Cifrado y hash

Introducción

El módulo **Cifrado y Hashing le** proporciona las instrucciones y dispositivos para desarrollar sus habilidades prácticas en los siguientes temas.

- Fundamentos criptográficos
- Comparación de algoritmos hash
- Comparación de valores hash

Tiempo de laboratorio: tomará aproximadamente 1 hora completar este laboratorio.

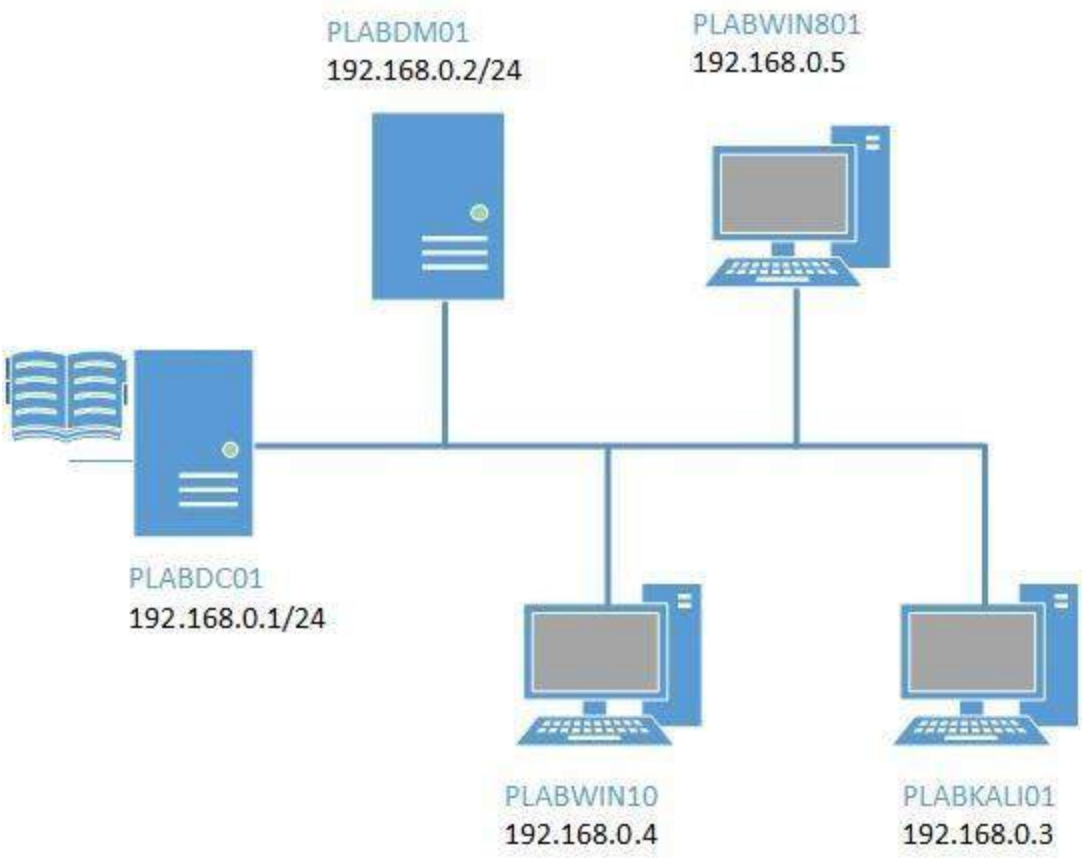
Objetivos del examen

Los siguientes objetivos del examen están cubiertos en este laboratorio:

- Determinar controles de seguridad de datos (por ejemplo, datos en reposo, datos en tránsito)

Diagrama de laboratorio

Durante su sesión, tendrá acceso a la siguiente configuración de laboratorio. Dependiendo de los ejercicios, puede o no usar todos los dispositivos, pero se muestran aquí en el diseño para obtener una comprensión general de la topología del laboratorio.



Conectando a tu laboratorio

En este módulo, trabajará en el siguiente equipo para llevar a cabo los pasos definidos en cada ejercicio.

- **PLABDC01** (Windows Server 2012 R2 - Controlador de dominio)
- **PLABWIN10** (Windows 10 - Miembro de dominio)

Para comenzar, simplemente elija un dispositivo y haga clic en **Encender**. En algunos casos, los dispositivos pueden encenderse automáticamente.

Ejercicio 1 - Fundamentos criptográficos

La criptografía es el proceso de intentar mantener la integridad y la confidencialidad de la información, el uso de herramientas criptográficas ayuda a simplificar el proceso de generar y confirmar la integridad de la información, al tiempo que ayuda a proporcionar confidencialmente para proteger de la visualización no autorizada de materiales.

Esto ayuda enormemente con la seguridad de la información que está recibiendo de la ubicación de origen. Además con el hash, puede confirmar, por ejemplo, que un programa que ha descargado no se ha modificado de alguna manera al verificar su valor hash producido por el autor con su propio valor.

En este ejercicio, aprenderá a usar una herramienta llamada CryptoDemo y conceptos sobre Hashing trabajando en estas tareas:

- Instalación de CryptoDemo
- CryptoDemo Encryption
- Descifrado de CryptoDemo
- Valores clave
- Hashing

Para obtener más información sobre criptografía, consulte el material de su curso o utilice su motor de búsqueda favorito para investigar este tema con más detalle.

Tarea 1 - Instalación de CryptoDemo

Aquí instalaremos la herramienta y nos prepararemos para usarla para obtener más información sobre los conceptos básicos criptográficos.

Paso 1

Asegúrese de haber alimentado los dispositivos necesarios indicados en la introducción.

Conéctese a **PLABWIN10** .

Se muestra el escritorio.

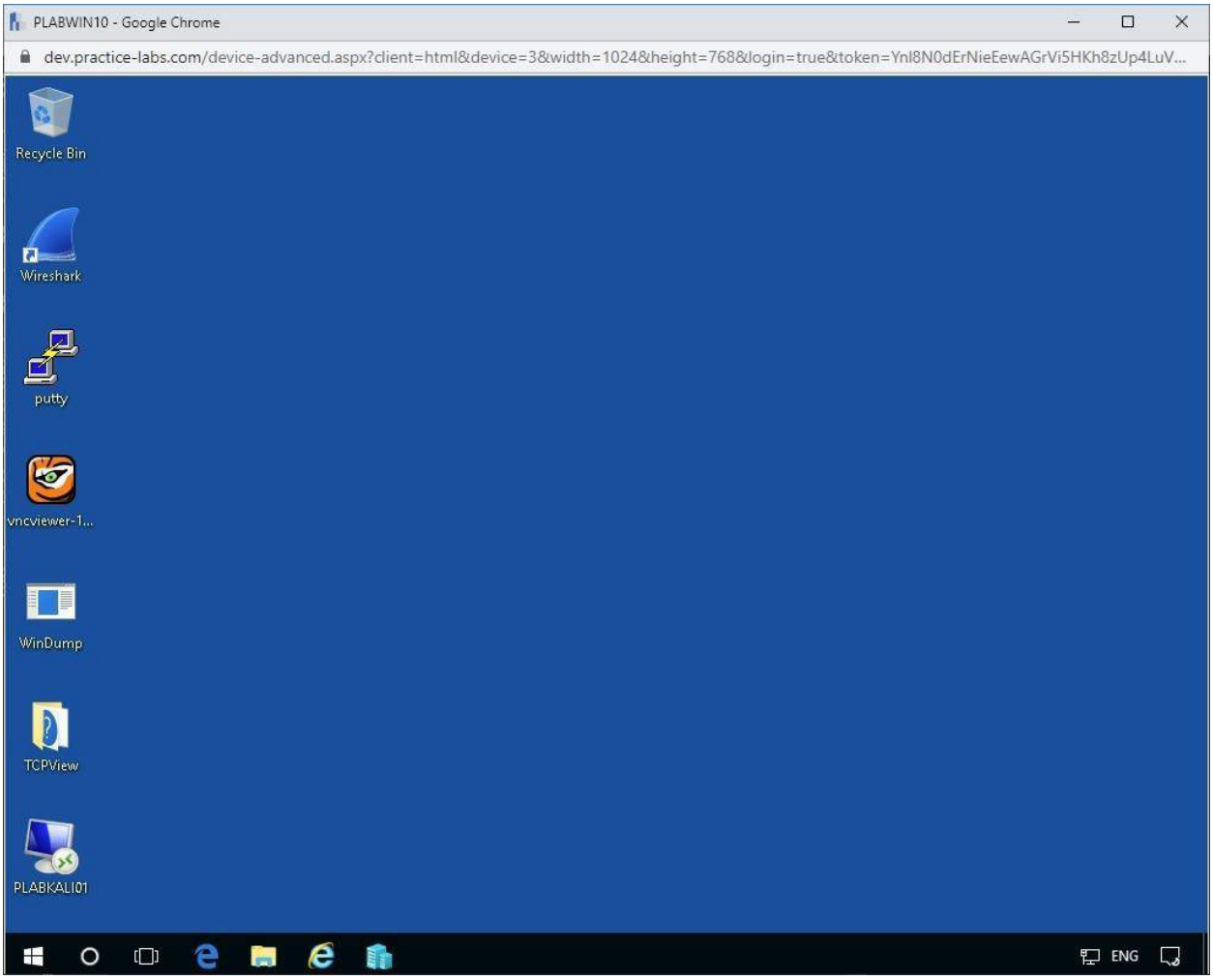


Figura 1.1. Captura de pantalla de PLABWIN10: Escritorio

Paso 2

Abra **Internet Explorer** ; la página de inicio predeterminada es la Intranet de Practice Labs.

Vaya a **Herramientas** , luego a la carpeta **Herramientas de piratería** .

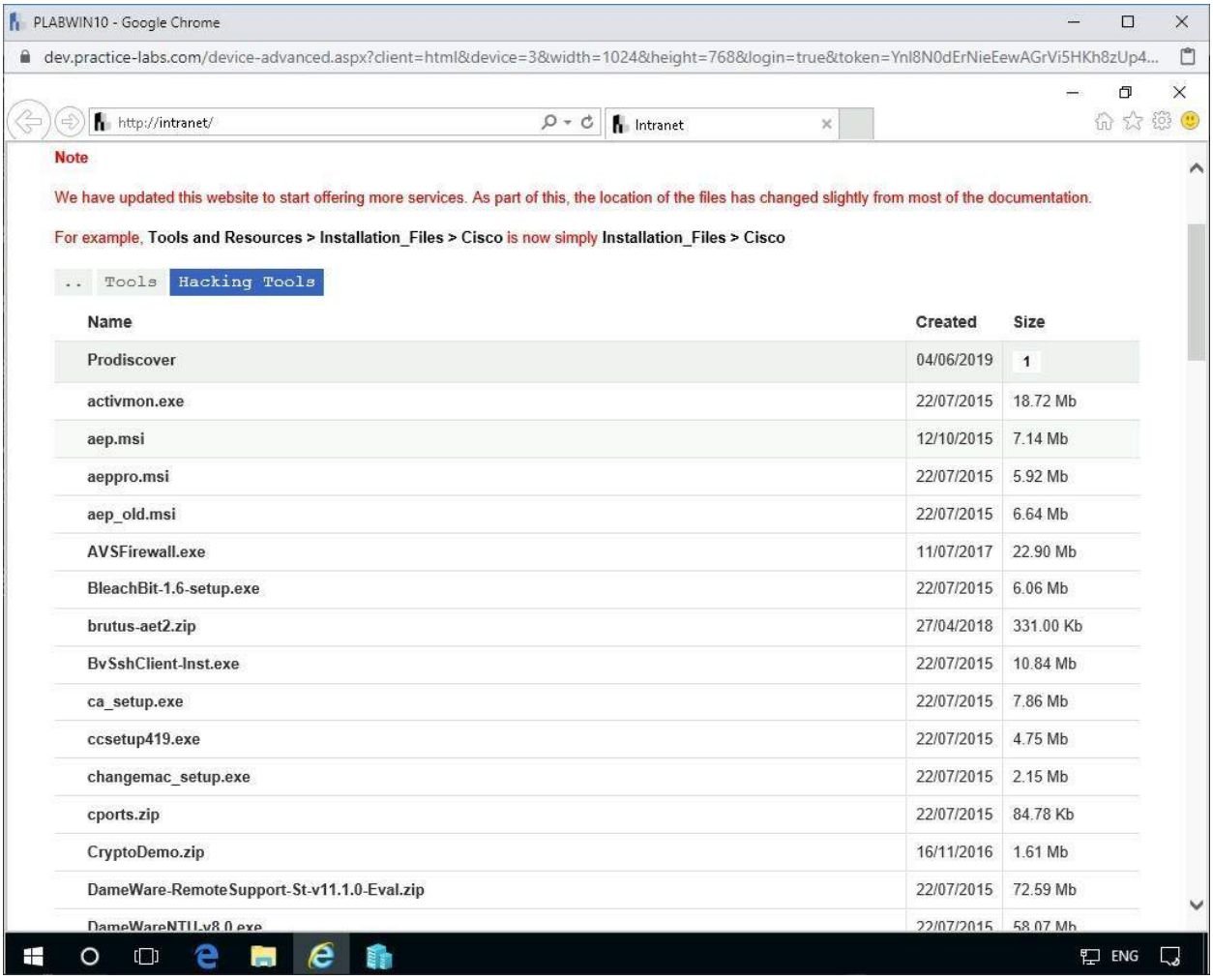


Figura 1.2. Captura de pantalla de PLABWIN10: Hacking Folder

Al comienzo de la página Herramientas de piratería, encontrará el programa comprimido.

Guarde **CrytoDemo.zip** en la carpeta Descargas

Paso 3

Navega a la carpeta **Descargas** .

Haga clic derecho en el documento comprimido
y **presione** la función **Extraer todo** .

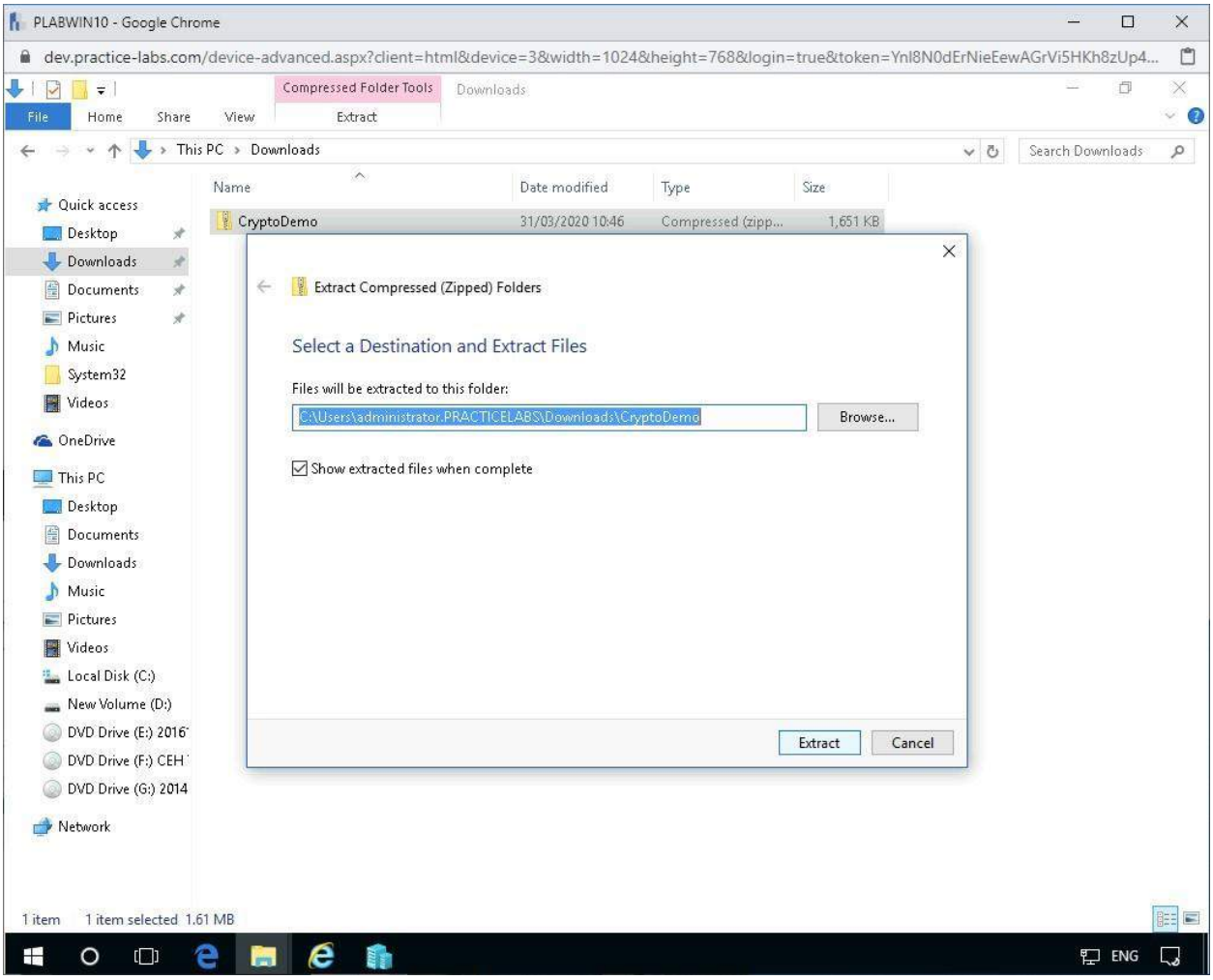


Figura 1.3. Captura de pantalla de PLABWIN10: Extracción del programa comprimido a la carpeta Descargas

Paso 4

Haga doble clic en la carpeta extraída y vea el contenido como se muestra a continuación.

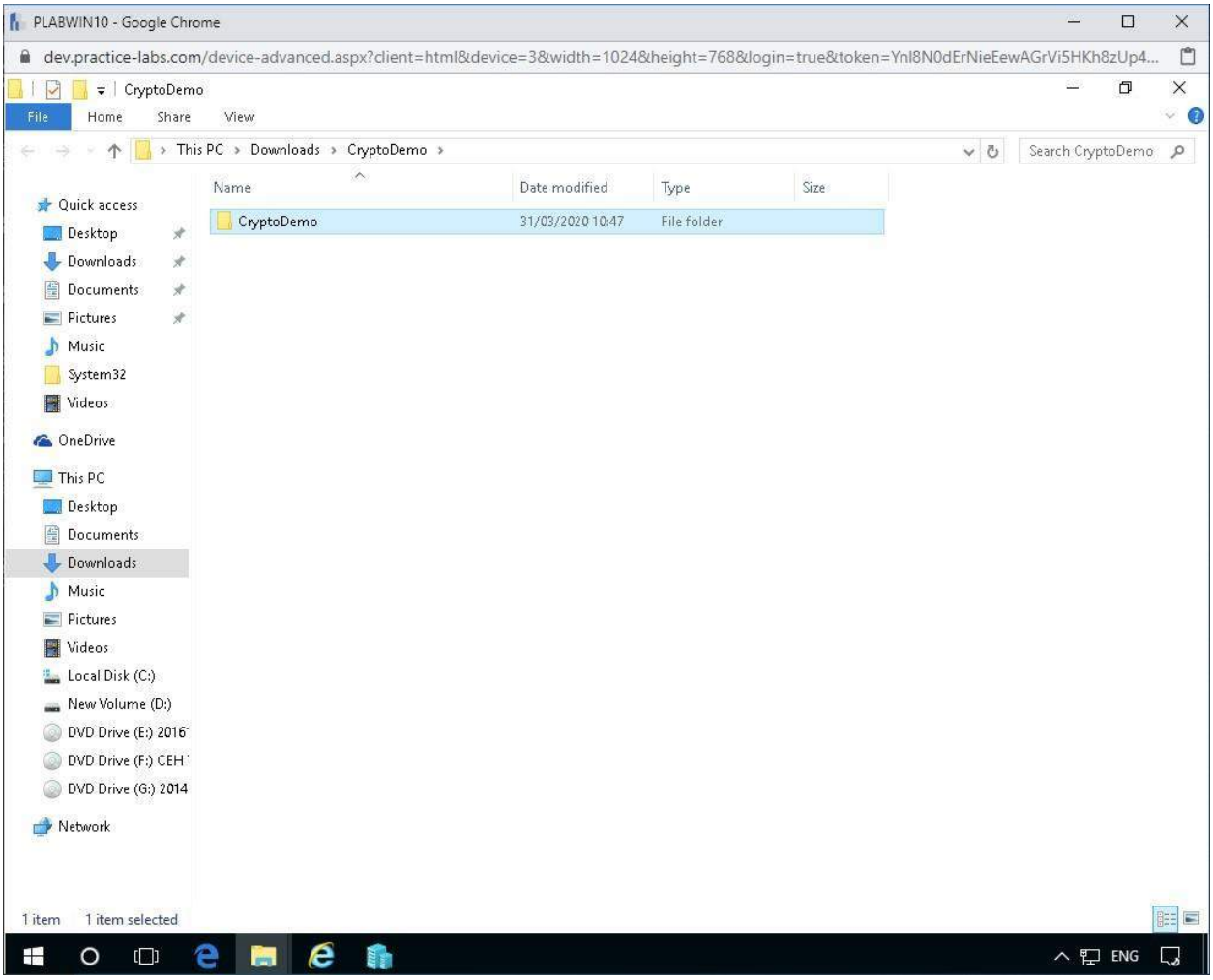


Figura 1.4. Captura de pantalla de PLABWIN10: Explorando la carpeta CryptoDemo en descargas

Navegue hasta el archivo de instalación y haga doble clic en el archivo de instalación.

Nota: *Es posible que reciba una advertencia de Control de cuenta de usuario. Presione Sí y continúe con la instalación.*

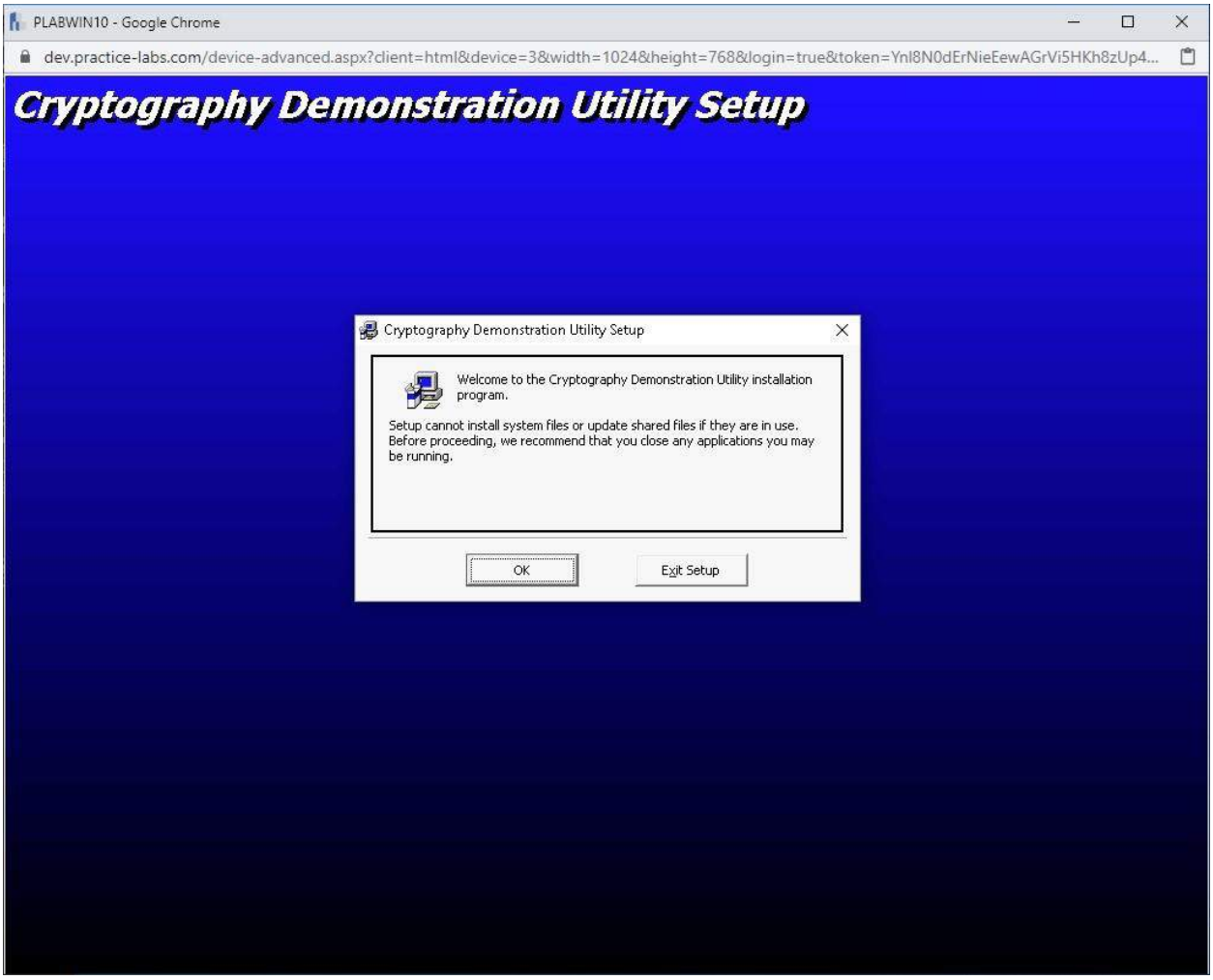


Figura 1.5. Captura de pantalla de PLABWIN10: asistente de instalación para CryptoDemo

Paso 5

Presione **OK** e instálelo en el siguiente directorio:

```
C:\Program Files
```

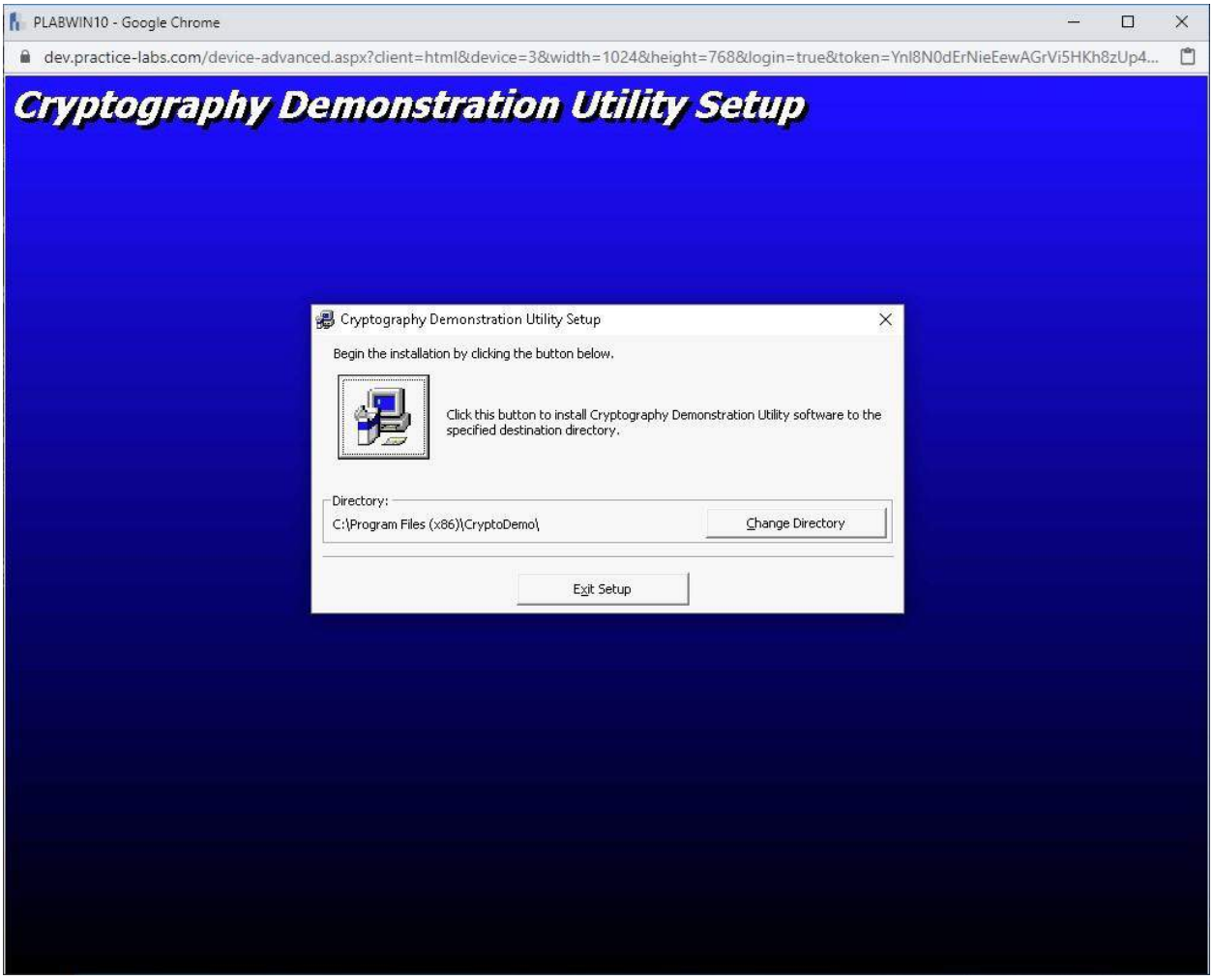


Figura 1.6. Captura de pantalla de PLABWIN10: asistente de instalación para CryptoDemo

Luego presione el icono del botón de la computadora para comenzar la instalación.

Presione **Continuar** en cada etapa adicional para completar la instalación.

Paso 6

Cierre todas las ventanas del Explorador de archivos y haga clic en el **ícono de Inicio** de Windows 10 .

Luego navegue a la **Demostración de criptografía** y haga clic en el programa **CrytoDemo1.0** para comenzar.

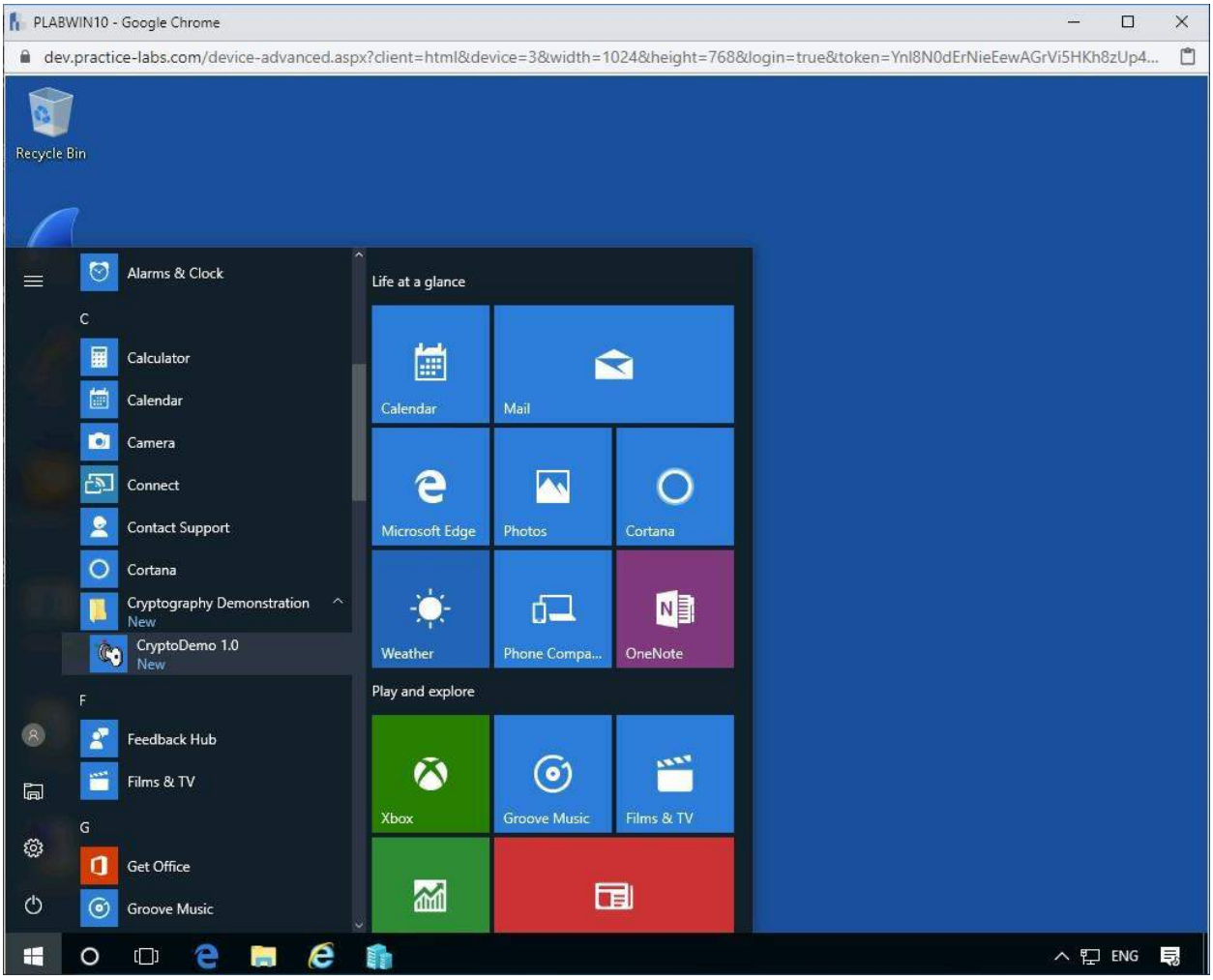


Figura 1.7. Captura de pantalla de PLABWIN10: CryptoDemo en el menú del programa

Arriba podemos ver el programa en el menú de inicio, y abajo podemos ver el mismo programa una vez que se ha abierto.

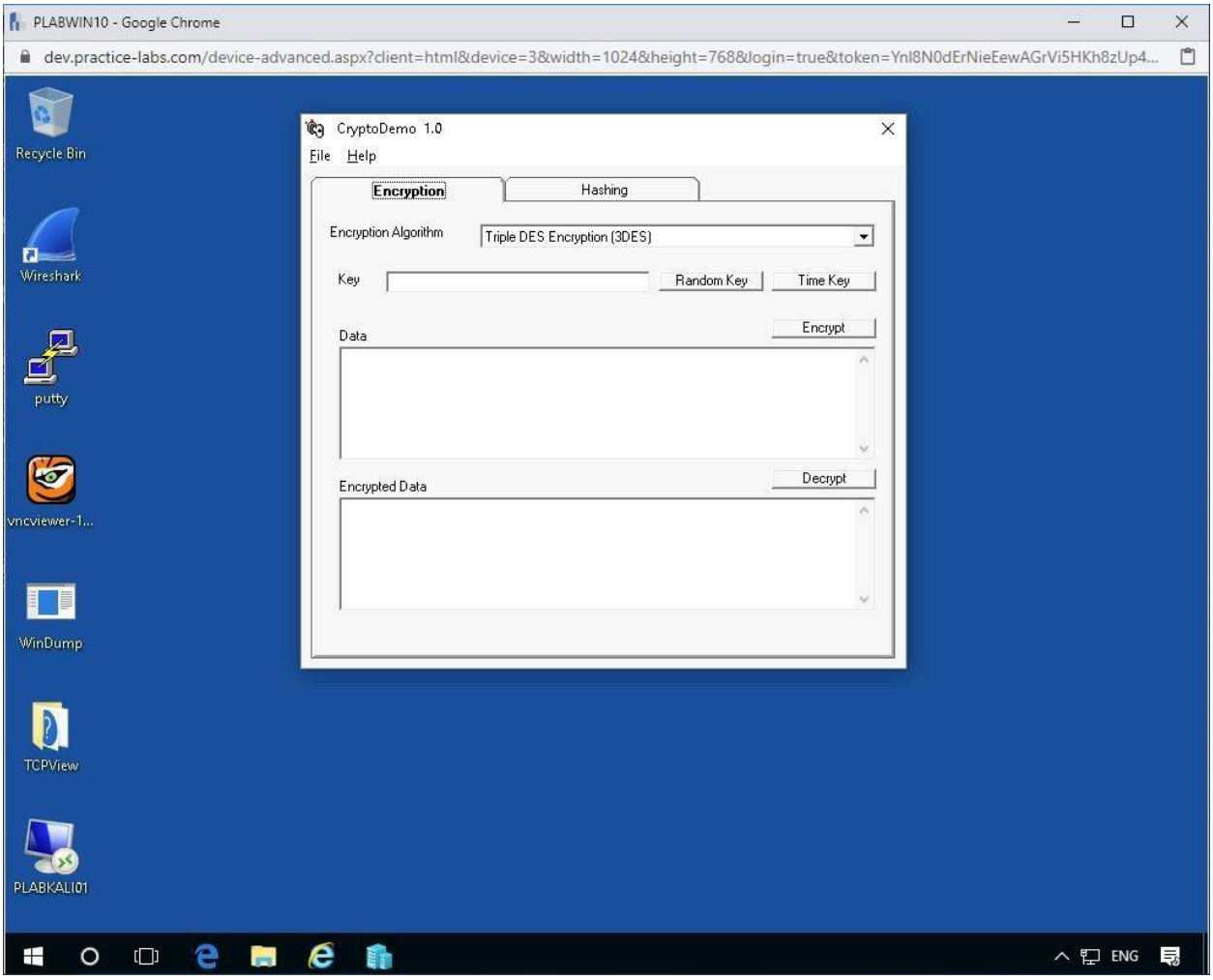


Figura 1.8. Captura de pantalla de PLABWIN10: CryptoDemo al inicio

Ahora estamos listos para continuar con la próxima tarea.

Tarea 2: cifrado de CryptoDemo

Ahora aplicaremos el algoritmo de cifrado 3DES para ver la salida y comenzar a reconocer qué genera dicha salida en términos de valores. Esto, de hecho, ayuda a las personas experimentadas a reconocer diferentes algoritmos a simple vista.

Paso 1

Tómese un momento para estudiar la interfaz; Este programa está diseñado para ayudar a practicar y aprender más sobre el cifrado.

Expanda el menú desplegable para el **Algoritmo de cifrado** y elija **Triple DES Encryption (3DES**).

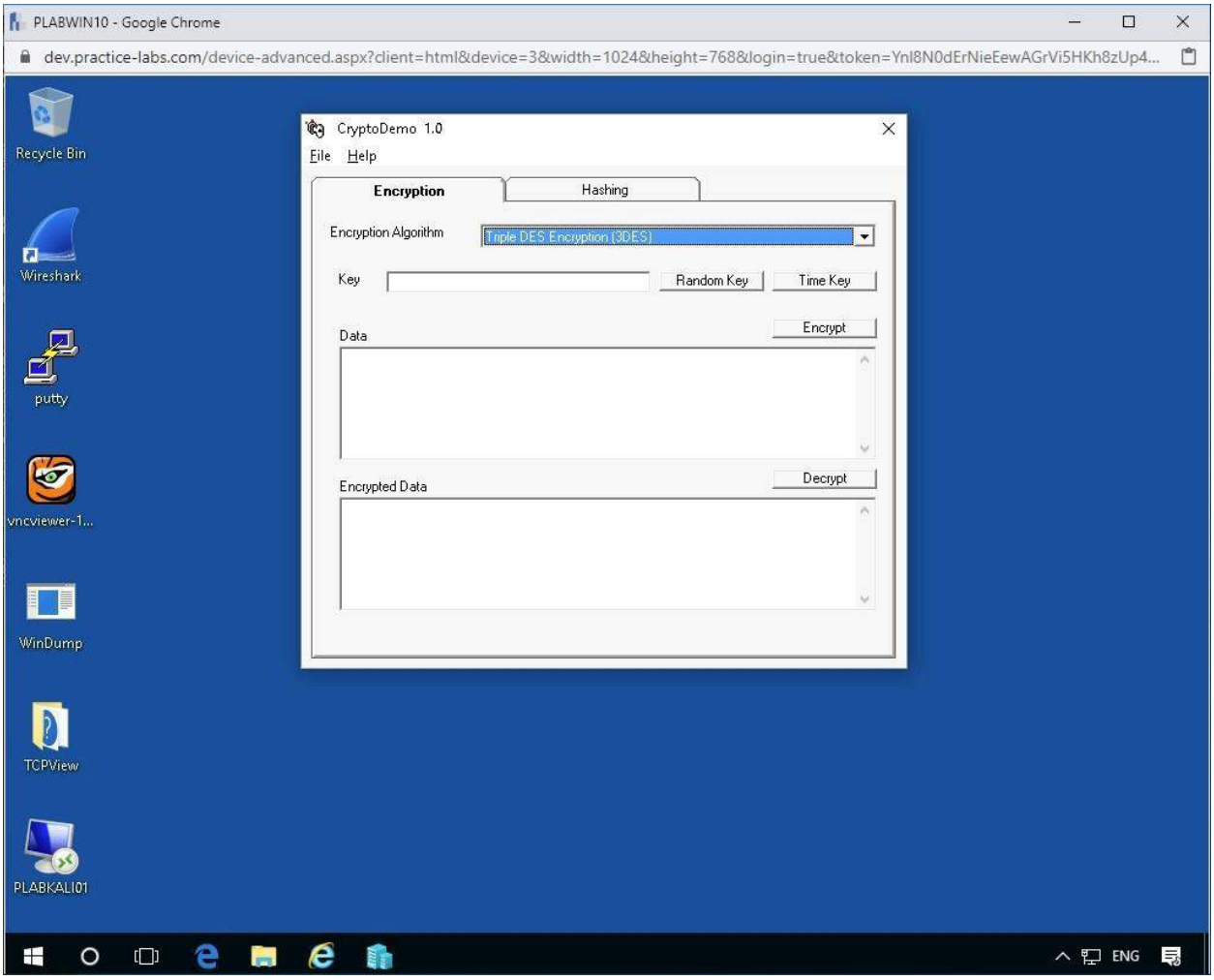


Figura 1.9. Captura de pantalla de PLABWIN10: CryptoDemo seleccionando el algoritmo 3DES

Paso 2

En la sección a continuación, puede ingresar una clave de su elección o utilizar la siguiente clave.

Escriba lo siguiente en el campo:

```
Practice-Labs.com
```

Paso 3

Ahora ingresaremos algo de texto en el campo de Datos para encriptar.

```
Welcome to Practice Labs, we hope you are really
enjoying the course!!
```

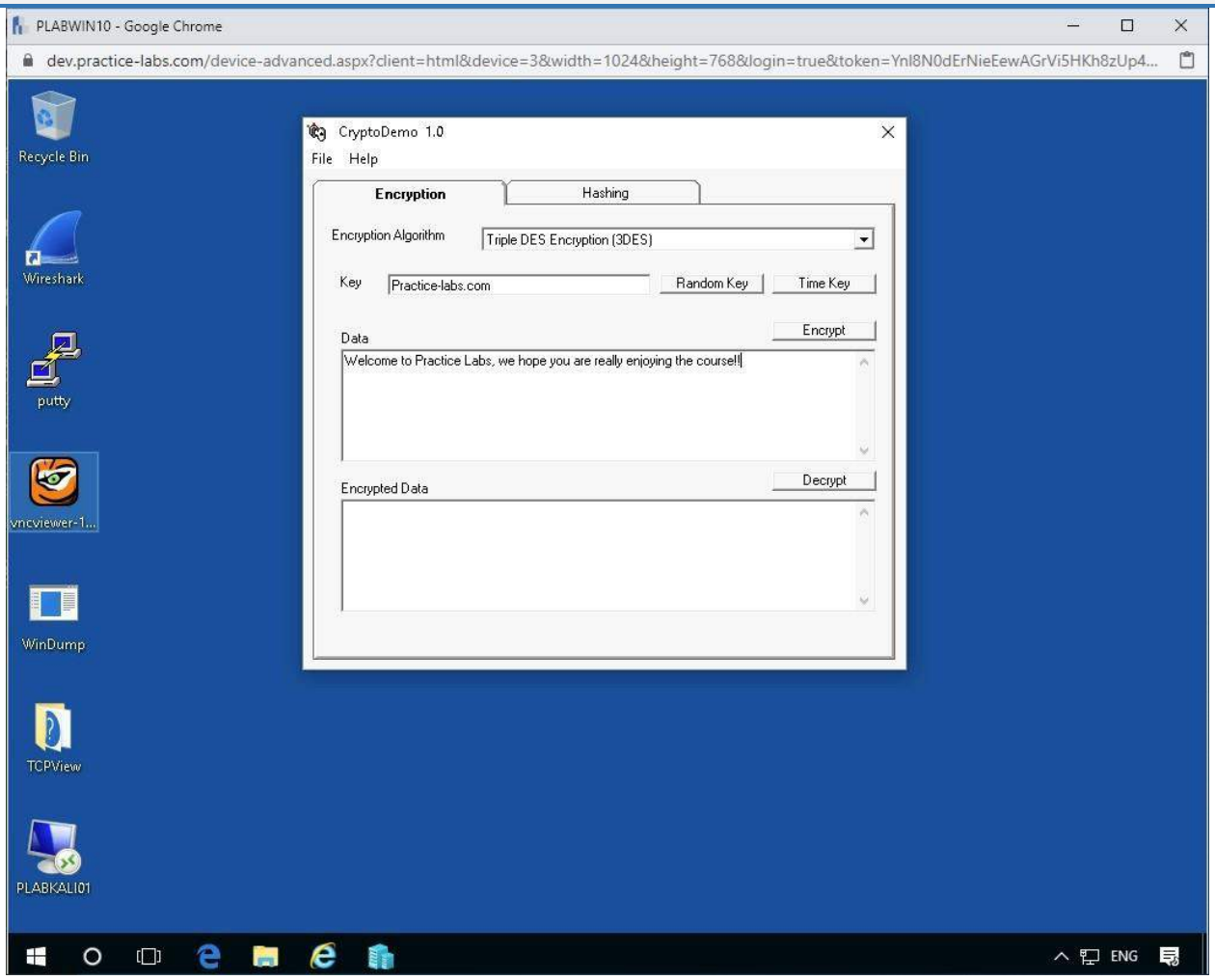


Figura 1.10. Captura de pantalla de PLABWIN10: CryptoDemo escribiendo en el texto

Ahora presione el botón **Cifrar** para ver el resultado del cifrado y se mostrará un resultado en el campo **Datos cifrados** .

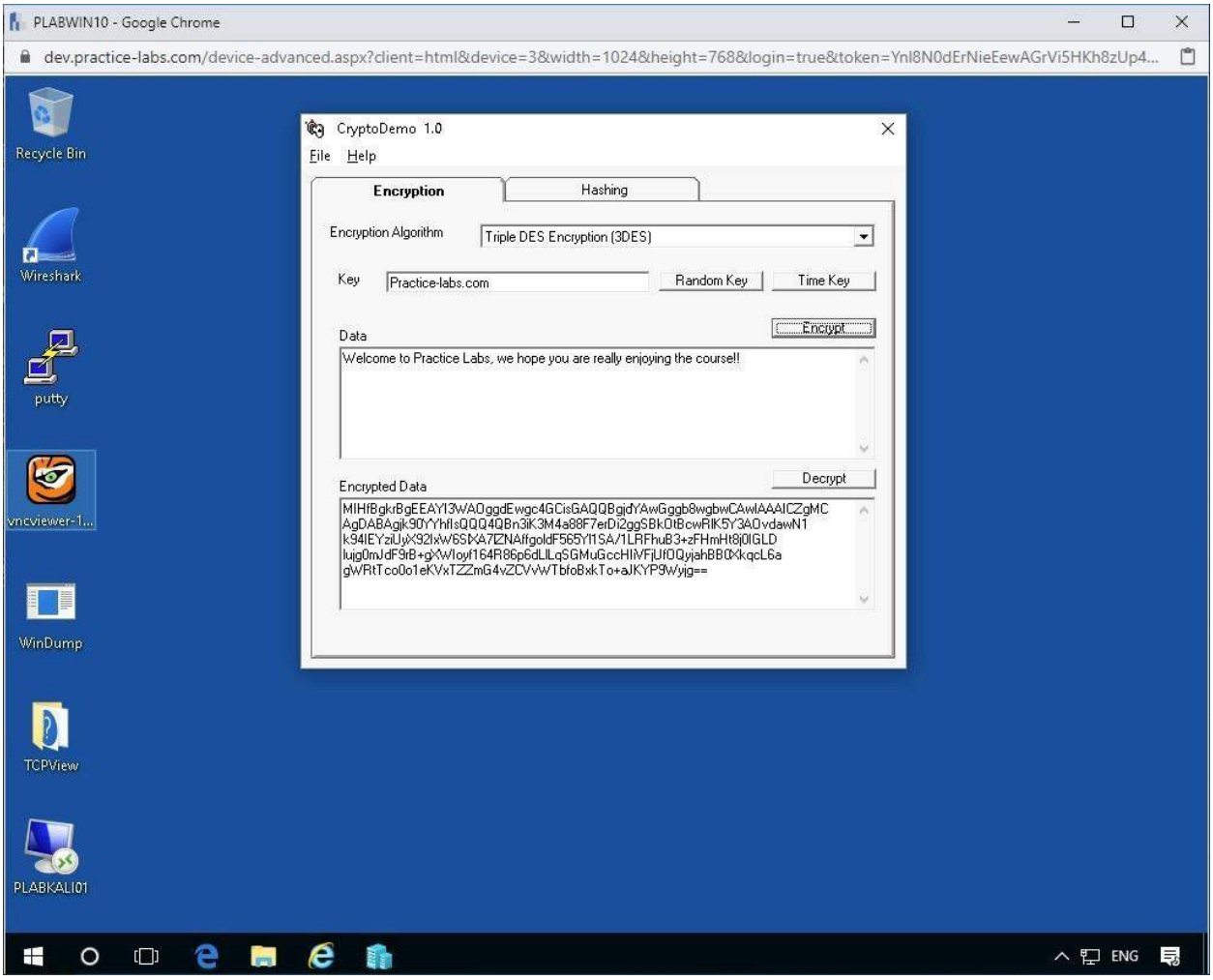


Figura 1.11. Captura de pantalla de PLABWIN10: texto cifrado de CryptoDemo

Puede presionar el botón **Cifrar** tantas veces como desee y verá resultados diferentes de los datos de salida; Este es uno de los conceptos más importantes detrás del cifrado de un texto. El texto cifrado debe ser diferente e ilegible.

Tarea 3: descifrado de CryptoDemo

Después de cifrar texto plano con CryptoDemo, pasamos a descifrar el contenido y nos aseguramos; tiene el mismo contenido que el previsto originalmente.

Paso 1

Ahora tenga cuidado, elimine solo el campo **Datos que** contiene el texto escrito que ingresó y no cambie la Clave ni el tipo de Algoritmo.

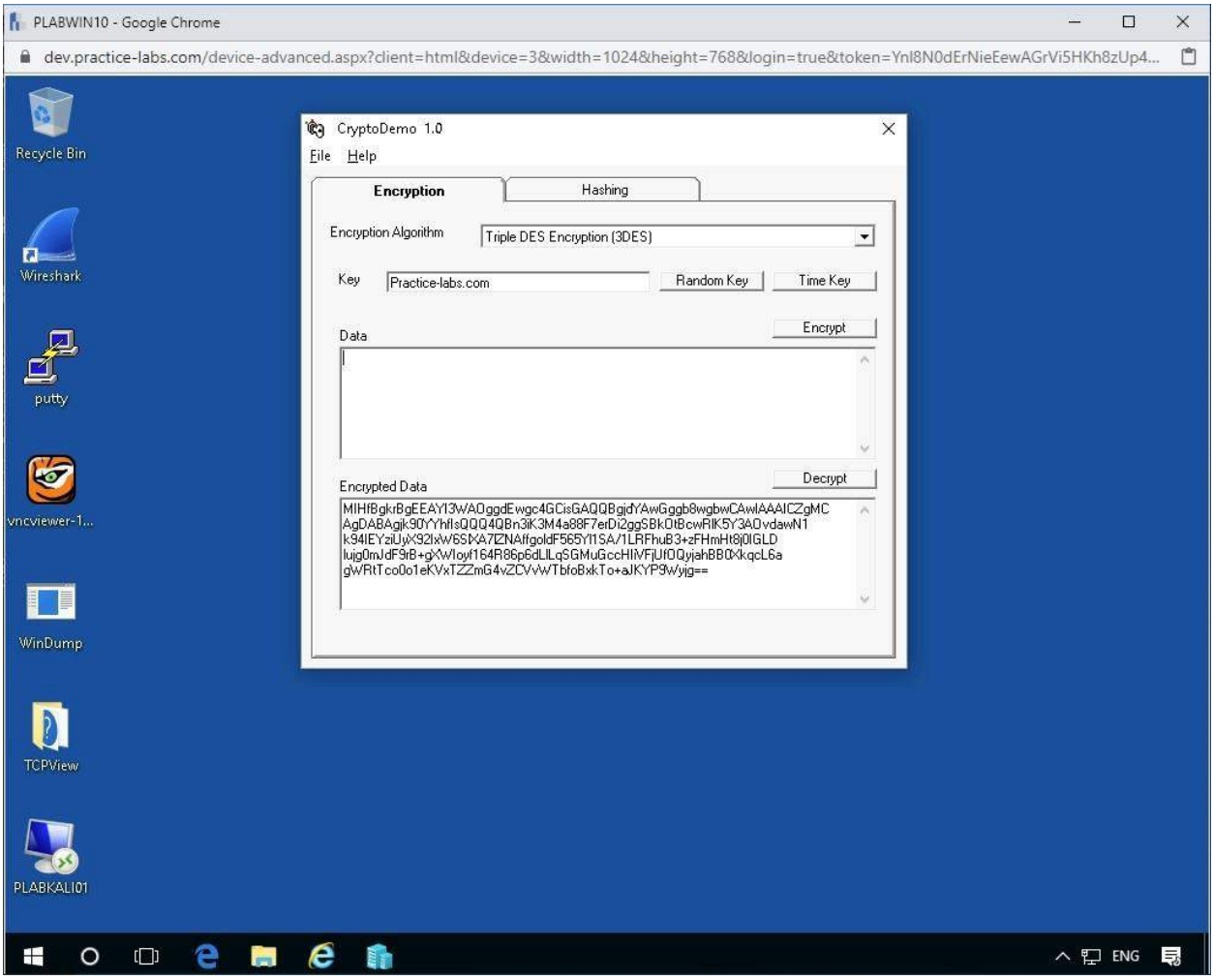


Figura 1.12. Captura de pantalla de PLABWIN10: descifrado de CryptoDemo

Presione el botón **Descifrar** para ver el resultado nuevamente en el campo **Datos** .

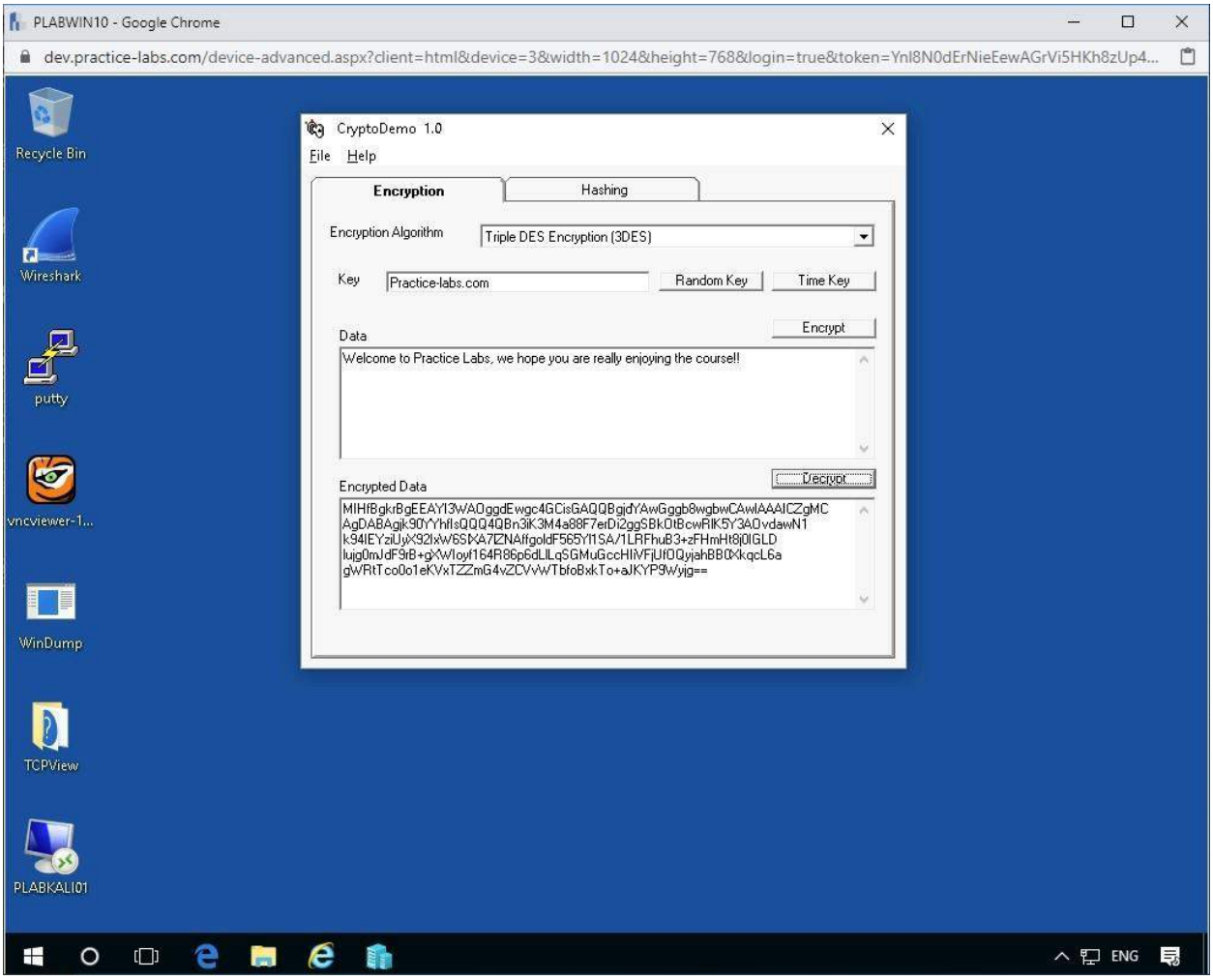


Figura 1.13. Captura de pantalla de PLABWIN10: resultados de descifrado de CryptoDemo

Tendrá el mismo texto original descifrado de los datos.

Ahora puede probar los otros tipos de algoritmos de DES, RC2, RC4 para ver la salida de estos.

Paso 2

Intente eliminar un solo carácter o más de los Datos cifrados. Aquí se eliminó el último = firmado presentando la siguiente imagen.

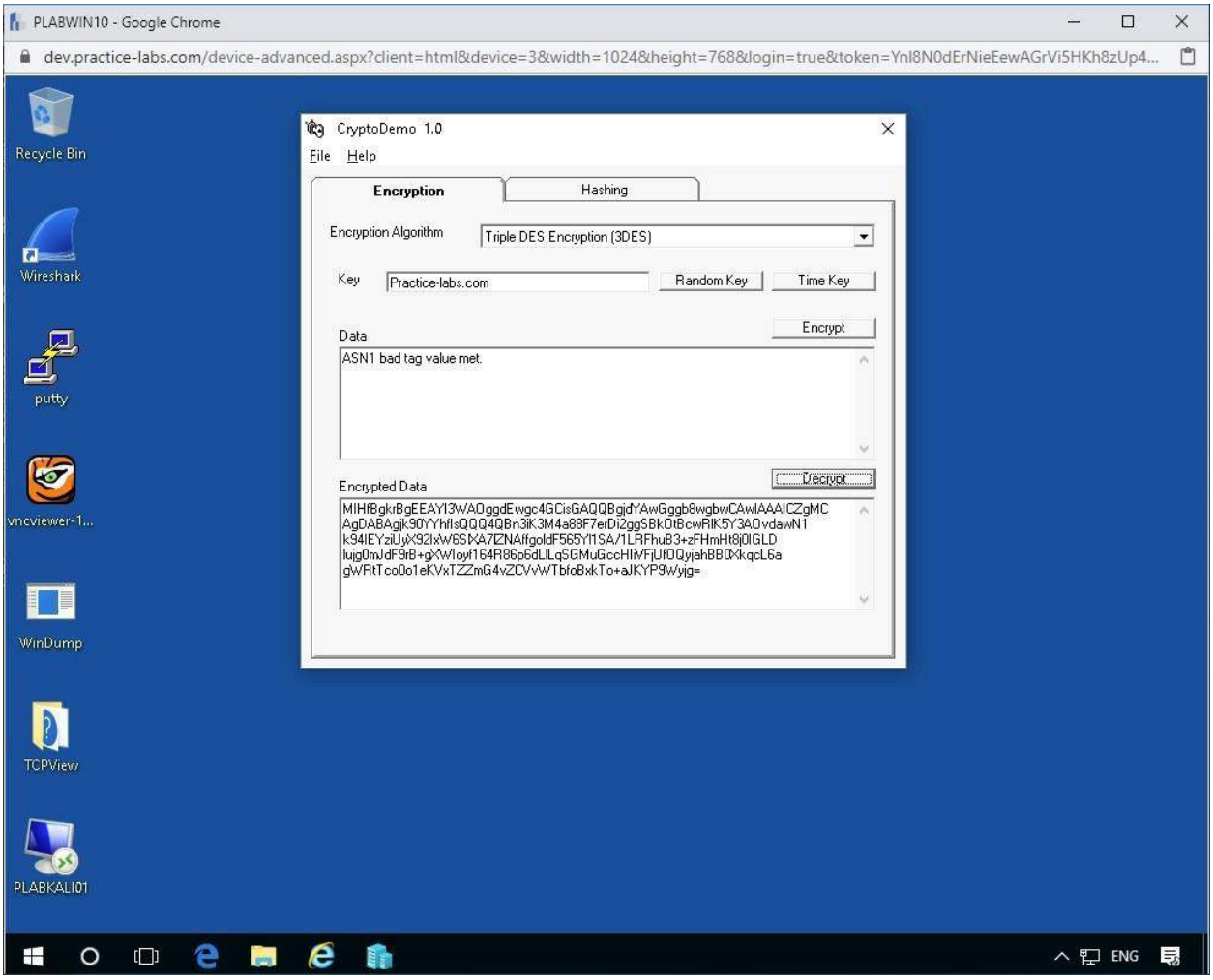


Figura 1.14. Captura de pantalla de PLABWIN10: resultados de descifrado de CryptoDemo

Debería obtener algo similar ya que el programa no pudo decodificar los datos cifrados. Este es un resultado positivo.

Tarea 4: valores clave

En general, mezclar tantas variables como sea posible con longitudes de cadena largas produce una clave segura para cifrar o hacer hash, sin embargo, aquí utilizaremos las opciones presentadas de Clave aleatoria y Clave de tiempo.

Ahora aplicaremos estos formatos clave para ver los resultados.

Paso 1

Anteriormente ingresamos la nuestra, sin embargo, en realidad, esta es una clave mal asegurada y una mejor opción sería generar una clave de valor aleatorio o de tiempo que sea mucho más segura.

Eliminar el contenido de los **datos cifrados** .

Probemos con el botón **Clave aleatoria** para ver qué clave se le presenta.

Nota: *es aleatorio, por lo que su clave no debe coincidir con las imágenes, tampoco lo harán sus valores de tiempo*

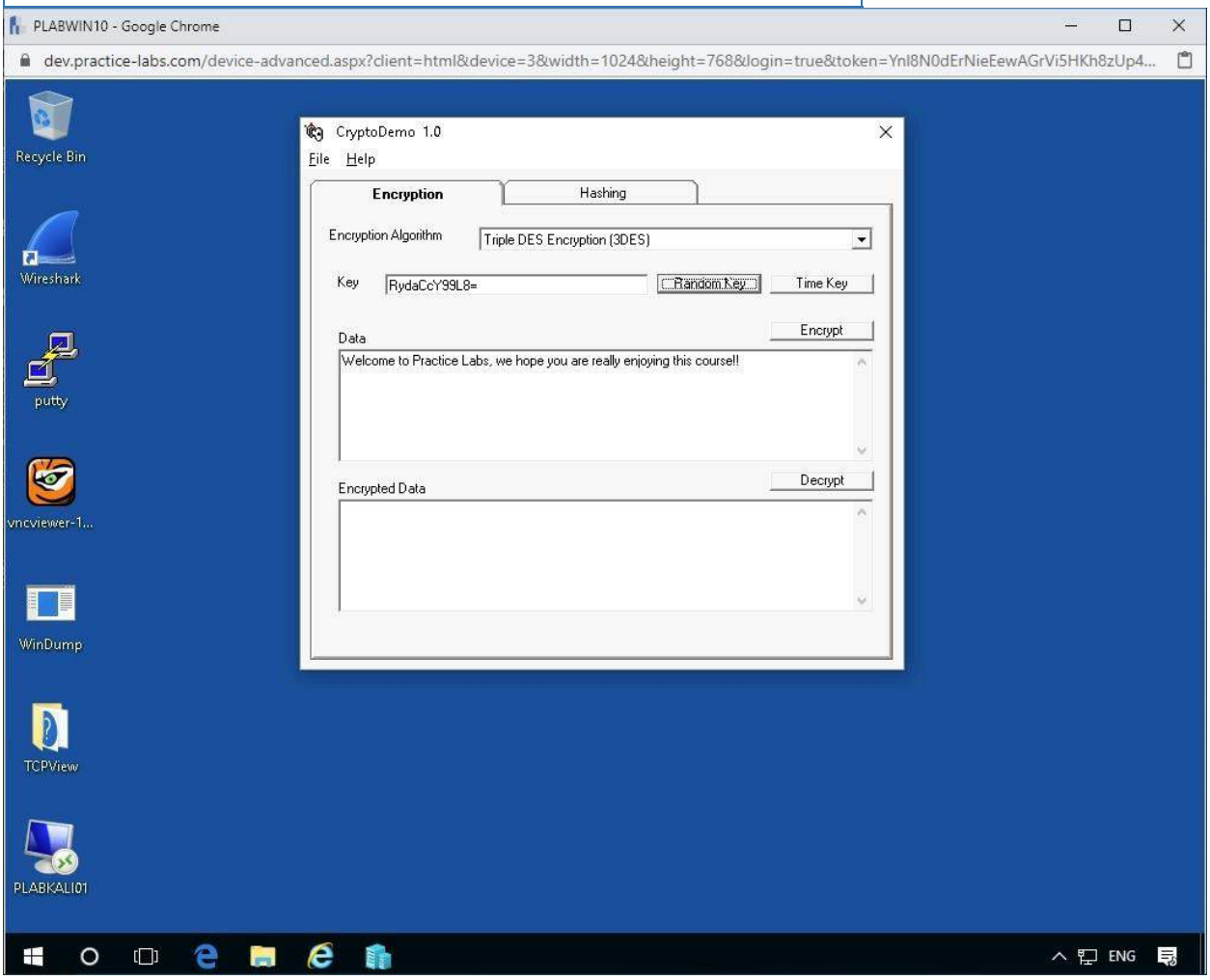


Figura 1.15. Captura de pantalla de PLABWIN10: resultados de descifrado de CyptoDemo

Nuevamente **presione el** botón **Cifrar** para ver el texto cifrado generado con este tipo de clave.

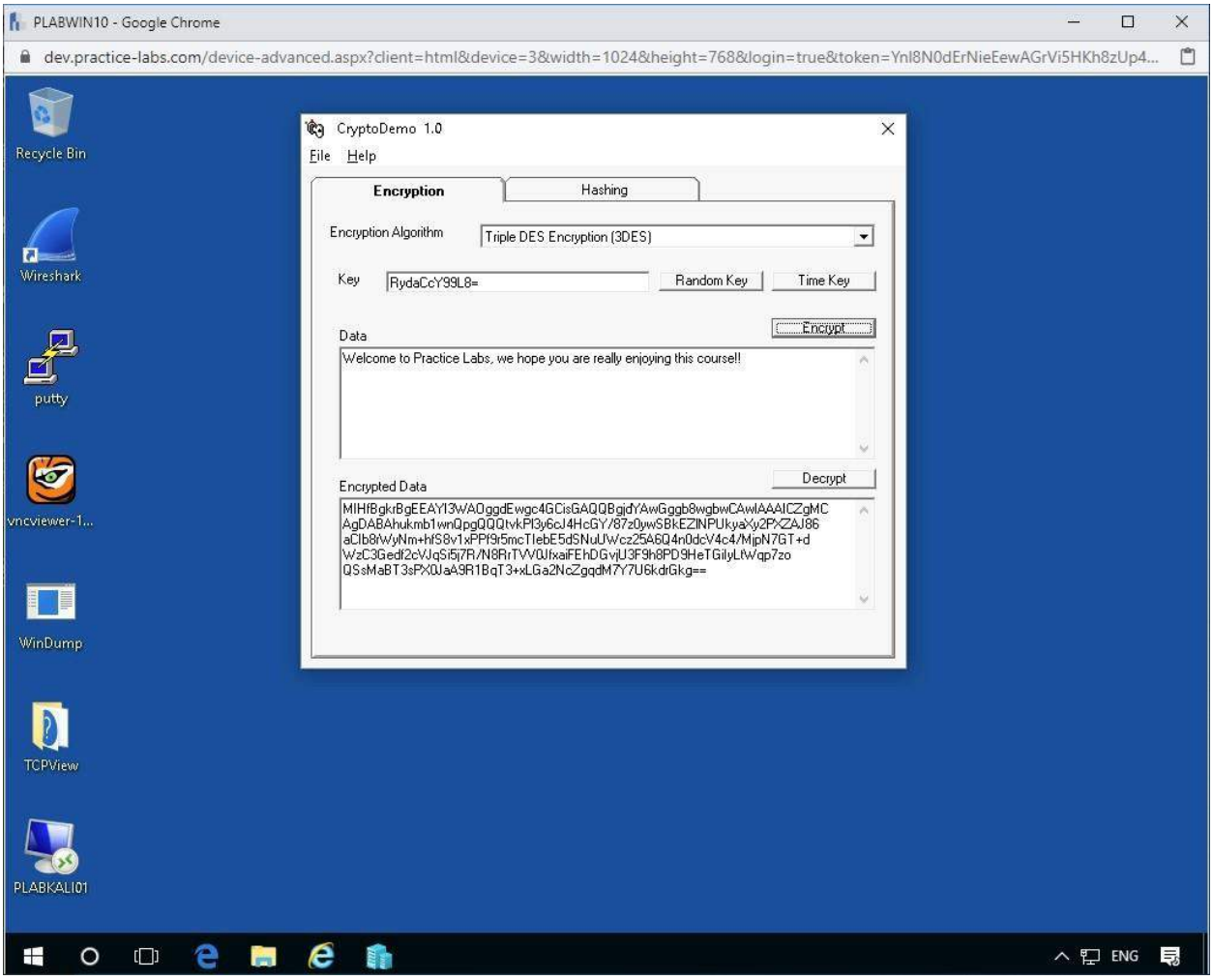


Figura 1.16. Captura de pantalla de PLABWIN10: resultados de descifrado de CryptoDemo

De la imagen de arriba podemos ver un resultado muy diferente usando este valor clave.

Paso 2

Ahora elimine los datos cifrados nuevamente y presione el botón de la **tecla de tiempo** .

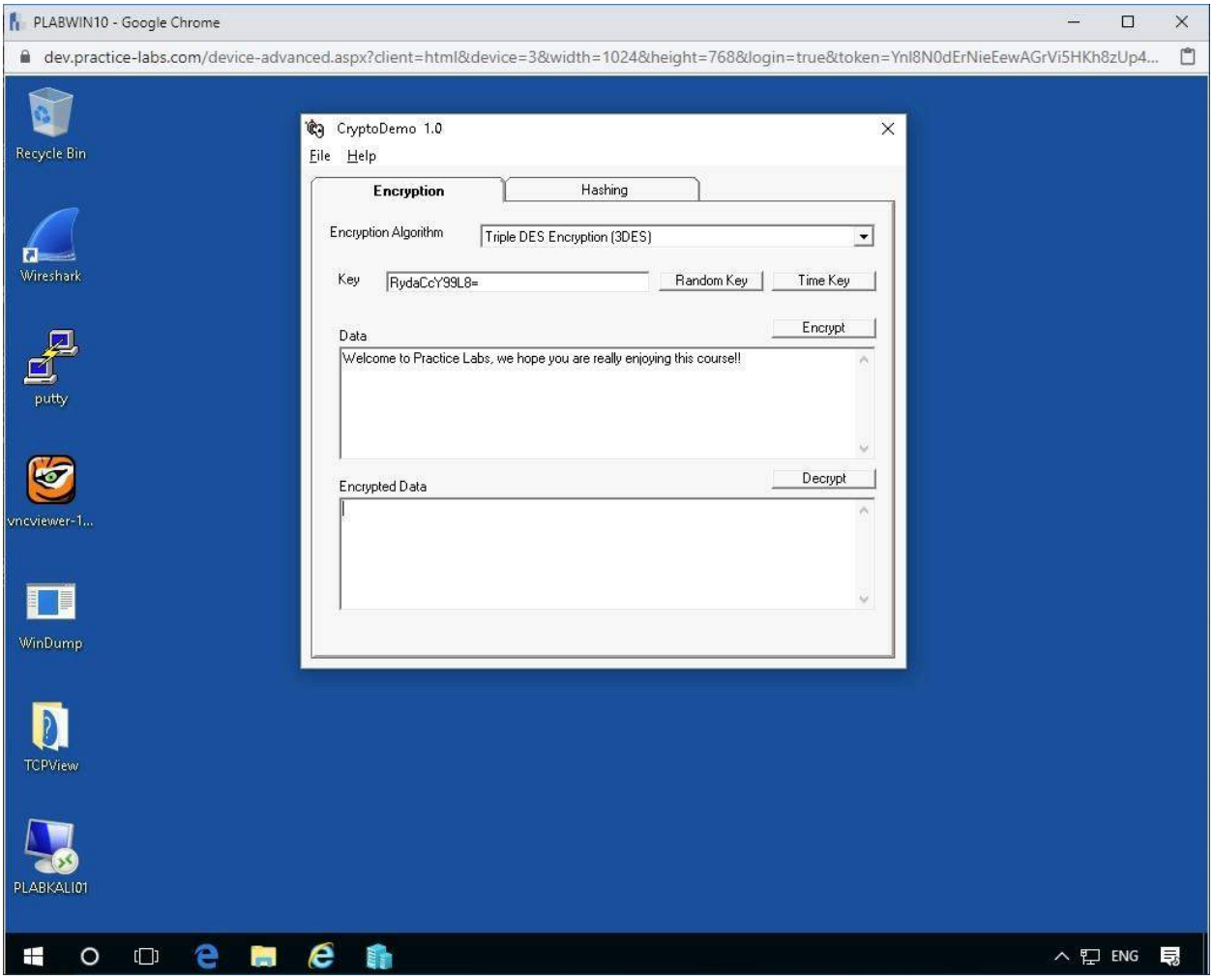


Figura 1.17. Captura de pantalla de PLABWIN10: resultados de descifrado de CryptoDemo

Nuevamente **presionemos el** botón **Cifrar** y veamos los valores generados.

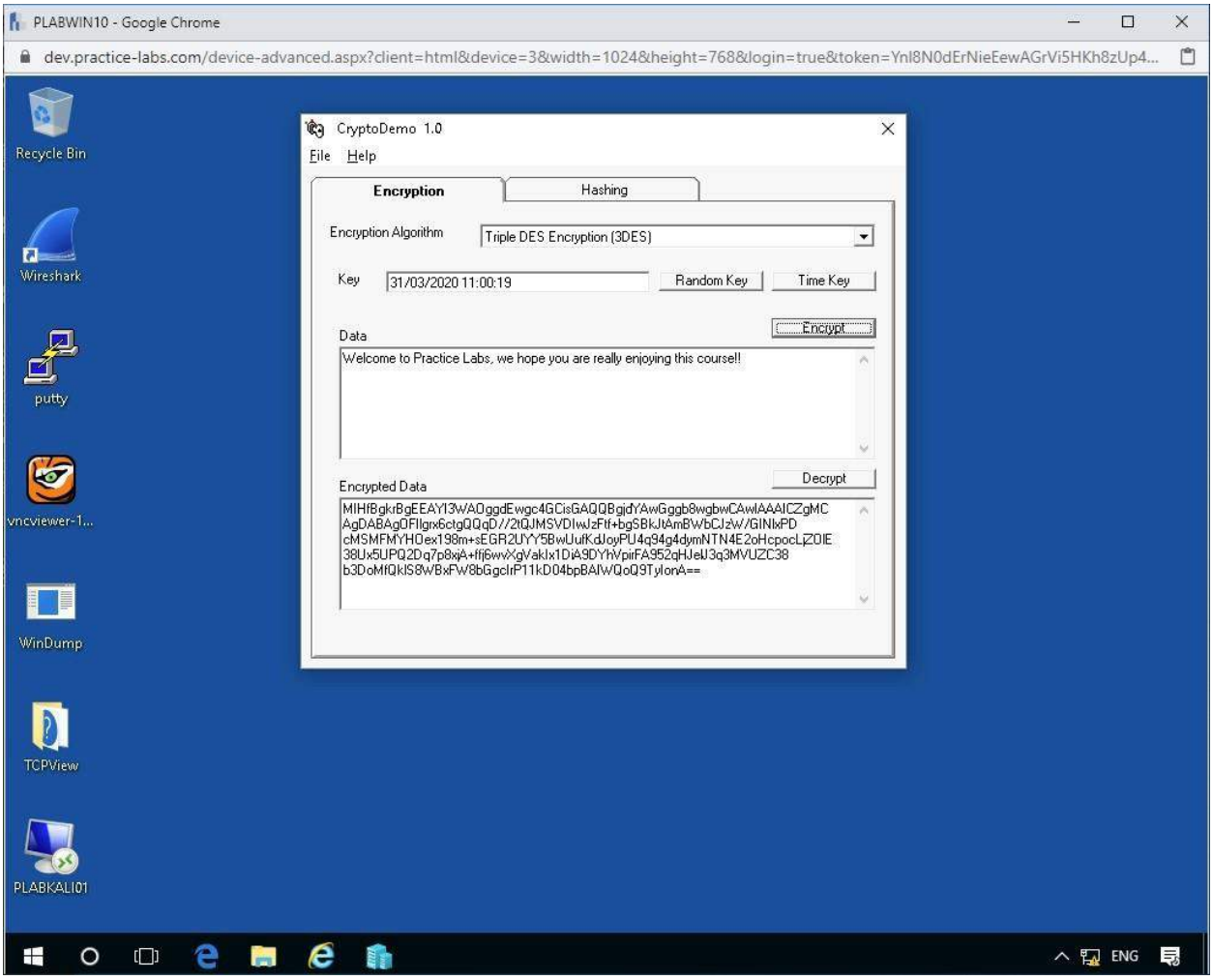


Figura 1.18. Captura de pantalla de PLABWIN10: resultados de descifrado de CryptoDemo

Una vez más vemos otra salida que difiere del primer resultado.

Tarea 5 - Hashing

Hashing un valor se utiliza para asignar datos de cualquier tamaño y proporcionar un método para verificar la integridad y también la autenticidad de los datos y sus autores.

Aquí aplicaremos la misma herramienta para ver resultados hash.

Paso 1

Haga clic en la pestaña **Hashing** en la parte superior, y verá que el Algoritmo Hash se ha establecido en **MD5,** que es un tipo de hash muy común.

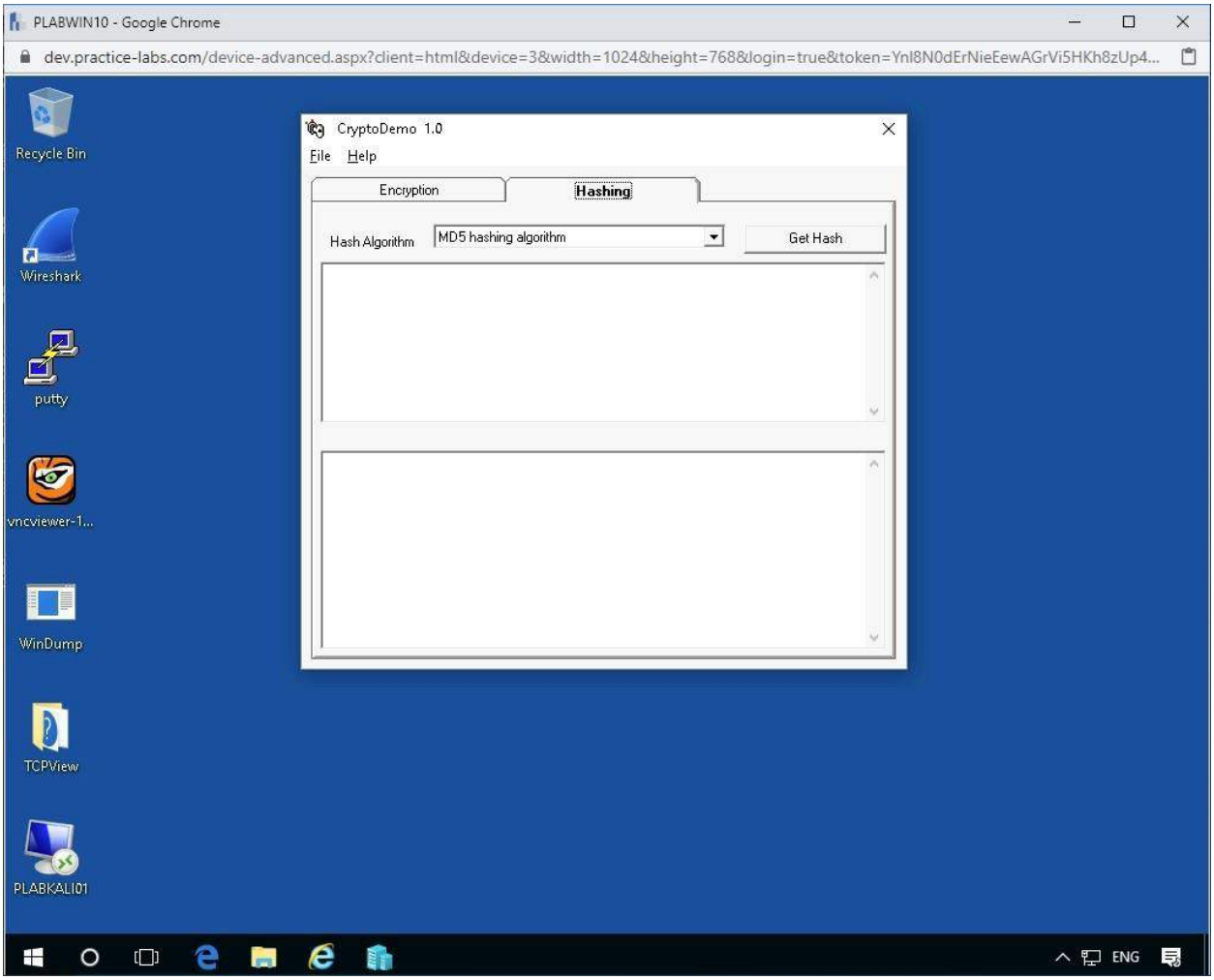


Figura 1.19. Captura de pantalla de PLABWIN10: pantalla de CryptoDemo Hashing

Paso 2

Dentro del campo superior, escribe algo diferente.

```
Congratulations, you are learning how hashing
works!
```

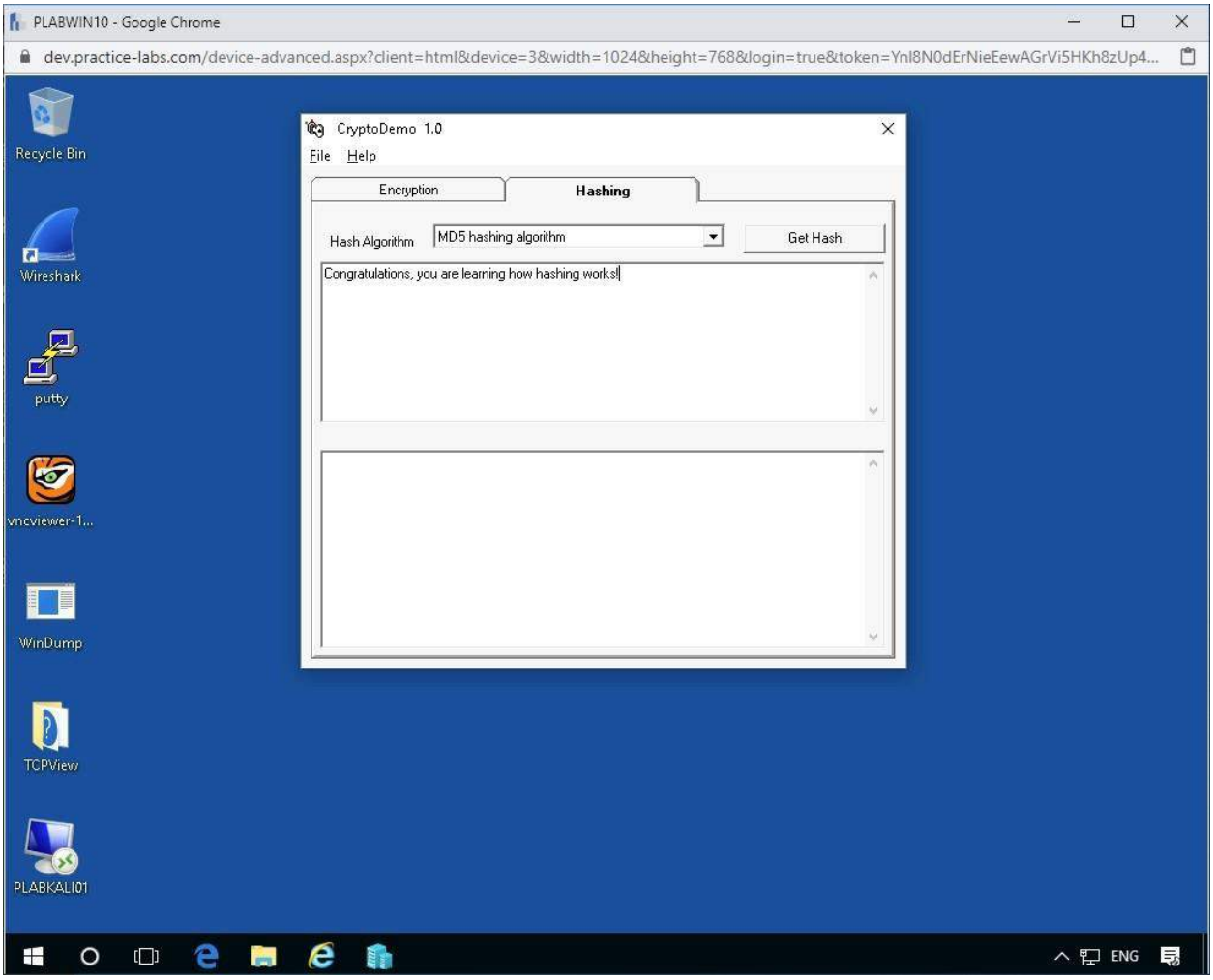


Figura 1.20. Captura de pantalla de PLABWIN10: pantalla CryptoDemo Hashing con hash MD5

A diferencia de la etapa de cifrado anterior, este hash no cambiará si presiona el botón.

Consigue Hash

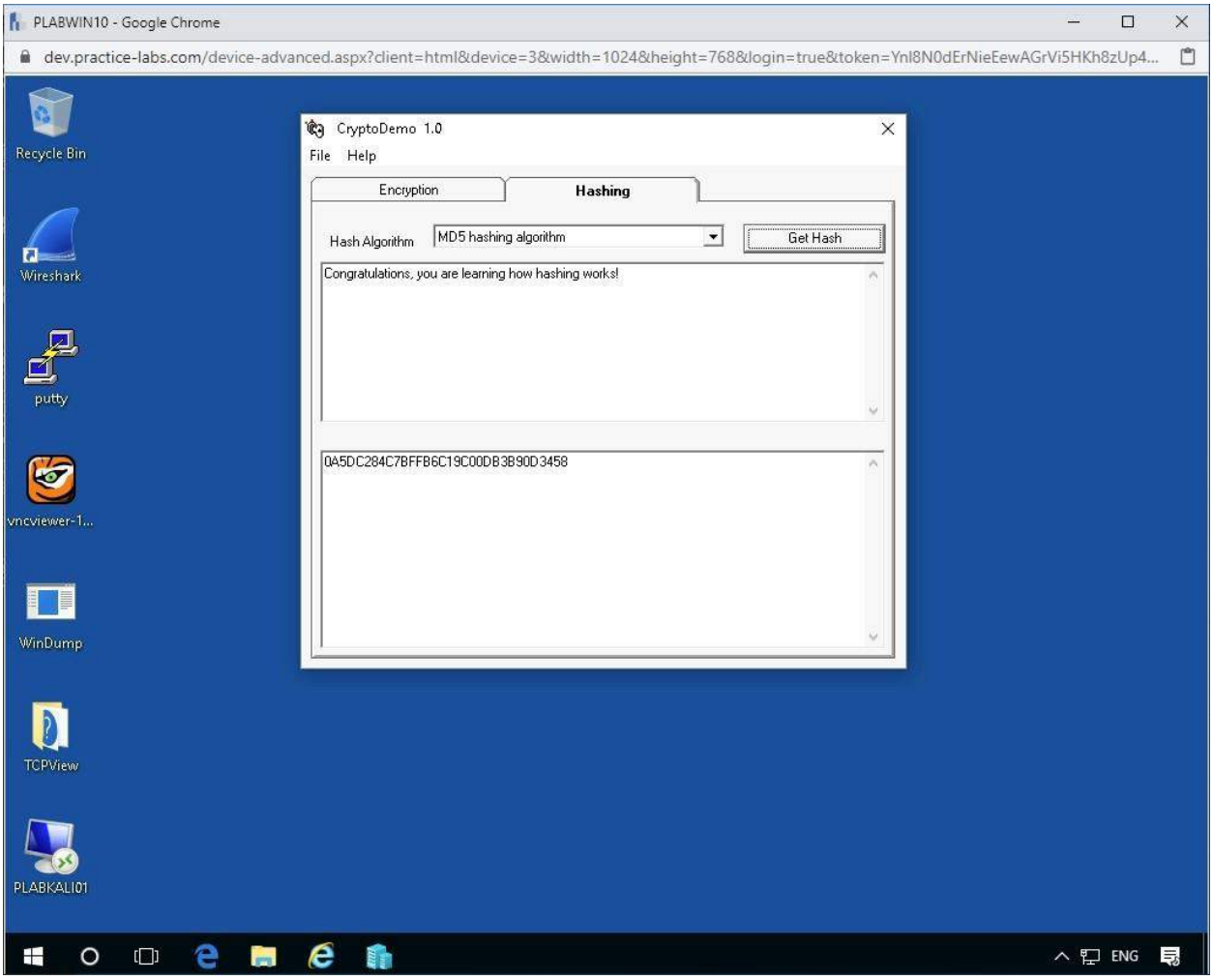


Figura 1.21. Captura de pantalla de PLABWIN10: pantalla CryptoDemo Hashing con hash MD5

Paso 3

En el menú desplegable del **algoritmo Hash** , haga clic en uno de los otros tipos, como **SHA1,** y luego presione el botón.

Consigue Hash

Ahora verá un resultado diferente para cada algoritmo.

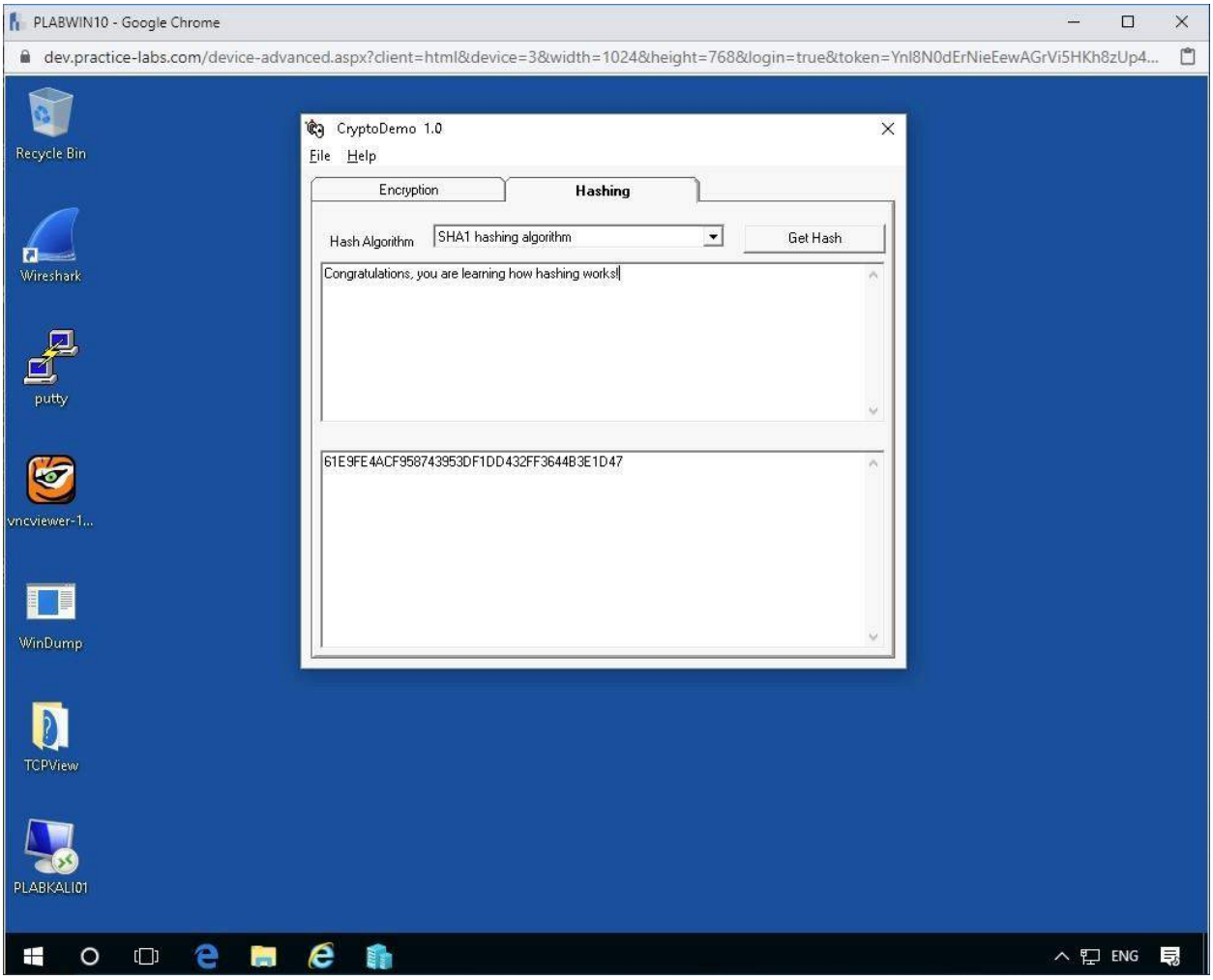


Figura 1.22. Captura de pantalla de PLABWIN10: CryptoDemo Hashing con hash SHA1

Salga del programa cuando haya terminado y pase al siguiente ejercicio.

Ejercicio 2: comparación de algoritmos de hash

Ahora veremos una variedad diferente de algoritmos en una comparación directa y utilizando Hash Calc, que es una calculadora que calcula resúmenes de mensajes, sumas de verificación y HMAC para archivos, así como para texto y cadenas hexadecimales. Proporciona 13 algoritmos populares de hash y suma de comprobación para los cálculos.

En este ejercicio, aprenderá lo siguiente:

- Instalar Hash Calc
- Usando Hash Calc

Para obtener información adicional sobre los algoritmos de Hash, consulte el material del curso o utilice su motor de búsqueda favorito para investigar este tema con más detalle.

Tarea 1: instalar HashCalc

En esta tarea, instalaremos Hash Calc y aprenderemos un poco más sobre cómo funciona, especialmente interesante es la capacidad de comparar numerosos resultados y ver cómo aparecen.

Paso 1

Asegúrese de que la ventana del **Explorador de archivos** esté abierta.

Vaya a la siguiente ruta de carpeta:

```
E:\CRYPTO
```

Desde el panel de detalles a la derecha, haga clic en el archivo **Hashcalc.zip** .

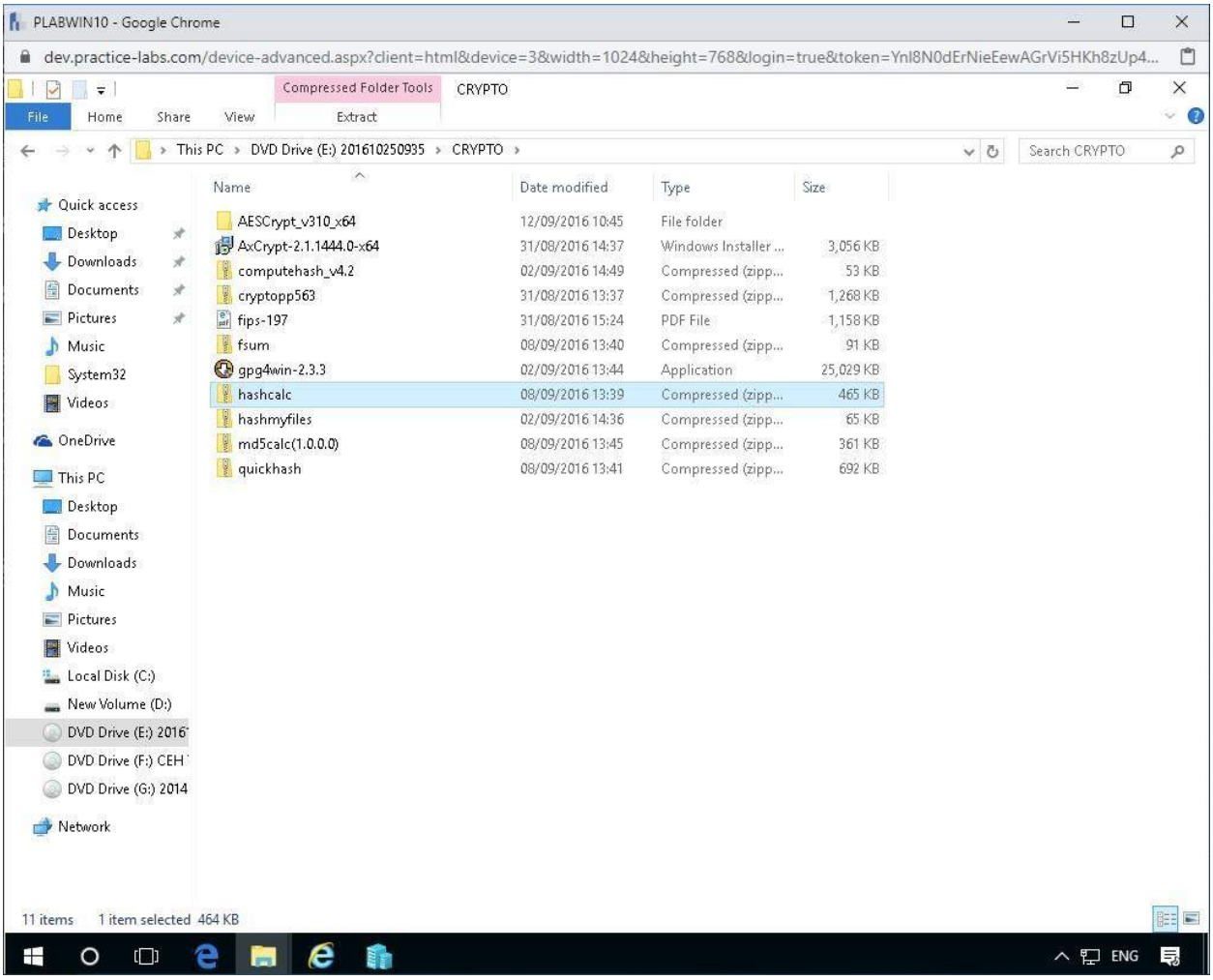


Figura 2.0. Captura de pantalla de PLABWIN10: Hashcalc

Haga doble clic en el archivo de **instalación** .

Siga los pasos de instalación e instálelo en el directorio C: \ Archivos de programa.

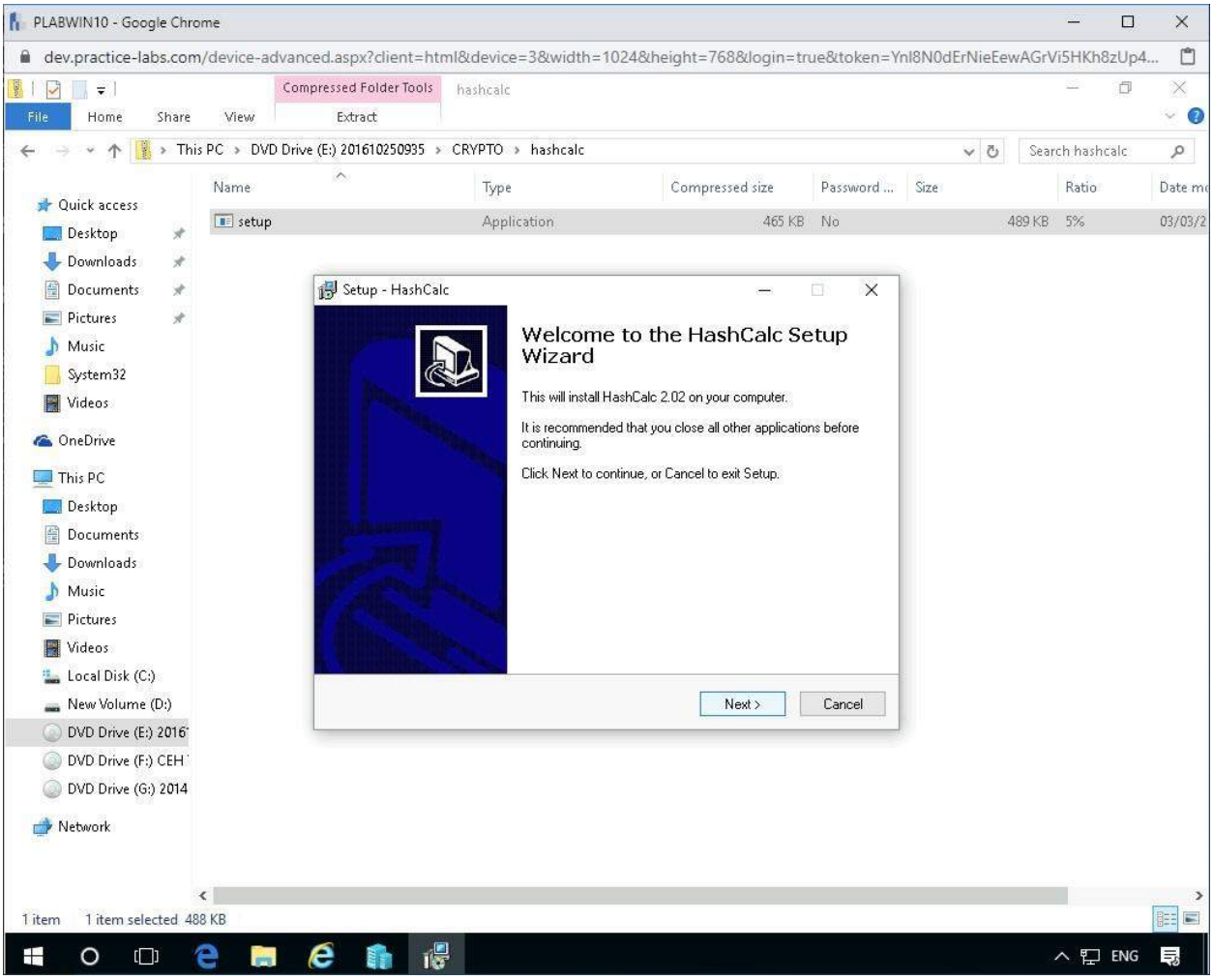


Figura 2.1. Captura de pantalla de PLABWIN10: Instalación de Hashcalc

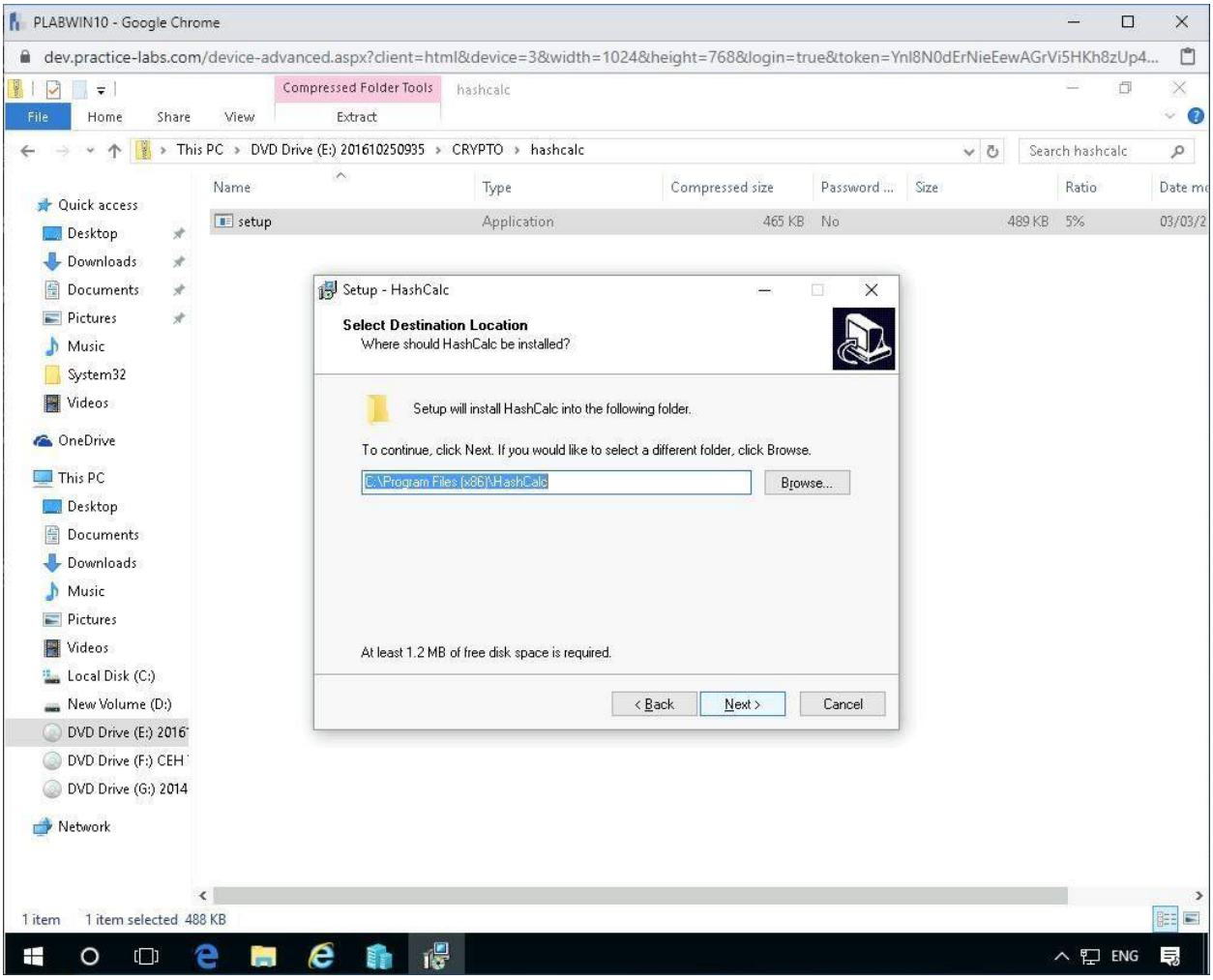


Figura 2.2. Captura de pantalla de PLABWIN10: instalación de Hashcalc en la unidad c

Continúe con la instalación en el directorio predeterminado.

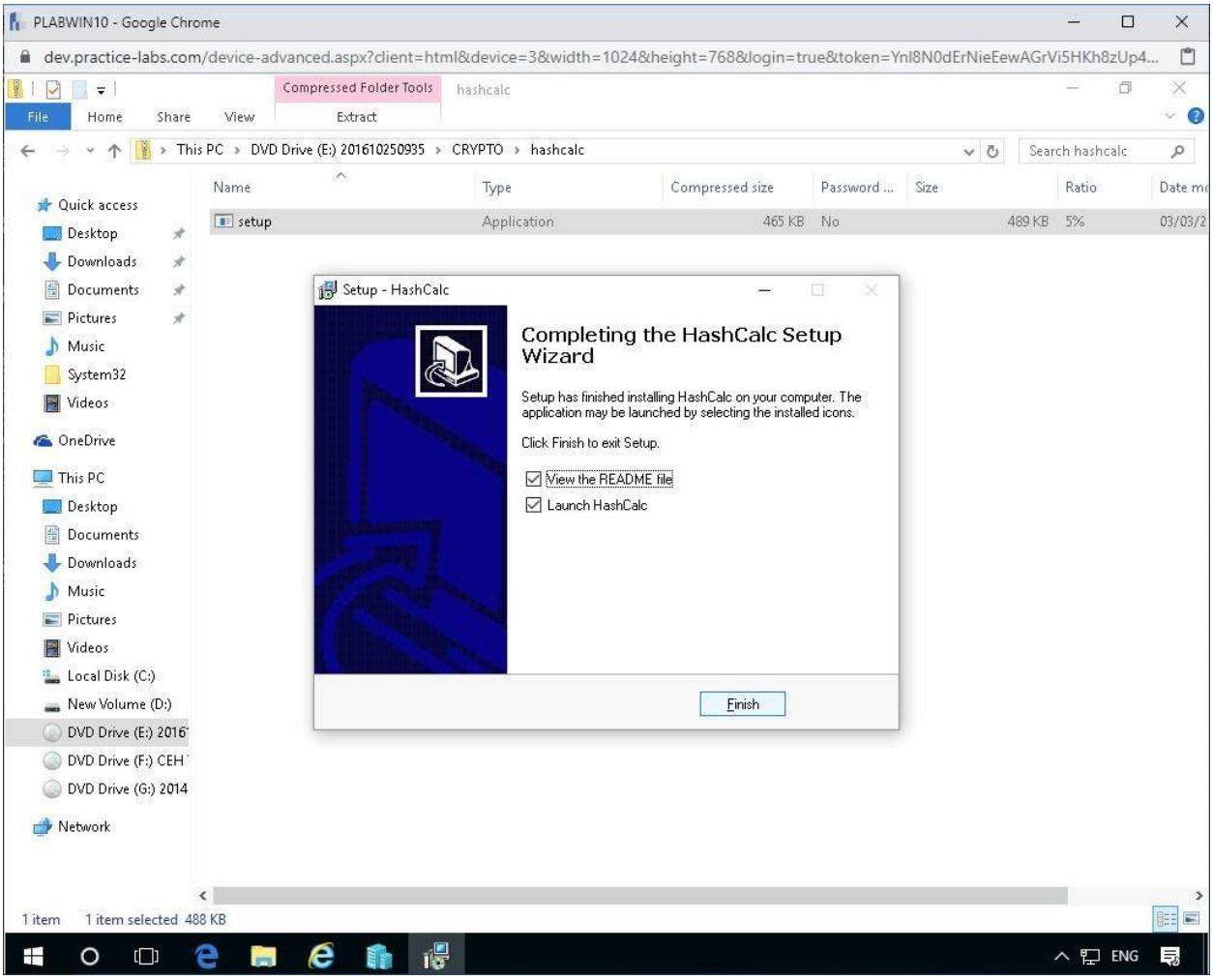


Figura 2.3. Captura de pantalla de PLABWIN10: instalación de Hashcalc finalizada

Tarea 2: uso de HashCalc

Ahora aplicaremos HashCalc para ver los resultados una vez que apliquemos algunos datos como texto de cadena.

Paso 1

Haga clic en el campo **Formato de datos** y cámbielo a **Cadena de texto.**

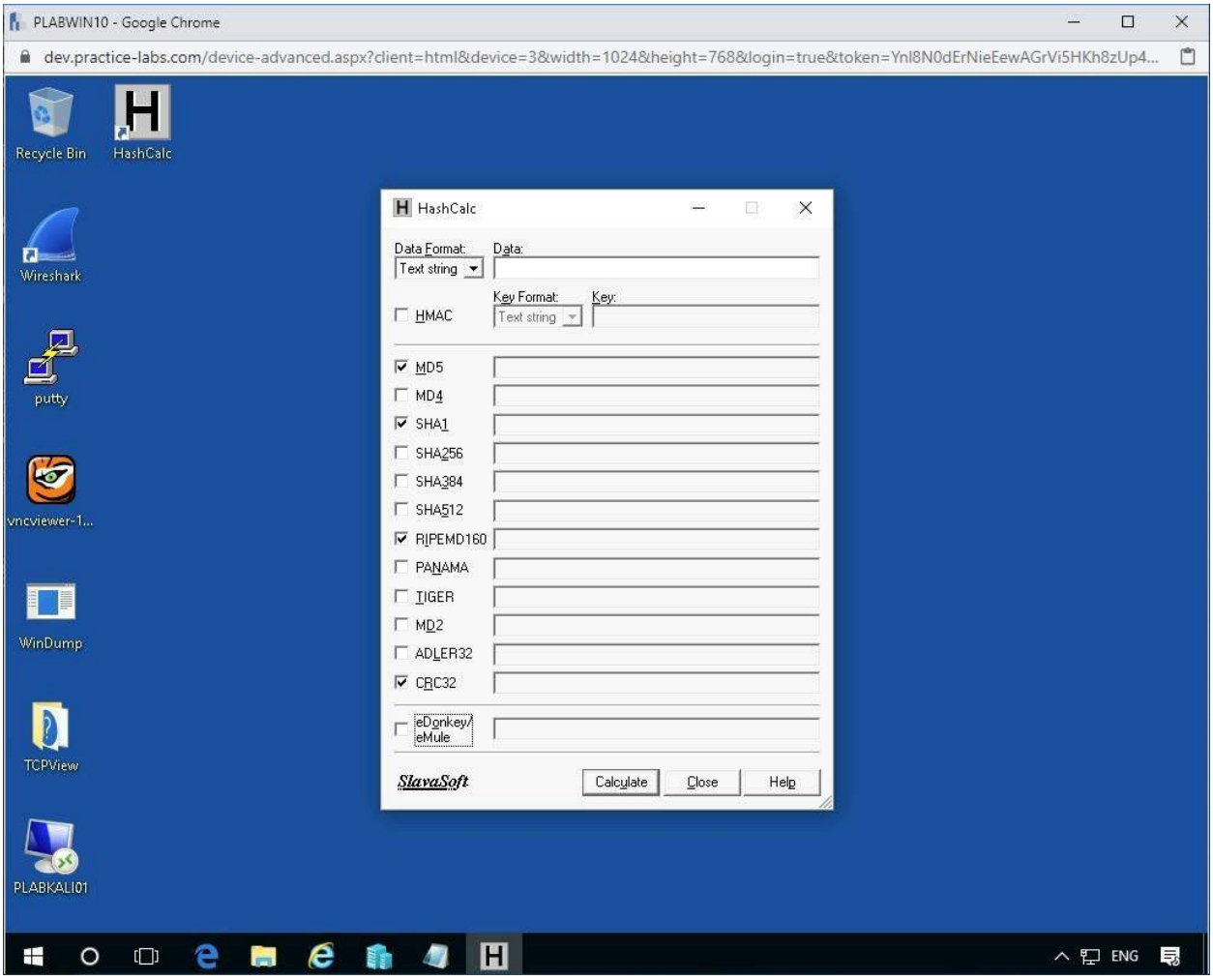


Figura 2.4. Captura de pantalla de PLABWIN10: interfaz Hashcalc

Ingrese algo de texto en el campo **Datos** como:

```
Welcome to Device PLABWIN10
```

Después de esto, asegúrese de que todas las casillas de verificación estén confirmadas para todos los algoritmos de hash, excepto HMAC, que deben dejarse vacíos.

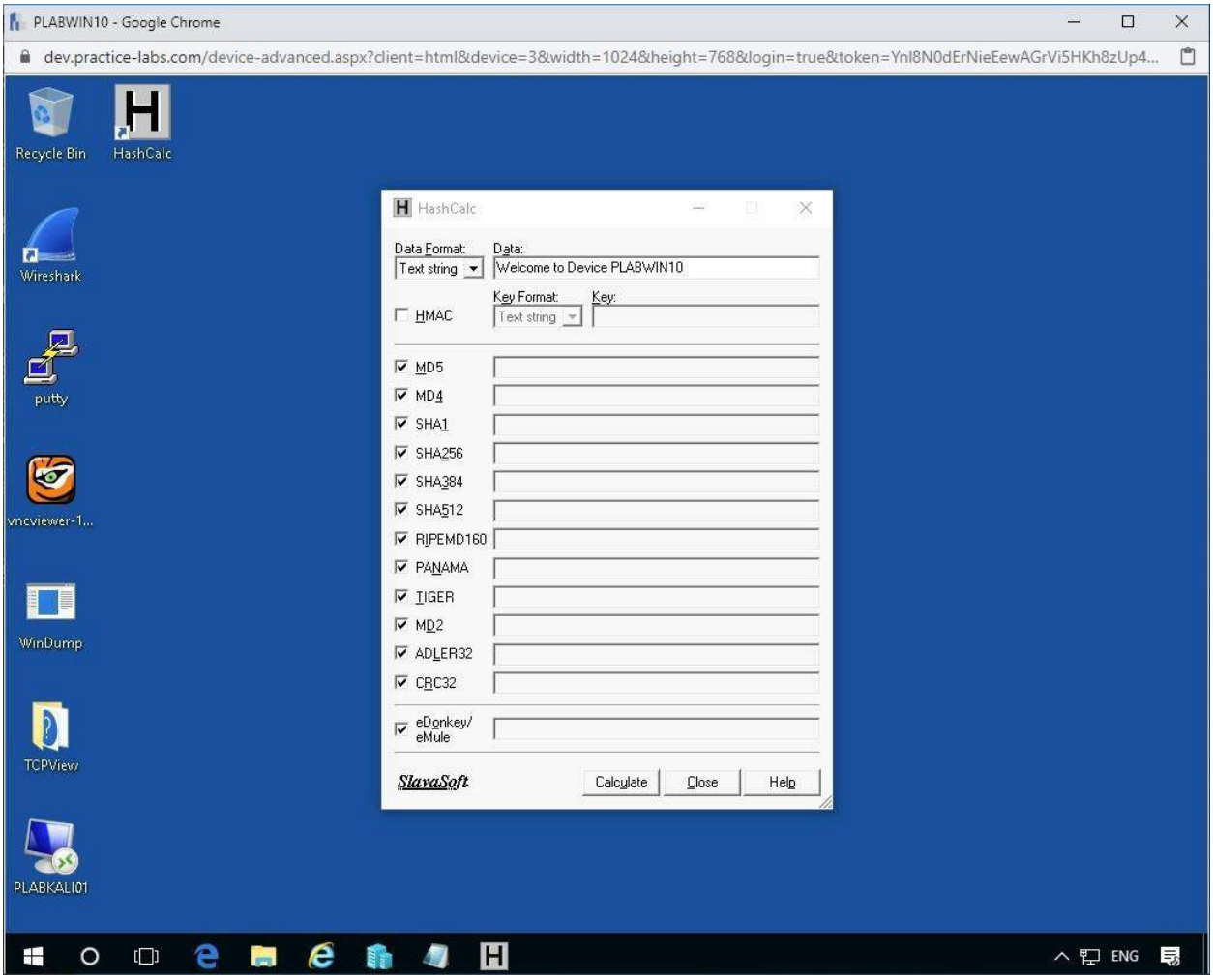


Figura 2.5. Captura de pantalla de PLABWIN10: interfaz Hashcalc

Haga clic en **Calcular** para ver sus resultados.

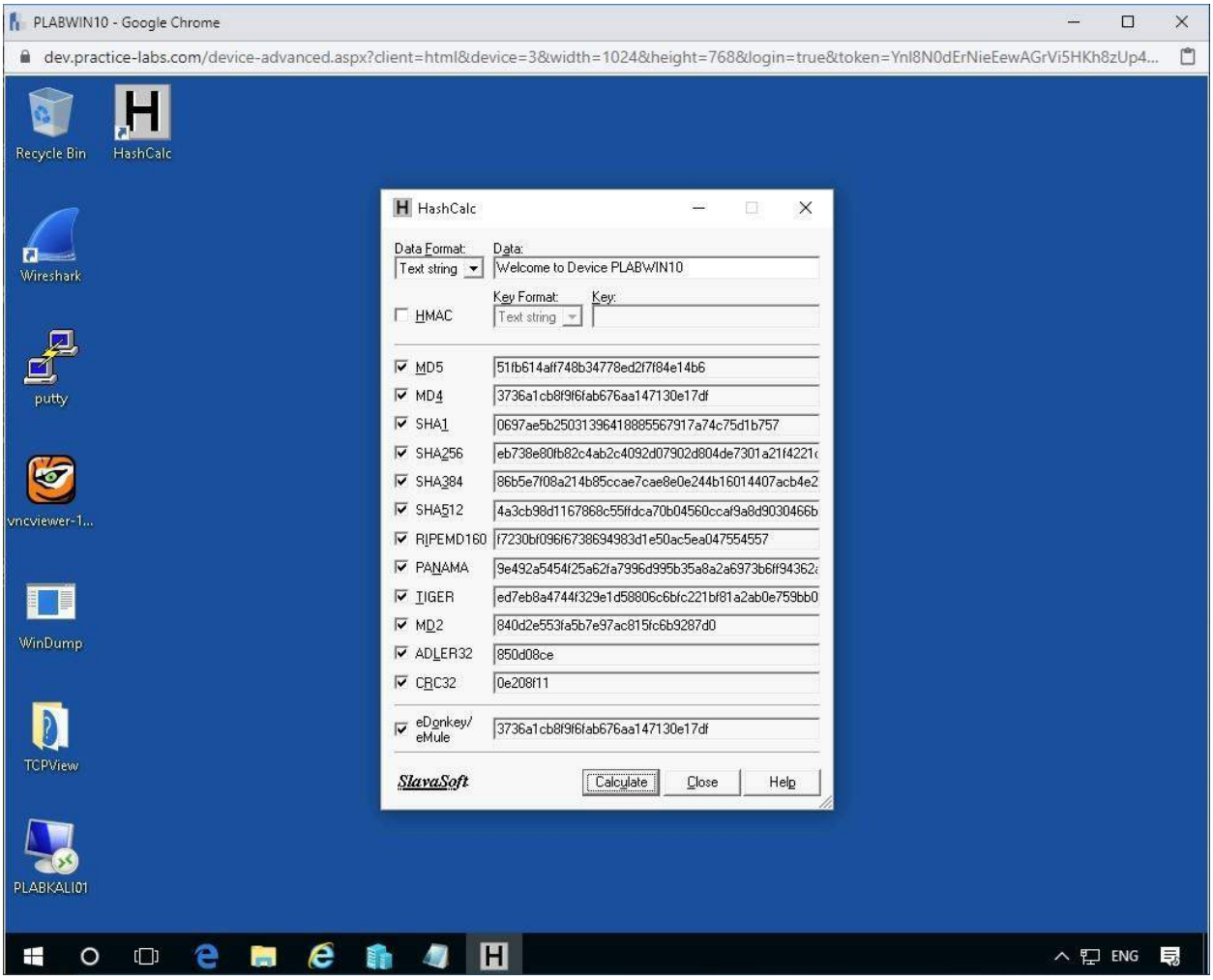


Figura 2.6. Captura de pantalla de PLABWIN10: resultados de Hashcalc

Cambie los **Datos** en el campo a lo que quiera y vea cómo los diferentes valores de Hashes se comparan entre sí. Notará que esencialmente los diferentes algoritmos producen hashes de longitudes establecidas que pueden usarse para identificarlos.

Paso 2

Ahora verifique el valor de HMAC y verá que solo se permitirá un número específico de tipos de Hash. Esto se debe a que un código de autenticación de mensaje hash con clave utiliza específicamente funciones hash.

Dentro del HMAC puede editar el **formato de clave** para permitir cadenas de texto o cadenas hexadecimales, usaremos cadenas de texto.

Para el **Valor clave** , ingrese la Clave de su elección o use la siguiente.

```
TidyMind
```

Nota: *Asegúrese de que todavía haya texto en el campo de datos.*

```
Welcome to Device PLABWIN10
```

Ahora presione el botón Calcular para ver sus resultados.

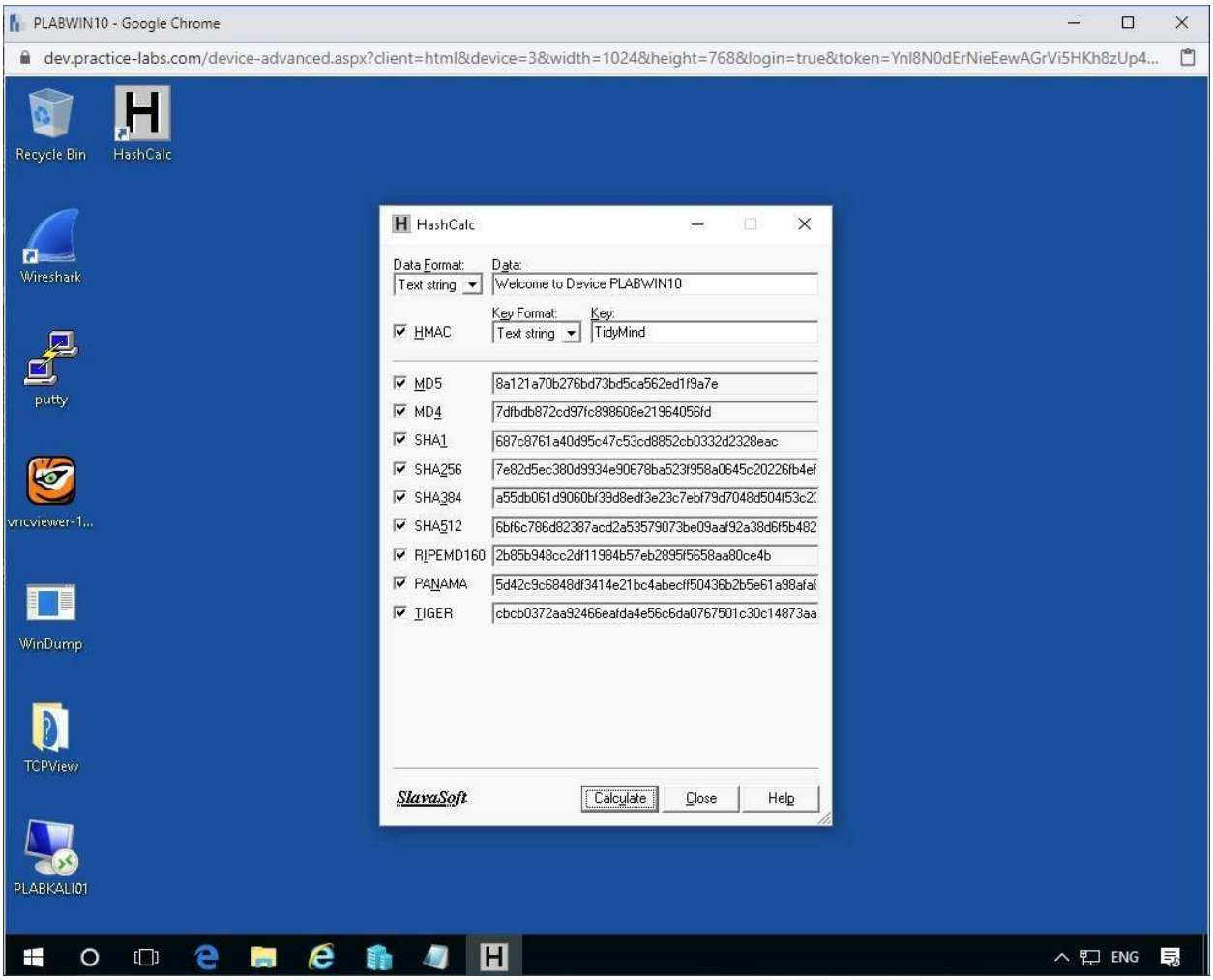


Figura 2.7. Captura de pantalla de PLABWIN10: resultados de Hashcalc

Recuerde que estos hashes se hicieron con la clave específica que se ingresó y, por lo general, esta sería una clave secreta.

Paso 3

Ahora puede cambiar el **formato de datos** a **cadena hexadecimal** y probarlo.

Aquí hay un valor hexadecimal para el color azul.

Escríbalo en el campo **Datos** , luego presione **Calcular** .

```
0000ff
```

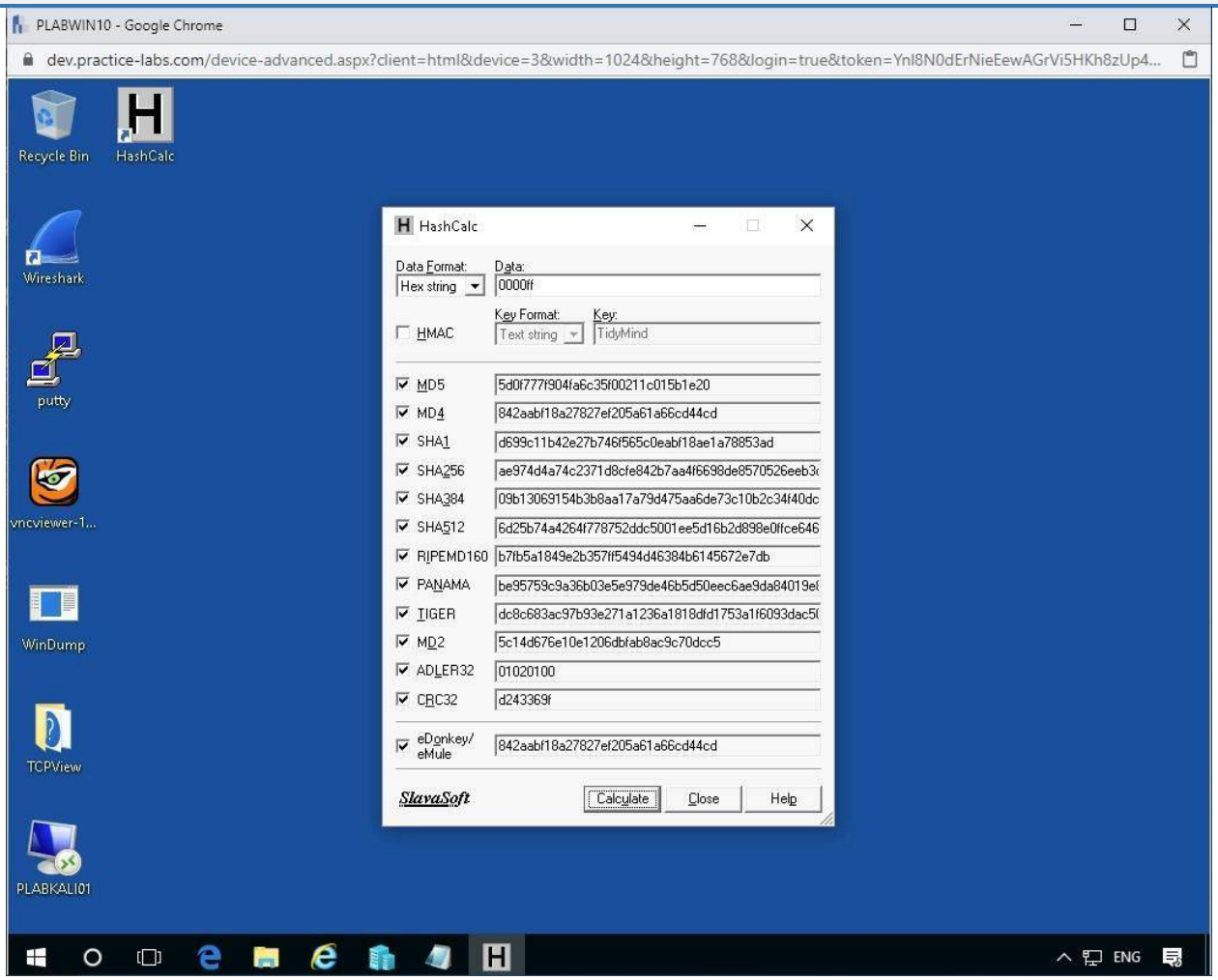


Figura 2.8. Captura de pantalla de PLABWIN10: resultados de Hashcalc con valor hexadecimal

Paso 4

Finalmente, cargaremos un archivo a Hashcalc para ser evaluado. En el **Formato de datos,** cambie el campo a **Archivo** .

En el **escritorio** hay un acceso directo llamado **Masilla** .

Cargaremos esto en el **Hashcalc** para ver qué valores se producen.

Haga clic en el icono "Examinar" que **aparece** como **puntos suspensivos:**

..

Luego navegue hasta el **Escritorio** para seleccionar **Putty.exe** .

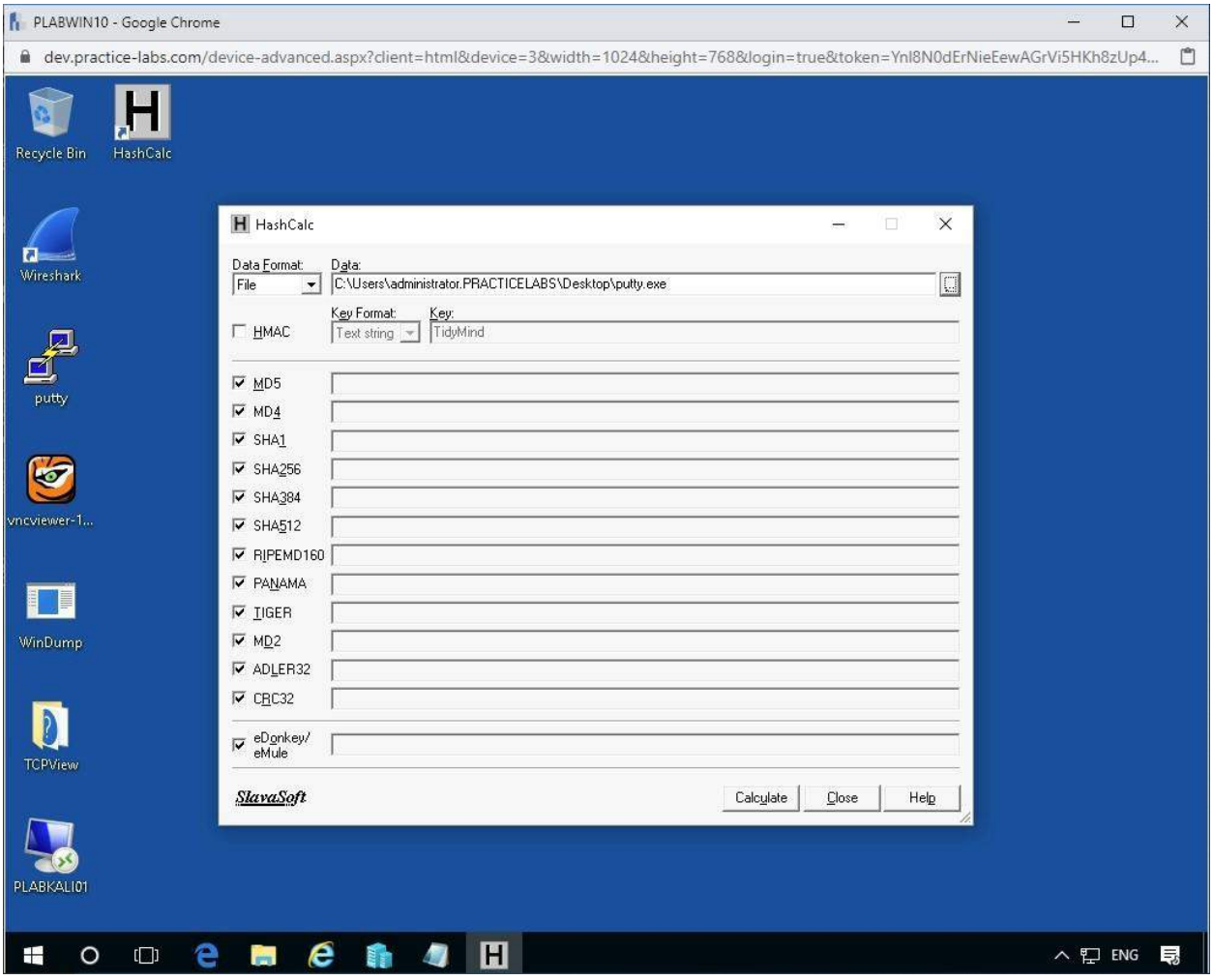


Figura 2.9. Captura de pantalla de PLABWIN10: Hashcalc con la ruta de masilla ingresada

Alerta: nuevamente asegúrese de que las casillas de verificación hayan sido marcadas, **EXCEPTO** para el **HMAC**

Una vez ingresado, presione el botón **Calcular** para ver los resultados del archivo hash.

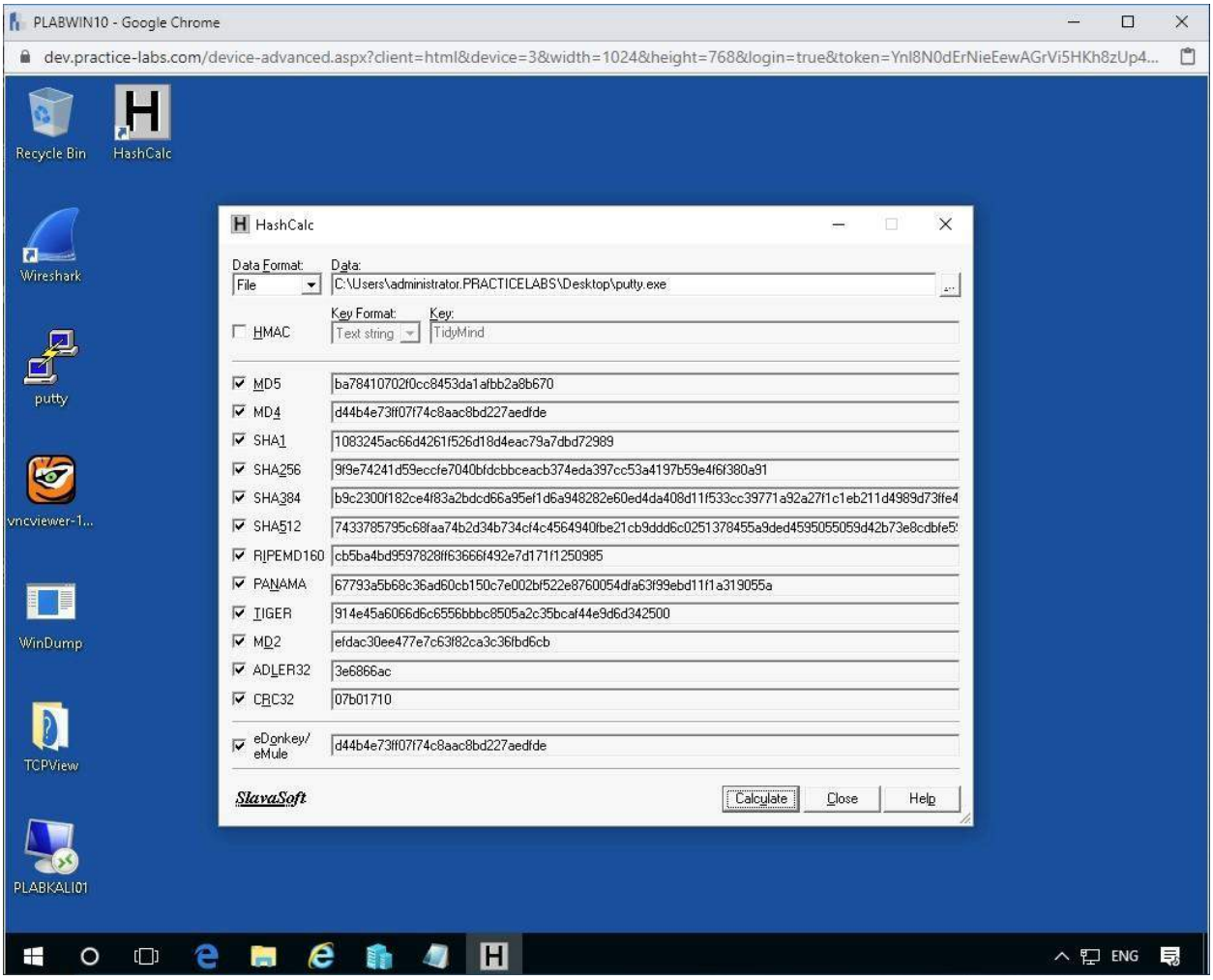


Figura 2.10. Captura de pantalla de PLABWIN10: Hashcalc con resultados de masilla

***Nota** : Utilizaremos estos cálculos hash en el próximo ejercicio.*

Ejercicio 3: comparación de valores hash

Aquí compararemos diferentes valores de hash y obtendremos una mejor comprensión de cómo los hash se comparan visualmente entre sí en ese estado.

En este ejercicio, aprenderá lo siguiente:

- Agarrando hashes del sitio web
- Usando una herramienta de comparación en línea

Nota: *Tenga en cuenta que durante este módulo se le pedirá que navegue a un sitio web externo. Los sitios web externos están sujetos a cambios; si observa que el contenido difiere del sitio web, infórmenos para que podamos actualizarlo.*

Para obtener información adicional sobre los valores de Hash, consulte el material del curso o utilice su motor de búsqueda favorito para investigar este tema con más detalle.

Tarea 1: agarrar valores de hash del sitio web

A menudo, cada sitio web tiene un valor Hash de los programas que ha creado. Estos valores están hechos por el autor, y podemos usarlos para confirmar la integridad de los programas o archivos para confirmar que son originales y no se alteran durante el tránsito.

Paso 1

Usando los valores Hash producidos por HashCalc, ahora los compararemos con los valores oficiales.

Esto se utiliza para asegurarse de que tengamos archivos que mantengan su integridad; ayuda a garantizar que los archivos no se hayan editado, agregado o cambiado en muchos sin notificación oficial.

En términos de programas, es un componente esencial para confirmar que no se ha inyectado código malicioso en Putty.exe.

Abra **Internet Explorer** y navegue a la URL oficial de descarga de masilla escribiendo:

```
https :// www . chiark . greenend . org . uk /~
sgtatham / putty / releases / 0 . 67 . html
```

Presione **Entrar** .

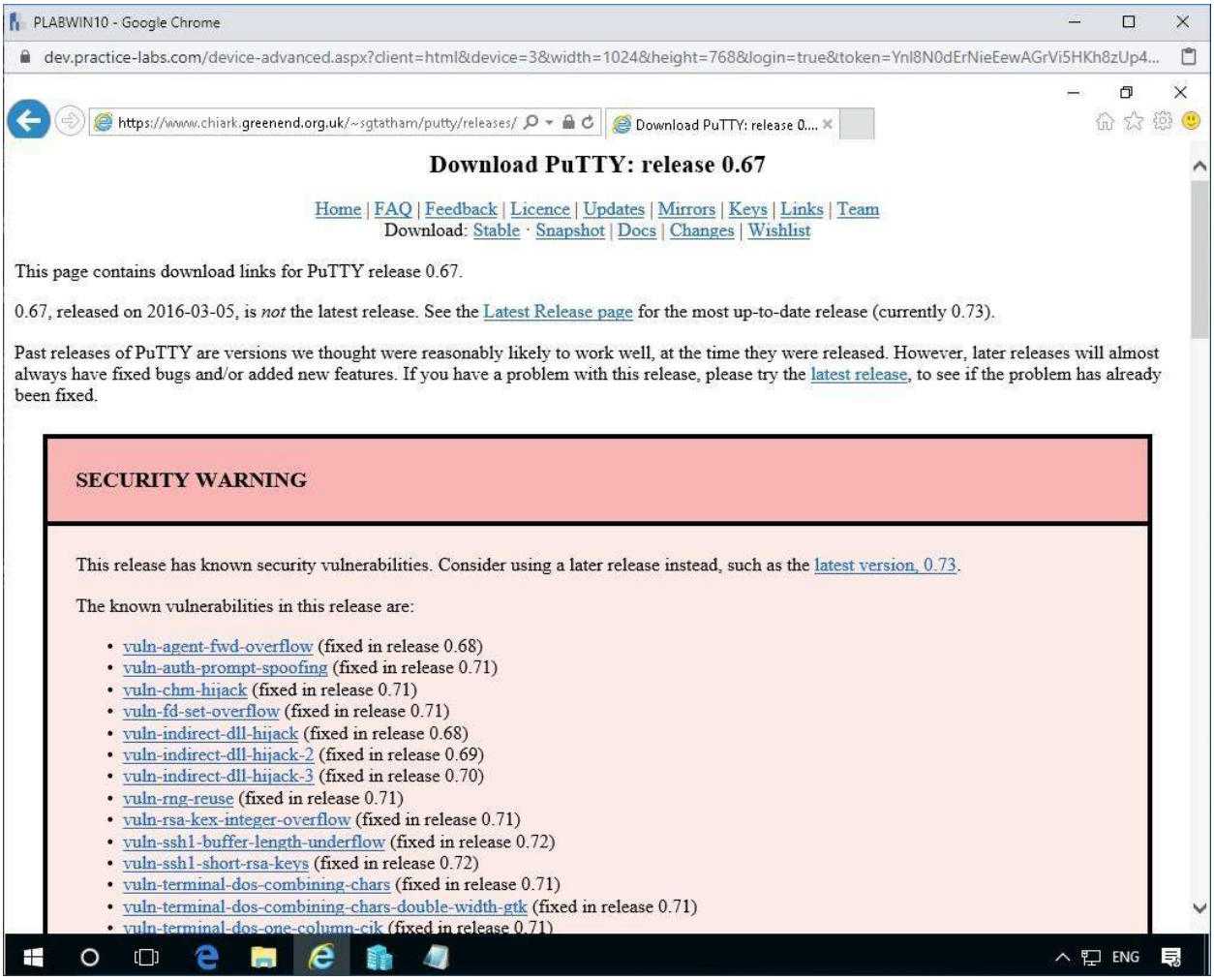


Figura 3.1. Captura de pantalla del sitio web de PLABWIN10: Putty

Una vez aquí, navegue a las **sumas** de **verificación** para todos los archivos anteriores.

Importante: Estamos usando Putty (beta 0.67)

Denotado por el
encabezado **Sumas de comprobación para todos los archivos anter iores**

Estamos buscando dos archivos para verificar

1. MD5
2. SHA-1

Haga clic en el enlace para **(o por FTP).**

Será recibido por una larga lista de Hash Sums para MD5.

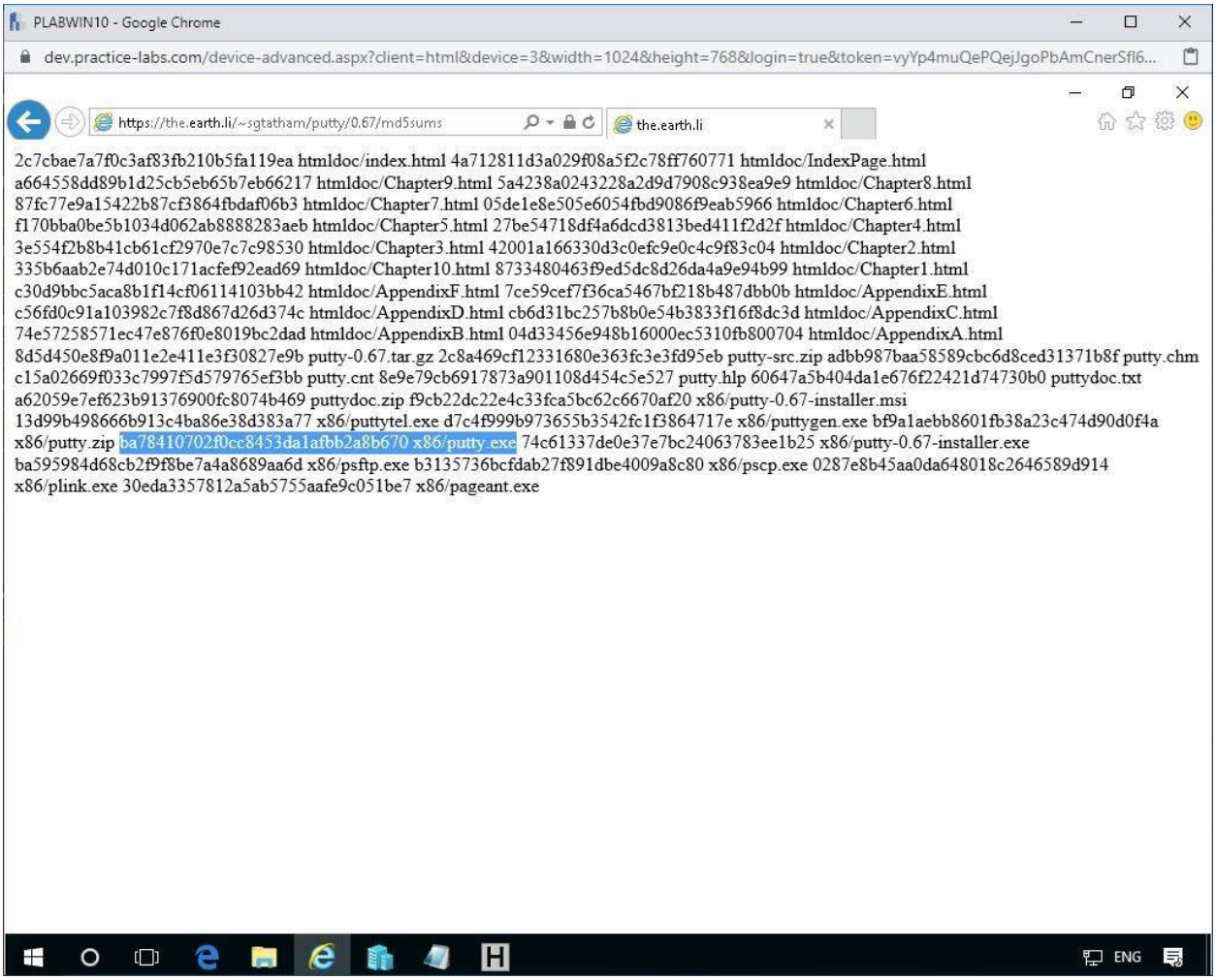


Figura 3.2. Captura de pantalla de PLABWIN10: Sumas hash MD5 de Putty

El md5sum para Putty.exe es:

```
ba78410702f0cc8453da1afbb2a8b670  x86/putty.exe
```

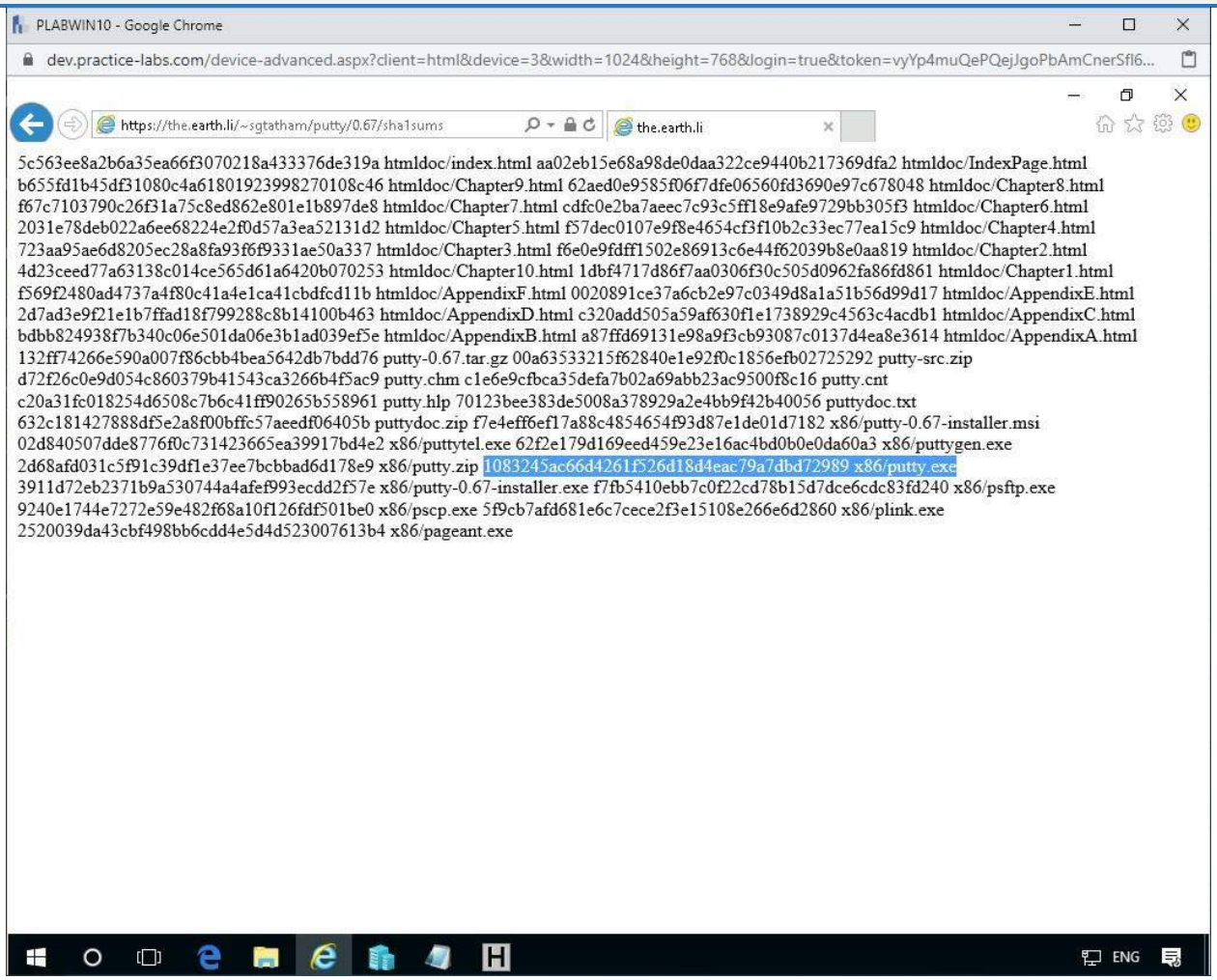


Figura 3.3. Captura de pantalla de PLABWIN10: sumas de hash de Putty SHA1

El sha1sum para Putty.exe es:

```
1083245ac66d4261f526d18d4eac79a7dbd72989
x86/putty.exe
```

Tarea 2: uso de la herramienta de comparación en línea

El sitio en línea ayuda a comparar valores entre sí para verificar si tenemos los mismos valores hash que el original.

Aquí usaremos esta herramienta en línea y la combinaremos con los resultados de HashCalc.

Paso 1

Abra otra pestaña en **Internet Explorer** y navegue a la siguiente página:

```
http://onlinemd5.com/
```

Presione **Entrar** .

Ahora compararemos los valores para el MD5 y el SHA1 que se encuentran en el sitio web con los valores generados por la **Calculadora de Hash** .

Alerta: asegúrese de que el botón de radio MD5 haya sido marcado en el sitio.

Paso 2

Usando el valor MD5 producido para Putty.exe, este valor debe copiarse en onlinemd5.com e ingresarse en el campo MD5 titulado:

```
File Checksum:
```

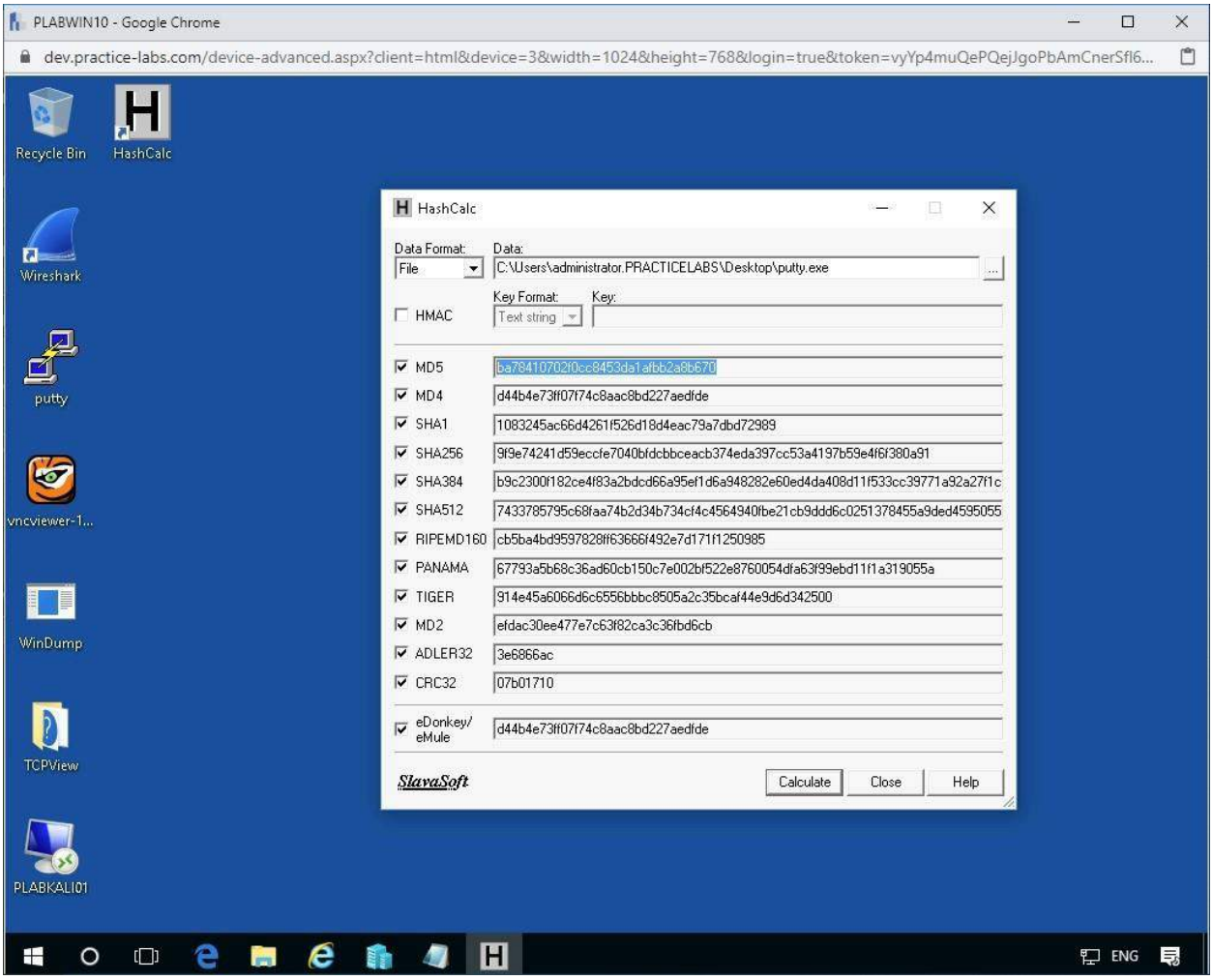


Figura 3.4. Captura de pantalla de PLABWIN10: copiando el valor de suma MD5.

Copie el valor del sitio web de masilla en la calculadora Onlinemd5 en el campo llamado:

```
Compare with:
```

Presione el botón **Comparar** .

Si es lo mismo, tenemos una aprobación de estos valores Hash y el archivo de datos es exactamente el mismo que el de los autores.

Paso 3

Ahora realice el mismo trabajo con el SHA1 copiando los valores SHA1 del Hashcalc y del sitio web de masilla en OnlineMD5.

Alerta: asegúrese de marcar el botón de radio SHA1.

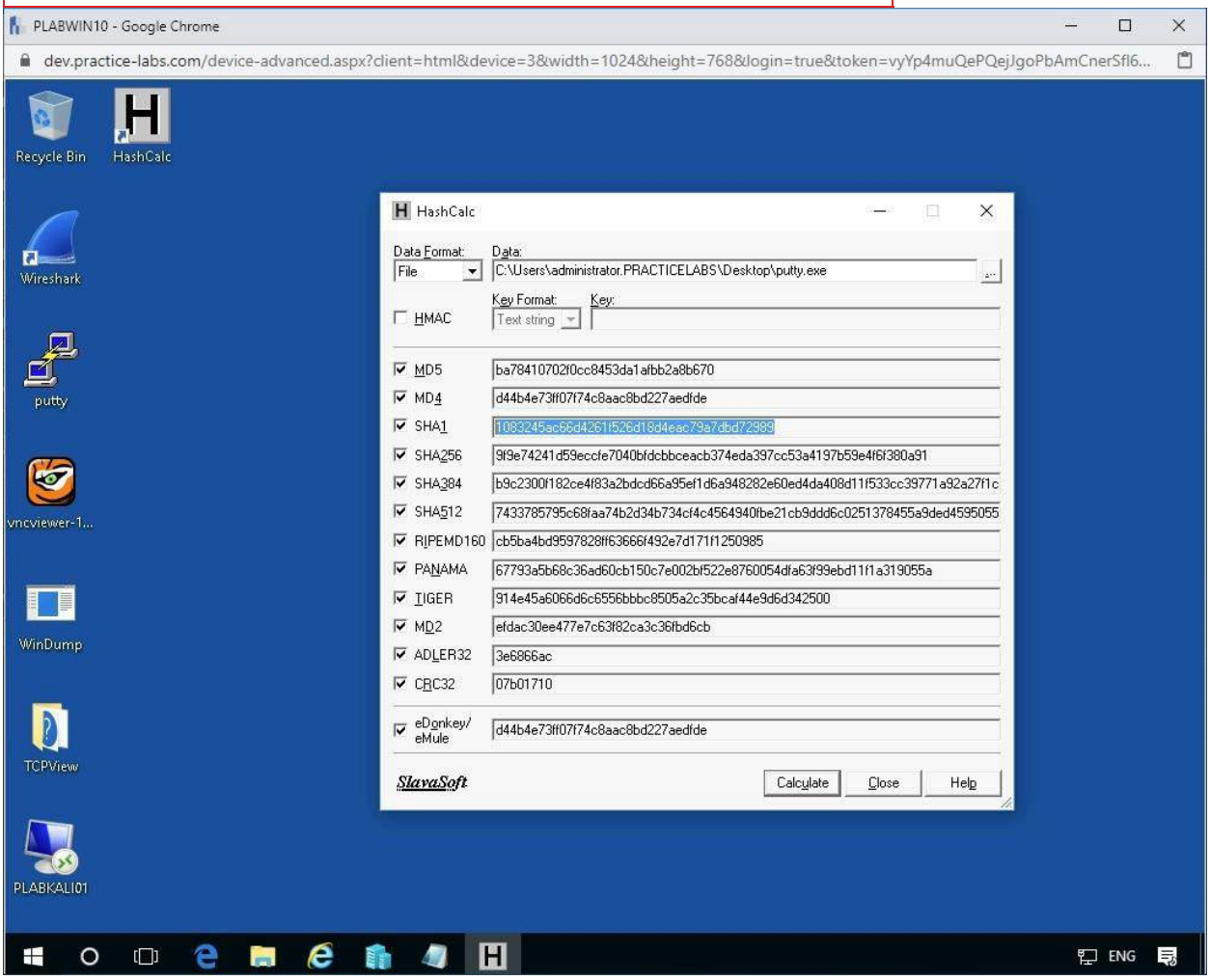


Figura 3.5. Captura de pantalla de PLABWIN10: copiando el valor SHA1.

Debería tener un resultado positivo de una aprobación de estos valores hash.

Si lo desea, puede continuar realizando una verificación adicional con SHA-256.

Resumen

Cubriste las siguientes actividades en este módulo:

- Fundamentos criptográficos
- Comparación de algoritmos hash
- Comparación de valores hash