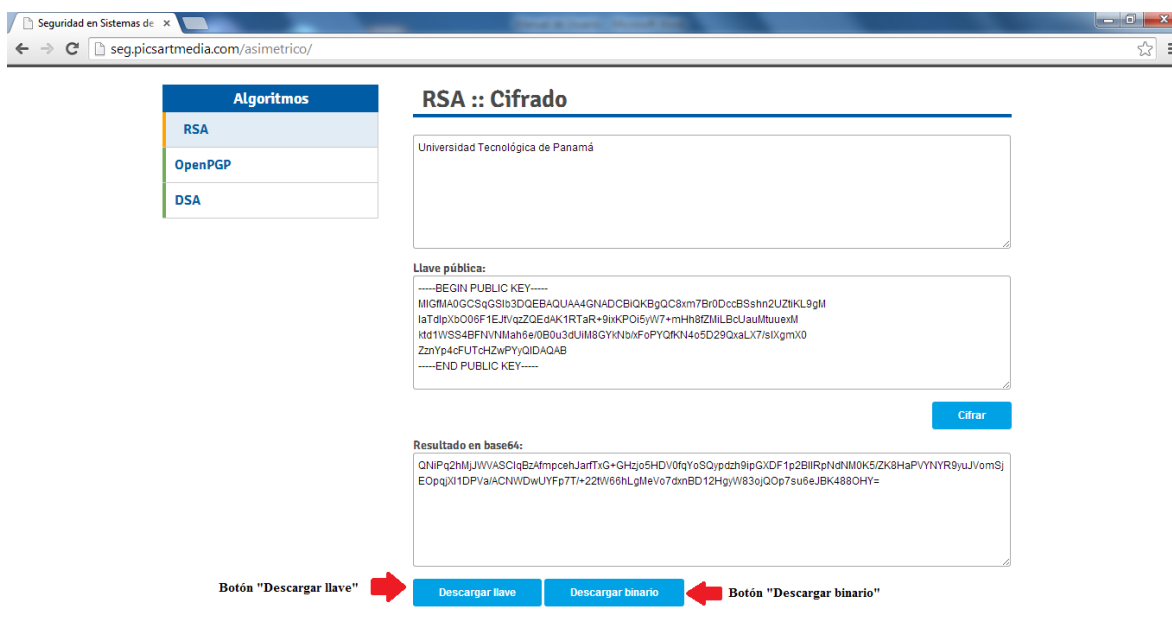
El programa le indicará que la tarea se está ejecutando:



Se desplegará una caja de texto con el mensaje cifrado:



Se le ofrece la opción de descargar el archivo cifrado al presionar el botón “Descargar binario” y descargar la llave pública al presionar el botón “Descargar llave”



3.3. Descifrar

3.3.1. Descifrar un mensaje

Para descifrar un mensaje debe:

- 1- Escoger la opción “Descifrar texto en base64”
- 2- Ingresar el texto cifrado
- 3- Presionar el botón de descifrar

The screenshot shows a web browser window with the URL `seg.picsartmedia.com/asimetrico/`. The page has a header with two buttons: "Descargar llave" and "Descargar binario". The main section is titled "RSA :: Descifrado". It contains a dropdown menu labeled "1" with the option "Descifrar texto en base64". Below this is a text input field labeled "2" containing the text "Universidad Tecnológica de Panamá". Underneath the input field is a section for the public key, titled "Llave pública:", which contains a block of text starting with "-----BEGIN PUBLIC KEY-----" and ending with "-----END PUBLIC KEY-----". At the bottom right of the form is a button labeled "3" with the text "Descifrar".

El programa le indicará que la tarea se está procesando:

This screenshot shows the same web application interface as the previous one, but with a loading state. A modal dialog box is centered on the screen, displaying a loading spinner and the text "Cargando. Por favor espere...". The background of the page is dimmed. The "Descifrar" button is still visible at the bottom right.

El resultado se muestra como sigue:

The screenshot shows a web browser window with the URL `seg.picsartmedia.com/asimetrico/`. The page title is "RSA :: Descifrado". There is a dropdown menu labeled "Descifrar texto en base64". Below it is a text input field containing a long base64 string. Underneath is a section for the public key, labeled "Llave pública:", containing a PEM-formatted key. A blue button labeled "Descifrar" is positioned to the right of the key. Below the key is a section labeled "Resultado:" with a text output field displaying "Universidad Tecnológica de Panamá".

3.3.2. Descifrar archivo binario

Para descifrar un archivo binario debe:

- 1- Escoger la opción "Descifrar archivo binario"
- 2- Presionar el botón "Seleccionar archivo"
- 3- Presionar el botón de descifrar

The screenshot shows the same web application but with the "Descifrar archivo binario" option selected in the dropdown menu. A file named "php-rsa.bin" is selected, indicated by a red circle with the number 2. The public key section remains the same. A blue button labeled "Cifrar" is now visible above the key section. The "Resultado:" section is empty. At the bottom of the page, there is a footer with contact information for the Universidad Tecnológica de Panamá, including the faculty, group name "Grupo: 1LS241", and a list of members: Andrade, Óscar; Estrada, Demetrio; and Lau, Francisco. A download button labeled "Mostrar todas las descargas..." is also present.

El resultado se muestra como sigue:

The screenshot shows a web browser window with the address bar displaying "seg.picsartmedia.com/asimetrico/". The page title is "Seguridad en Sistemas de". The main heading is "RSA :: Descifrado". Below the heading, there is a dropdown menu labeled "Descifrar archivo binario" with a downward arrow. Underneath, it says "Archivo binario a descifrar:" followed by a button labeled "Seleccionar archivo" and the text "php-rsa.bin". A section titled "Llave pública:" contains a text area with a public key: "-----BEGIN PUBLIC KEY-----\nMIGfMA0GCQsQSlb3DQEBQUAA4GNADCBQgQC8xm7Br0DccBSshn2UZtkL9gM\nlaTdlpXb006F1EJvqZQEdAK1RTaR+9ixKPOi5W7+mHh8ZMILBcUauMtuexM\nltd1WSS4BFNVNMah6e/0B0u3dUIM8GYKnbxF0PYQKN4o5D29QxaLK7/sIXgmX0\nZznYp4cFUTCH2wPYyQIDAQAB\n-----END PUBLIC KEY-----". To the right of this text area is a blue button labeled "Descifrar". Below this, a section titled "Resultado:" contains a text area displaying the decrypted result: "Universidad Tecnológica de Panamá". At the bottom of the browser window, a download bar shows a file named "php-rsa.bin" with a download icon and a button labeled "Mostrar todas las descargas...".

4. Mensajes de Error

4.1. Al presionar el botón “Cifrar” sin ingresar un mensaje:

Seguridad en Sistemas de Información
Proyecto Semestral

INICIO ALGORITMOS DE CLAVE SIMÉTRICA ALGORITMOS DE CLAVE ASIMÉTRICA MANUAL DE USUARIO

Algoritmos

- DES
- Triple DES
- Blowfish **Debes ingresar el texto a cifrar**
- AES

DES :: Cifrado

Texto a cifrar

Llave: 1cf4a4f

Cifrar

DES :: Descifrado

Descifrar texto en base64

4.2. Al ingresar una llave pública con una longitud inferior a la requerida en los algoritmos simétricos:

Seguridad en Sistemas de Información
Proyecto Semestral

INICIO ALGORITMOS DE CLAVE SIMÉTRICA ALGORITMOS DE CLAVE ASIMÉTRICA MANUAL DE USUARIO

Algoritmos

- DES
- Triple DES
- Blowfish
- AES

DES :: Cifrado

Universidad Tecnológica de Panamá

Llave: 1cf4a4f

La llave debe tener un mínimo de 8 caracteres.

Cifrar

DES :: Descifrado

Descifrar texto en base64

4.3. Al no ingresar una llave pública en los algoritmos simétricos:

The screenshot shows a web browser at the URL `seg.picsartmedia.com/simetrico/`. The page has a blue header with navigation links: INICIO, ALGORITMOS DE CLAVE SIMÉTRICA, ALGORITMOS DE CLAVE ASIMÉTRICA, and MANUAL DE USUARIO. On the left, a sidebar titled 'Algoritmos' lists DES, Triple DES, Blowfish, and AES. The main content area is titled 'DES :: Cifrado'. It features a large text input field containing 'Universidad Tecnológica de Panamá'. Below it is a 'Llave:' label and an empty text input field. To the right of this field is a red error message: 'Debes ingresar una llave'. A blue 'Cifrar' button is positioned below the key input field. Further down, the section 'DES :: Descifrado' is visible, showing a dropdown menu set to 'Descifrar texto en base64' and an empty text area labeled 'Texto en base64 a descifrar'.

4.4. Al presionar el botón “Descifrar” sin ingresar un mensaje:

This screenshot shows the 'Blowfish :: Descifrado' section of the application. The 'AES' algorithm is selected in the sidebar. The 'Llave:' input field is populated with the hexadecimal string '1cfe4a4f5d52bb8717c3fd5332ab368b8c56debc00c3f6ce30463843'. A blue 'Cifrar' button is located below the key field. In the 'Blowfish :: Descifrado' section, the dropdown menu is set to 'Descifrar texto en base64'. The text area for 'Texto en base64 a descifrar' is empty. A red error message, 'Debes ingresar el texto a cifrar', points to this empty text area. Below the text area is another 'Llave:' input field with the same hexadecimal key, and a blue 'Descifrar' button. The footer of the page contains contact information for the Universidad Tecnológica de Panamá, the professor Saulo Alzpría, and the group members: Andrade, Óscar; Estrada, Demetrio; Lau, Francisco; and Zamorano, Corina.

4.5. Al intentar ejecutar una solicitud incorrecta por las posibles razones:

- El archivo binario no corresponde al algoritmo seleccionado.
- La llave proporcionada no es la indicada para el mensaje cifrado.
- El tamaño de la llave en bits no corresponde al mensaje cifrado.

