

1. Organizar grupos de 3.
2. Desarrollar una presentación en IA Presenter, con los dos últimos laboratorios que les envié y un análisis sobre este artículo

(<https://cybersecurityventures.com/ransomware-report-2021/>)

3. Subir la presentación a GitHub y enviarme el enlace.

Nombres: Jairo Rolando Acuña Lancheros.

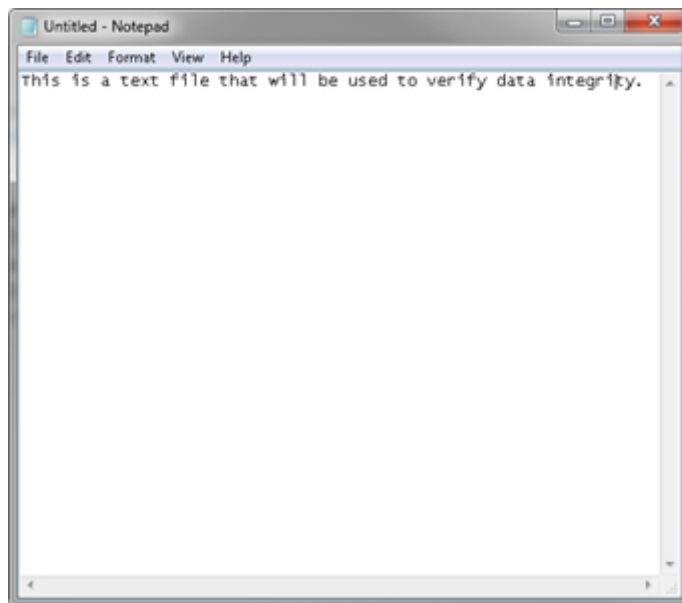
Juan David Luna Suárez.

Edier Leonardo González Vera.

Carlos Alberto Romero.

Práctica de laboratorio: Comparar datos con un hash Paso 1: Crear un archivo de texto

-
- a. Busque en su equipo el programa Bloc de notas y ábralo.
 - b. Escriba algún texto en el programa.



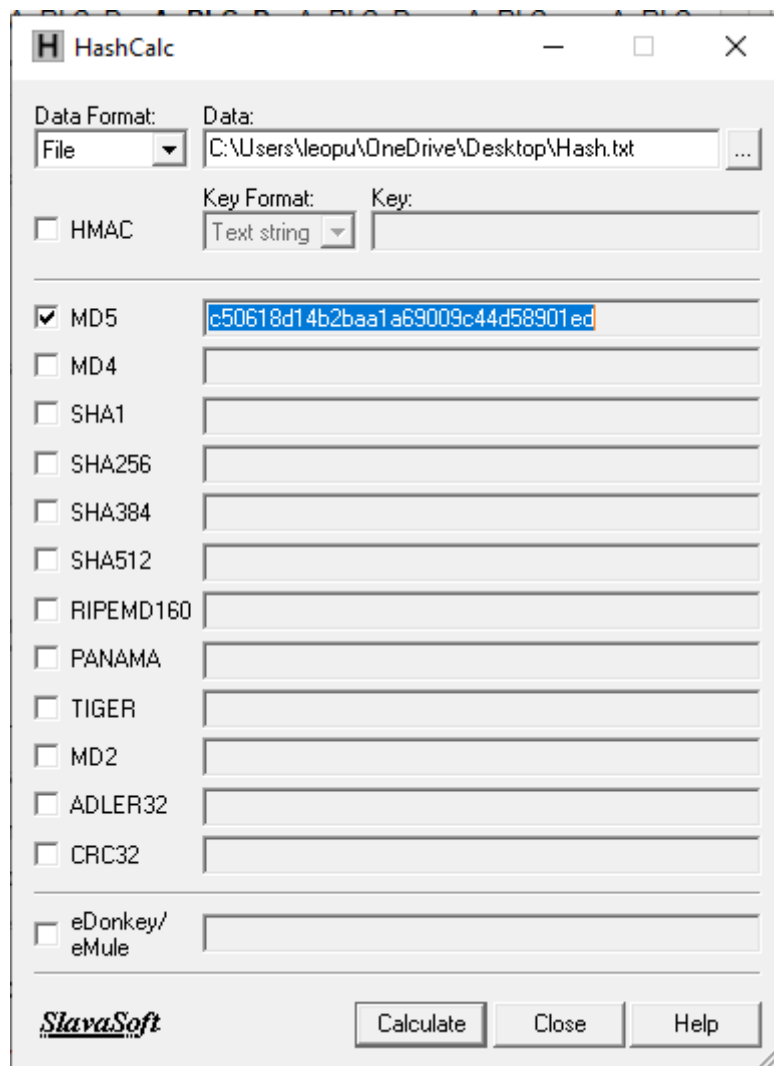
- c. Elija Archivo > Guardar.
- d. Navegue hasta Escritorio.
- e. Escriba Hash en el campo Nombre de archivo: y haga clic en Guardar.

Paso 2: Instalar HashCalc

a. Abra un navegador web y vaya a <http://www.slavasoft.com/download.htm>. !
[Descripción de la imagen](/img/imagen2.png) b. Haga clic en Descargar en la fila HashCalc 2.02. c. Abra el archivo hashcalc.zip y ejecute el archivo setup.exe que está en su interior. ![Descripción de la imagen](/img/imagen3.png) d. Siga el asistente de instalación para instalar HashCalc. e. Haga clic en Finalizar en la última pantalla y cierre el archivo README si está abierto. Puede leer el archivo, si lo desea. f. HashCalc ahora está instalado y en funcionamiento. ![Descripción de la imagen](/img/imagen4.png) Paso 3: Calcular un hash del archivo Hash.txt

a. Establezca los siguientes elementos en HashCalc: 1) Formato de los datos: Archivo. 2) Datos: haga clic en el botón ... que está junto al campo Datos, navegue hasta el Escritorio y elija el archivo Hash.txt. 3) Quite la selección de HMAC. 4) Quite la selección de todos los tipos de hash, excepto MD5.

b. Haga clic en el botón Calcular. ¿Cuál es el valor junto a MD5?
c50618d14b2baa1a69009c44d58901ed



Paso 4: Haga un cambio en el archivo Hash.txt a. Navegue hasta el Escritorio y abra el archivo Hash.txt. b. Realice un cambio menor en el texto, como eliminar una letra, o agregar un espacio o un punto. c. Haga clic en Archivo > Guardar y cierre el Bloc de notas.

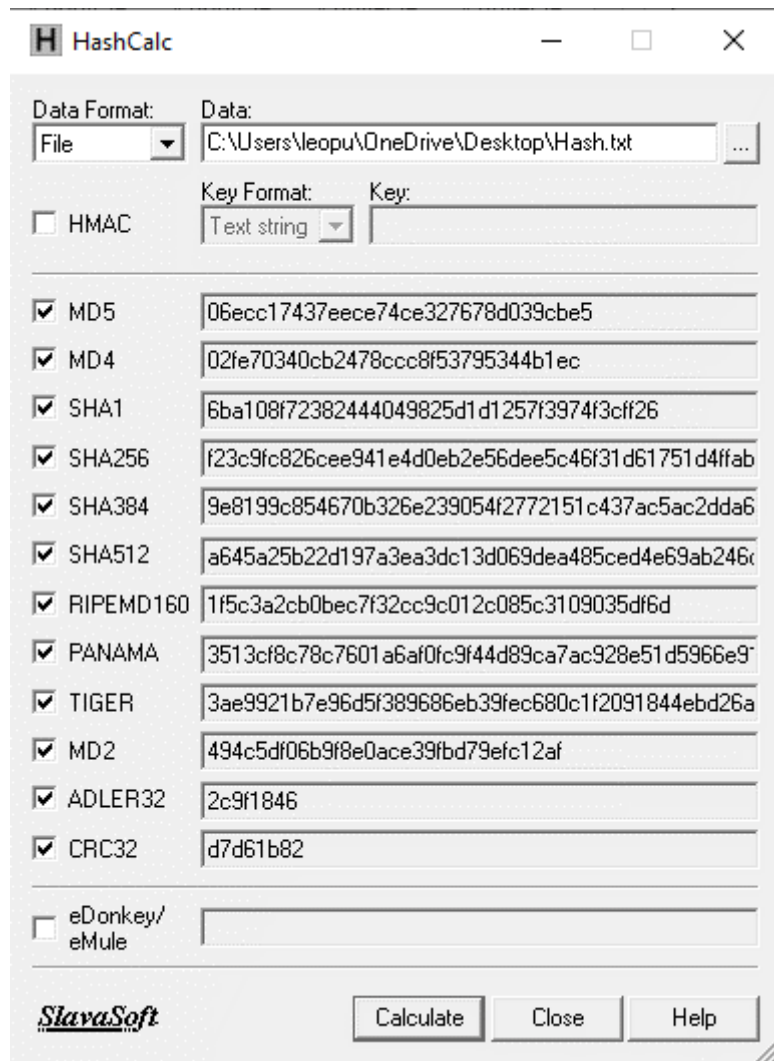
Paso 5: Calcule un nuevo hash del archivo Hash.txt a. Haga clic en el botón Calcular en HashCalc nuevamente. ¿Cuál es el valor junto a MD5?

06ecc17437eece74ce327678d039cbe5 ![Descripción de la imagen]

(/img/imagen6.png) ¿El valor es diferente del valor registrado en el paso 3?

Si, el valor del hash code ha cambiado b. Coloque una marca junto a todos los tipos de hash. c. Haga clic en Calcular. d. Fíjese cómo muchos de los tipos de hash crean un hash de longitud diferente. ¿Por qué? Cada decodificación usa diferentes

métodos de encriptacion Cada uno tiene su propio algoritmo de encriptamiento y por eso el resultado con cada uno es diferente



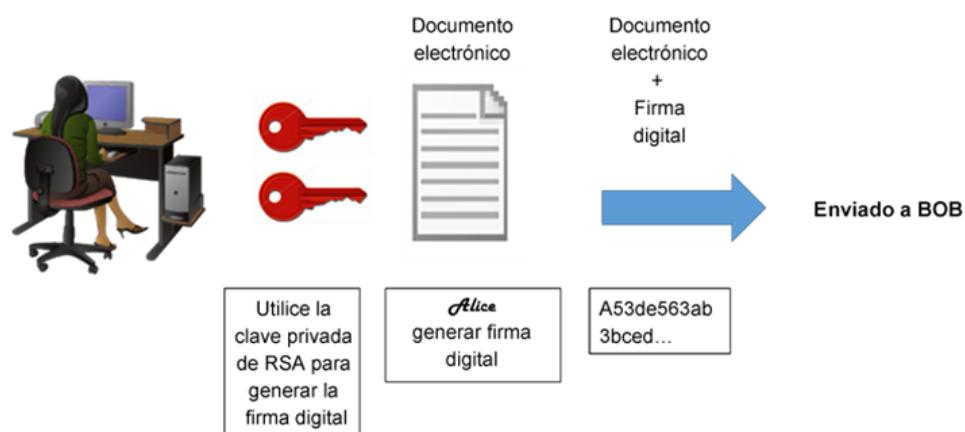
Práctica de laboratorio: uso de firmas digitales Parte 1: Uso de firmas digitales En esta parte, utilizará una página web para verificar la firma de un documento entre Alice y Bob. Alice y Bob comparten un par de claves RSA privadas y públicas. Cada uno de ellos usa la clave privada para firmar un documento jurídico. Luego se envían los documentos entre sí. Alice y Bob pueden verificar la firma de cada uno con la clave pública. También deben acordar un exponente público compartido para el cálculo.

Clave RSA pública

d94d889e88853dd89769a18015a0a2e6bf82b
f356fe14f251fb4f5e2df0d9f9a94a68a30c428b

	39e3362fb3779a497eacea37100f264d7fb9f b1a97fbf621133de55fdbcb9b1ad0d7a31b3792 16d79252f5c527b9bc63d83d4ecf4d1d45cbf8 43e8474bab6c655e9bb6799cba77a47eafa838 296474afc24beb9c825b73ebf549
Clave RSA pública	47b9cfde843176b88741d68cf096952e95081 3151058ce46f2b048791a26e507a1095793c1 2bae1e09d82213ad9326928cf7c2350acb19c 98f19d32d577d666cd7bb8b2b5ba629d25ccf 72a5ceb8a8da038906c84dcd1fe677dffb2c0 29fd8926318eede1b58272af22bda5c5232be 066839398e42f5352df58848adad11a1
Exponente público	10001

Paso 1: Firme el documento Alice firma un documento jurídico y lo envía a Bob mediante las claves públicas y privadas RSA que se muestran en la tabla anterior. Ahora Bob tendrá que verificar la firma digital de Alice para confiar en la autenticidad de los documentos electrónicos.



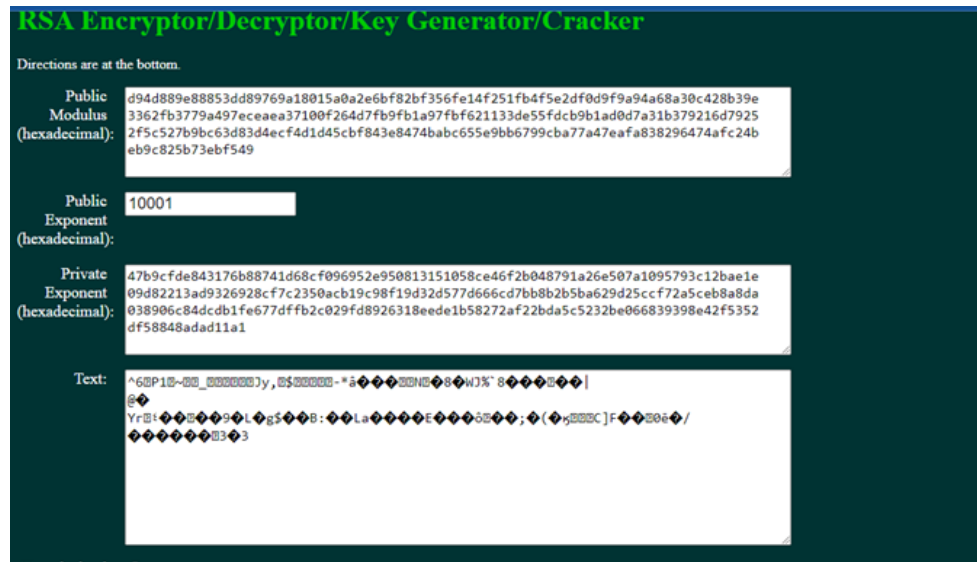
Paso 2: Verifique la firma digital. Bob recibe el documento con una firma digital que se muestra en la siguiente tabla. Tabla

Firma de Alice	0xc8 0x93 0xa9 0x0d 0x8f 0x4e 0xc5 0xc3 0x64 0xec 0x86 0x9d 0x2b 0x2e 0xc9 0x21 0xe3 0x8b 0xab 0x23 0x4a 0x4f 0x45 0xe8 0x96 0x9b 0x98 0xbe 0x25 0x41 0x15 0x9e 0xab 0x6a 0xfb 0x75 0x9a 0x13 0xb6 0x26 0x04 0xc0 0x60 0x72 0x28 0x1a 0x73 0x45 0x71 0x42 0x83 0xd4 0x7f 0x57 0xd1 0xac 0x91 0x8c 0xae 0x2f 0x3b 0xd2 0x99 0x30 0x3e 0xe8 0xa8 0x3a 0xb3 0x5d 0xfb 0x4a 0xc9 0x18 0x19 0xfd 0x3f 0x0c 0x0a 0x1f 0x3d 0xa4 0xa4 0xfe 0x02 0x9d 0x96 0x2f 0x50 0x34 0xd3 0x95 0x55 0xe0 0xb7 0x2a 0x46
-----------------------	---

0xa4 0x9e 0xae 0x80 0xc9 0x77 0x43 0x16
 0xc0 0xab 0xfd 0xdc 0x88 0x95 0x05 0x56
 0xdf 0xc4 0xfc 0x13 0xa6 0x48 0xa3 0x3c 0xe2
 0x87 0x52 0xc5 0x3f 0x0c 0x0d

![[Descripción de la imagen]](/img/imagen9.png)

a. Copie y pegue las claves públicas y privadas de la Tabla 1 arriba en los cuadros Módulo público y Exponente privado en el sitio web, como se muestra en la imagen anterior. b. Asegúrese de que el Exponente público sea 10001. c. Pegue la firma digital de Alice de la Tabla 2 en el cuadro llamado Texto de la página web, como se muestra arriba. d. Ahora BOB puede verificar la firma digital al hacer clic en el botón Verificar cerca del centro de la parte inferior de la página web. ¿Qué firma se identifica?



Paso 3: Generar una firma de respuesta. Bob recibe y verifica el documento electrónico y la firma digital de Alice. Ahora Bob crea un documento electrónico y genera su propia firma digital con la clave RSA privada de la Tabla 1. (Nota: el nombre de Bob aparece en letras mayúsculas).

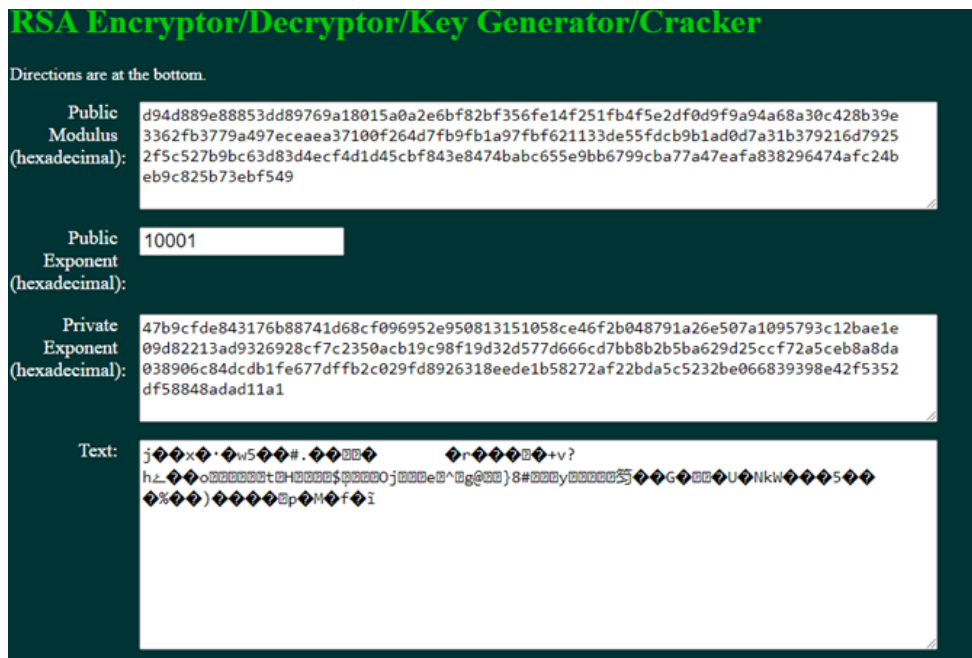
Firma de Bob

0x92 0x13 0xeb 0xcd 0x4b 0xe8 0x60 0xb4
 0x85 0xb6 0xc6 0xda 0xe4 0xf7 0x5c 0xc8
 0x0e 0xe4 0xdc 0x3c 0x18 0x8f 0x21 0xf1
 0xaa 0x10 0xc5 0x56 0xa6 0xa5 0x11 0xd0
 0x19 0xb4 0xac 0x75 0x29 0x67 0x05 0x9e
 0xef 0x97 0x16 0xa8 0x94 0x10 0x11 0x6e
 0x74 0x41 0xac 0xeb 0x51 0x35 0xfd 0x7e
 0xae 0x29 0x96 0x7d 0x9c 0x40 0x9b 0xc0
 0x1a 0x02 0x74 0x1c 0xcc 0x05 0xf8 0x76
 0xb1 0x69 0xe9 0xb0 0x07 0xa6 0x4d 0x1d
 0x2e 0x9c 0x95 0xf8 0xd4 0x7e 0xcb 0x3c

0x32 0xe7 0xf0 0x43 0x48 0xf2 0x69 0xef 0xfd
 0x89 0x7e 0x2c 0xe8 0xfa 0xd2 0x94 0xc7
 0x2a 0xed 0x7f 0xbf 0xfc 0x74 0xdd 0xa3 0x18
 0x37 0xf9 0x51 0x0a 0x2e 0x4b 0x09 0xac
 0x61 0xf3 0xe1 0x66 0xe0 0x86

Bob envía el documento electrónico y la firma digital a Alice.

Paso 4: Verifique la firma digital. a. Copie y pegue las claves públicas y privadas de la Tabla 1 arriba en los cuadros Módulo público y Exponente privado en el sitio web, como se muestra en la imagen anterior. b. Asegúrese de que el Exponente público sea 10001. c. Pegue la firma digital de Bob de la Tabla 4 en el cuadro llamado Texto de la página web, como se muestra arriba. d. Ahora Alice puede verificar la firma digital al hacer clic en el botón Verificar cerca del centro de la parte inferior de la página web. ¿Qué firma se identifica?



RSA Encryptor/Decryptor/Key Generator/Cracker

Directions are at the bottom.

Public Modulus (hexadecimal): d94d889e88853dd89769a18015a0a2e6bf82bf356fe14f251fb4f5e2df0d9f9a94a68a30c428b39e3362fb3779a497ecea37100f264d7fb9fb1a97fbf621133de55fdbc9b1ad0d7a31b379216d79252f5c527b9bc63d83d4ecf4d1d45cbf843e8474bab655e9bb6799cba77a47eafa838296474afc24beb9c825b73ebf549

Public Exponent (hexadecimal): 10001

Private Exponent (hexadecimal): 47b9cfde843176b88741d68cf096952e950813151058ce46f2b048791a26e507a1095793c12bae1e09d82213ad9326928cf7c2350acb19c98f19d32d577d666cd7bb8b2b5ba629d25ccf72a5ceb8a8da038906c84dcb1fe677dff2c029fd8926318eede1b58272af22bda5c5232be066839398e42f5352df58848adad11a1

Text: j...x...w5...#...+v?
 h...o...t...H...\$...j...e...^...g...}...8...y...5...G...U...Nkw...5...
 ...p...H...f...i

Parte 2: Cree su propia firma digital Ahora que ve cómo funcionan las firmas digitales, puede crear su propia firma digital. Paso 1: Generar un nuevo par de claves RSA. Vaya a la herramienta del sitio web y genere un nuevo conjunto de claves públicas y privadas RSA. a. Borre el contenido de los cuadros llamados Módulo público, Módulo privado y Texto. Solo use el mouse para resaltar el texto y presione la tecla Eliminar en su teclado. b. Asegúrese de que la casilla “Exponente público” tenga 10001. c. Genere un nuevo conjunto de claves RSA haciendo clic en el botón Generar cerca del extremo inferior derecho de la página web.

RSA Encryptor/Decryptor/Key Generator/Cracker

Directions are at the bottom.

Public
Modulus
(hexadecimal):

a6971851ef3b1f42ceb7d1268ca67f0f3a18b114fdd99994eae06ab96b351c9c40f9fafdbb78388a
dcfe9236f63ecf302364c18d0af094fef0ca964cea844b9946dfb35380535e55f14aade3bf91c0c7
673ce6c6d61c9d12d1cb5408b34ae45e1d85aca6d3658f1475f45cd7caa6eeefc78394c78dec12a
237d2595ac2b7869

Public
Exponent
(hexadecimal):

10001

Private
Exponent
(hexadecimal):

a53859907979e38938c82a10d7921196228276ae610dbd3a6ab06468bd211dd0ebc5ee7e3545a8f
ae9a749d3a201510a329bca48be30b82c581c70b45d42bbc9f9c68f61c4a54dc450ae128641d4dd3
e24bd8197ed792725e3b44e81b4c2448d6ab00e87977e9ff82de2667a8572da6d273e9490fc611e
d727210a93fd1761

Text:

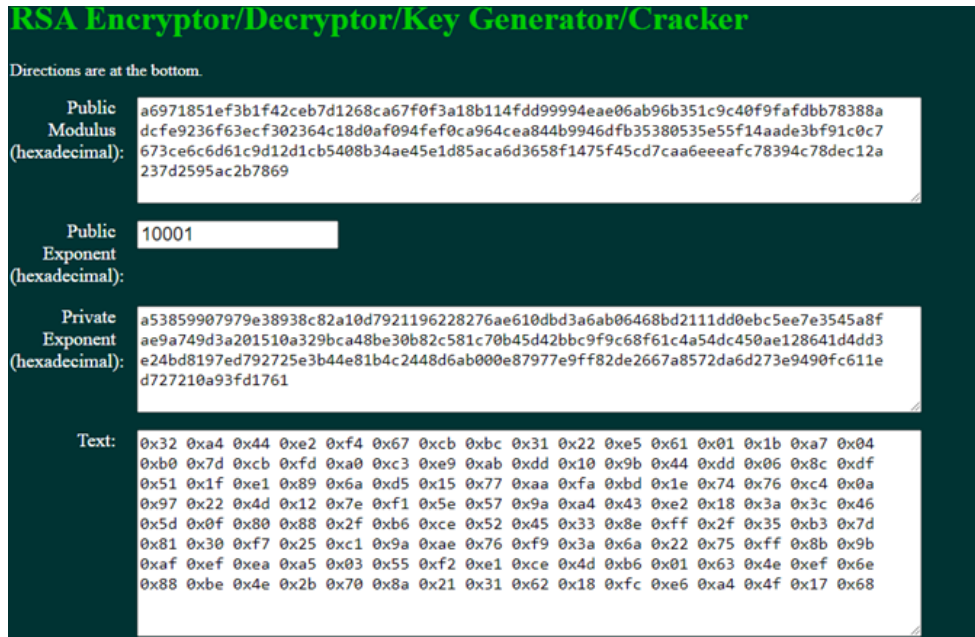
d. Copie las nuevas claves en la Tabla 5.

Clave pública	a6971851ef3b1f42ceb7d1268ca67f0f3a18b1 14fdd99994eae06ab96b351c9c40f9fafdbb78 388adcfe9236f63ecf302364c18d0af094fef0ca 964cea844b9946dfb35380535e55f14aade3bf 91c0c7 673ce6c6d61c9d12d1cb5408b34ae45e1d85a ca6d3658f1475f45cd7caa6eeefc78394c78de c12a237d2595ac2b7869
Clave privada	a53859907979e38938c82a10d79211962282 76ae610dbd3a6ab06468bd211dd0ebc5ee7e 3545a8fae9a749d3a201510a329bca48be30b 82c581c70b45d42bbc9f9c68f61c4a54dc450a e128641d4dd3 e24bd8197ed792725e3b44e81b4c2448d6ab 000e87977e9ff82de2667a8572da6d273e949 0fc611ed727210a93fd1761

e. Ahora escriba su nombre completo en el cuadro llamado Texto y haga clic en Firmar.

Firma digital personal	0x32 0xa4 0x44 0xe2 0xf4 0x67 0xcb 0xbc 0x31 0x22 0xe5 0x61 0x01 0x1b 0xa7 0x04 0xb0 0x7d 0xcb 0xfd 0xa0 0xc3 0xe9 0xab 0xdd 0x10 0x9b 0x44 0xdd 0x06 0x8c 0xdf 0x51 0x1f 0xe1 0x89 0x6a 0xd5 0x15 0x77 0xaa 0xfa 0xbd 0x1e 0x74 0x76 0xc4 0x0a 0x97 0x22 0x4d 0x12 0x7e 0xf1 0x5e 0x57 0x9a 0xa4 0x43 0xe2 0x18 0x3a 0x3c 0x46
-------------------------------	--

0x5d 0x0f 0x80 0x88 0x2f 0xb6 0xce 0x52
 0x45 0x33 0x8e 0xff 0x2f 0x35 0xb3 0x7d
 0x81 0x30 0xf7 0x25 0xc1 0x9a 0xae 0x76
 0xf9 0x3a 0x6a 0x22 0x75 0xff 0x8b 0x9b 0xaf
 0xef 0xea 0xa5 0x03 0x55 0xf2 0xe1 0xce 0x4d
 0xb6 0x01 0x63 0x4e 0xef 0x6e 0x88 0xbe
 0x4e 0x2b 0x70 0x8a 0x21 0x31 0x62 0x18
 0xfc 0xe6 0xa4 0x4f 0x17 0x6



Parte 3: Intercambie y verifique las firmas digitales Ahora puede utilizar esta firma digital. Paso 1: Intercambie sus nuevas claves públicas y privadas en la Tabla 5 con su compañero. a. Registre las claves RSA públicas y privadas de su compañero en la Tabla 5. b. Registre ambas claves en la siguiente tabla.

Clave pública	bb465b62e54b58f248dde7359c5cf0f77ce5ccf ae57b09abc5f731329480e786da85ca1cb090 afed 18337c5af665352b49f1909b59661af2d566fc 81dd464d0549079a32f61f1e8bfc64c84cb957 8c40 82e68e6c99bf4caff4f0800ffa9db1240d06206 3bbac374d8180a4ebfe9cf4906873490b1be7 dcf8 285276877e8090e1
Clave privada	7861f1bcd0c86e94d062548e11c56ce0aa58c e3b39e8ad7ecdfe89d2af8f1dbadfcf2bf1e80e 395 f548a35795abd951ca668e1e4e8964295524a e8c8c40f4a0a7781e22349a7ce0187dd2edadcc

22fdb
 846aa61637c397fa886b6803877be941c6e72
 1382e56ed9431f16da9ba04f2a469996559fb0
 cc806 0fbe18415048eb01

RSA Encryptor/Decryptor/Key Generator/Cracker

Directions are at the bottom.

Public Modulus (hexadecimal):	bb465b62e54b58f248dde7359c5cf0f77ce5ccfae57b09abc5f731329480e786da85ca1cb090afed18337c5af665352b49f1909b59661af2d566fc81dd464d0549079a32f61f1e8bfc64c84cb9578c4082e68e6c99bf4cafff4f080ffa9db1240d062063bbac374d8180a4ebfe9cf4906873490b1be7dcf8285276877e8090e1
Public Exponent (hexadecimal):	10001
Private Exponent (hexadecimal):	7861f1bcd0c86e94d062548e11c56ce0aa58ce3b39e8ad7ecdf2e89d2af8f1dbadfcf2bf1e80e395f548a35795abd951ca668e1e4e8964295524ae8c8c40f4a0a7781e22349a7ce0187dd2edadc22fdb846aa61637c397fa886b6803877be941c6e721382e56ed9431f16da9ba04f2a469996559fb0cc8060fbe18415048eb01
Text:	Juan David Luna Suarez

Hexadecimal ☒

Character String ☐

Encrypt	Sign
Decrypt	Verify
Generate	Crack

Firma digital personal

0xb3 0x88 0x19 0xfe 0x48 0xd3 0xf5 0x75
 0x9e 0xe7 0xa7 0xdd 0xd9 0xfa 0xac 0xb4 0xf2
 0x96 0x3d 0x27 0xca 0x1c 0x32 0x69 0x75
 0xf9 0xd1 0x3d 0xb5 0x6c 0xc1 0x28 0xc5
 0x0f 0xf5 0x50 0xc9 0xca 0x7a 0xf9 0xa4 0x9a
 0xeb 0x93 0x9e 0x8a 0x6d 0xcf 0x48 0x3d
 0x1e 0xde 0x65 0x8d 0xc0 0xe3 0xb5 0x2b
 0x78 0x7b 0xd1 0x67 0xa9 0x99 0x6d 0xd4
 0x0d 0xf1 0x5c 0xb5 0x9f 0x6e 0xbb 0xfd 0x2e
 0xe5 0xe9 0xa8 0x0c 0x74 0xa0 0x7e 0xf6
 0x8a 0xf6 0x11 0x69 0x1e 0xf1 0x87 0xbf 0xc8
 0x12 0xf4 0x48 0x0a 0x11 0xff 0x70 0xcd
 0x43 0x8e 0xd2 0x06 0xd6 0xea 0xb0 0xb3
 0xd0 0xae 0x76 0x3a 0x15 0xdd 0x4e 0xc7
 0x63 0x2a 0x07 0xdd 0xd5 0x12 0x22 0x16
 0x84 0xa6 0x99 0xaf

Firma digital del compañero

Paso 2: Verifique la firma digital de sus compañeros a. Para verificar la firma digital de su compañero, pegue las claves públicas y privadas en los cuadros correspondientes llamados Módulos públicos y privados en la página web. b. Ahora pegue la firma digital en el cuadro llamado Texto. c. Ahora verifique su firma digital al hacer clic en el botón Verificar. d. ¿Qué aparece en el cuadro llamado Texto?

The screenshot shows a web application titled "RSA Encryptor/Decryptor/Key Generator/Cracker" with a dark green background. The interface includes several input fields and buttons:

- Public Modulus (hexadecimal):** A large text area containing a long hexadecimal string.
- Public Exponent (hexadecimal):** A text input field containing the value "10001".
- Private Exponent (hexadecimal):** A large text area containing a long hexadecimal string.
- Text:** A text input field containing a hexadecimal string: "0x4a 0x75 0x61 0x6e 0x20 0x44 0x61 0x76 0x69 0x64 0x20 0x4c 0x75 0x6e 0x61 0x20 0x53 0x75 0x61 0x72 0x65 0x7a".
- Hexadecimal** and **Character String** radio buttons are present, with "Character String" selected.
- At the bottom, there are six buttons: "Encrypt", "Decrypt", "Generate", "Sign", "Verify", and "Crack".

Aparece el nombre cifrado con formato hexadecimal

Analisis del caso rasomware El ransomware, es un tipo de malware informático de rescate que no permite a los usuarios o empresas a acceder a su sistema. Los hackers que realizan el ransomware solicitan el pago en Bitcoins a los afectados para devolver o liberar la información. A pesar del éxito de las autoridades en la eliminación de las bandas que realizan este "Secuestro de la información", los delincuentes cibernéticos avanzan en las actividades delictivas. Aunque las empresas se preparan para evitar estos ransomware, sigue aumentando el

secuestro extorsivo de la información. Esta mala práctica no solamente afecta a las empresas, sino también a personas que son chantajeadas con publicar la información privada en distintas redes. Las recomendaciones para no ser víctima de ransomware es no dar clic sobre las URL o correos electrónicos maliciosos que pueden tener archivos infectados y que las empresas logren parchear la información o que tengan mecanismos de contingencia de continuidad del negocio, o mejor aún, llevar la información en la nube con un respaldo de la información, adicionalmente, para evitar el alza del ransomware, se recomienda no pagar el rescate de la información secuestrada, toda vez que, el pago aumenta este ciberdelito y en ocasiones a pesar de realizar el pago la información no es liberada. Ejemplo de ransomware en telefónica en el 2017

LA INTRANET GLOBAL

13 / 03 / 2017



URGENTE: APAGA TU ORDENADOR YA

El equipo de Seguridad ha detectado el ingreso a la red de Telefónica de un malware que afecta tus datos y ficheros. Por favor avisa a todos tus compañeros de esta situación.

Apaga el ordenador ya y no vuelvas a encenderlo **hasta nuevo aviso(*)**.

Te enviaremos un correo que podrás leer a través de tu móvil cuando la situación ya esté normalizada. Además, el martes informaremos en las entradas de los edificios sobre el acceso a la red.

Ante cualquier duda contacta con la Mesa de Ayuda (29000)

(*) Desconecta el móvil de la red WiFi pero no hace falta que lo apagues

Dirección de Seguridad

Los responsables de Telefónica han difundido este mensaje a los usuarios de su Intranet para que dejen de usar el ordenador de forma inmediata.

Aviso de ransomware



Analisis 2 acerca del articulo Ransomware

El contexto del año 2031 en materia de ciberseguridad sugiere dos aspectos importantes para rescatar: se requiere hacer inversión en este campo (a nivel personal, empresarial, estatal) y segundo, es relevante identificar el cibercrimen de mayor impacto que se posiciona con mayor frecuencia en los procesos de protección de la información. El artículo sugiere el secuestro de datos o ransomware, práctica que promueve pequeñas y grandes extorsiones por su recuperación y/o acceso.

Una particularidad del malware es su capacidad de mutar en su estructura para esconderse y atacar los sistemas operativos, de tal manera que su ubicación pueda tardar un tiempo en hacerse, ya sea por sus propiedades o por la poca consciencia respecto a su existencia; también cabe resaltar que el ritmo frenético de maximizar la producción de bienes y servicio, resta importancia a la capacidad de daño de este software destructivo.

Las publicaciones de diverso orden, opiniones, análisis y especulaciones de expertos y oportunistas describen escenarios de destrucción en la economía digitalizada, impacto en sectores reales como el financiero, inmobiliario, transacciones de redes, industriales, procesos sistematizados, entre otros. Tal

circunstancia se presenta como oportunidad de negocio y desarrollo de defensas corporativas que protejan a los usuarios de cualquier nivel ante las demandas de los extorsionistas.

Una de las estrategias que combate este malware son el sistema multicopiado de seguridad de datos, también con sistema de alertas de ransomware para encriptar y restaurar datos con intentos o efectivamente, prácticas de cifrado y restauración de data. El tiempo y la escalabilidad son elementos a favor de los ciberdelitos debido a los desarrollos tecnológicos en dispositivos de rápida expansión e internet de las cosas. Todo ello va en contravía de políticas globalizadas que promueven las ciudades inteligentes con la digitalización de los procesos industriales, la banca y demás espacios de interacción humana, sin necesidad de estar físicamente sino a través del ciber espacio.

Las soluciones nube y la realidad administrativa/organizacional de múltiples entidades hacen que los escenarios sean posibles de sortear, al igual que posibles nuevos lugares de ataque cibernético ya que los ecosistemas son los objetivos de primer orden para los sujetos dedicados a identificar y visualizar los huecos en los sistemas y aplicativos en uso. Son reconocidas las metodologías DevOps y DevSecOps para minimizar el ataque cyber, al igual que las utilizadas con el parcheo por medio de plataformas Cloud; la velocidad del desarrollo va a la par del desarrollo de las estrategias de destrucción.

Como oportunidad se visualiza la seguridad de data, la educación y capacitación preventiva, y las políticas y tácticas de los organismos de seguridad que combaten por aparte y en conjunto con algunas estrategias. El mercado promueve igualmente una dinámica de oferta/demanda que hace poroso e interesante a la vez el crecimiento de la industria digital.