Práctica de laboratorio: uso de firmas digitales

Objetivos

Comprender los conceptos detrás de la firma digital.

Parte 1: demostrar el uso de las firmas digitales.

Parte 2: demostrar la verificación de una firma digital.

Aspectos básicos/situación

Una firma digital es una técnica matemática utilizada para validar la autenticidad y la integridad de un mensaje digital. Una firma digital es el equivalente de una firma manuscrita. Las firmas digitales realmente pueden ser mucho más seguras. El propósito de una firma digital es evitar la manipulación y la suplantación de identidad en las comunicaciones digitales. En muchos países, incluido Estados Unidos, las firmas digitales tienen la misma importancia legal que las formas tradicionales de documentos firmados. El gobierno de los Estados Unidos actualmente publica las versiones electrónicas de presupuestos, leyes y proyectos parlamentarios con firmas digitales.

Recursos necesarios

- Equipo de escritorio o dispositivo móvil con acceso a Internet

Parte 1: Uso de firmas digitales

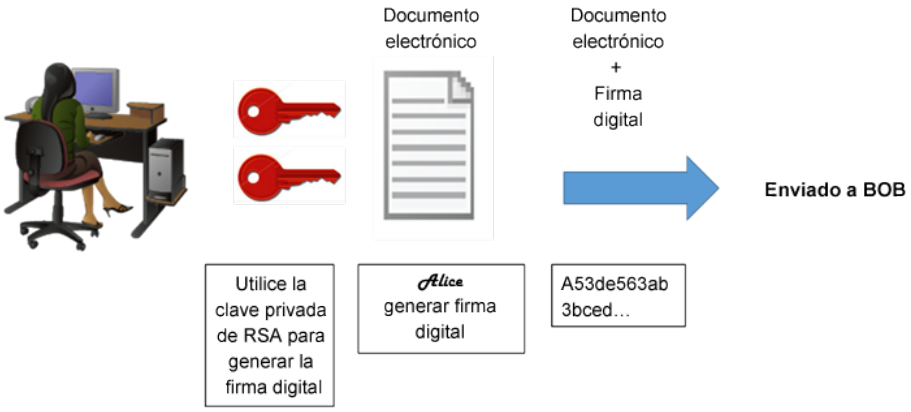
En esta parte, utilizará una página web para verificar la firma de un documento entre Alice y Bob. Alice y Bob comparten un par de claves RSA privadas y públicas. Cada uno de ellos usa la clave privada para firmar un documento jurídico. Luego se envían los documentos entre sí. Alice y Bob pueden verificar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

Tabla 1: claves RSA públicas y privadas

Clave RSA pública	d94d889e88853dd89769a18015a0a2e6bf82bf356fe14f251fb4f5e2df0d9f9a94a68a30c428b39e3362fb3779a497eceaea37100f264d7fb9fb1a97fbf621133de55fdcb9b1ad0d7a31b379216d79252f5c527b9bc63d83d4ecf4d1d45cbf843e8474babc655e9bb6799cba77a47eafa838296474afc24beb9c825b73ebf549
Clave RSA privada	47b9cfde843176b88741d68cf096952e950813151058ce46f2b048791a26e507a1095793c12bae1e09d82213ad9326928cf7c2350acb19c98f19d32d577d666cd7bb8b2b5ba629d25ccf72a5ceb8a8da038906c84dcdb1fe677dffb2c029fd8926318eede1b58272af22bda5c5232be066839398e42f5352df58848adad11a1
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.

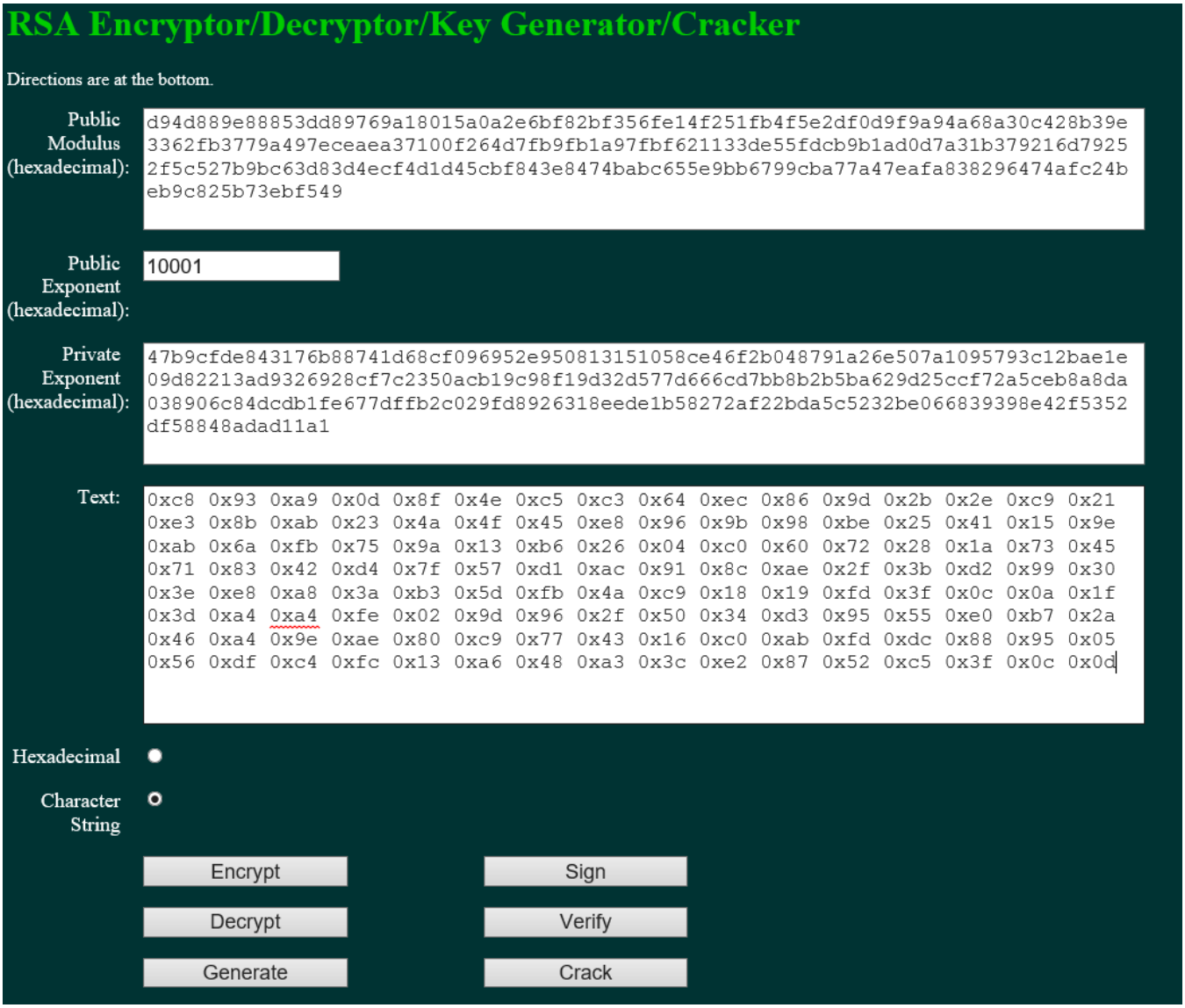
Bob recibe el documento con una firma digital que se muestra en la siguiente tabla.

Tabla 2: firma digital de Alice

Firma digital 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

Haga clic aquí para usar la herramienta en línea RSA a fin de verificar la autenticidad de la firma digital de Alice.

Tabla 3: herramienta de firma digital en línea



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).

Tabla 4: firma digital de BOB

Firma digital de BOB
0x6c 0x99 0xd6 0xa8 0x42 0x53 0xee 0xb5 0x2d 0x7f 0x0b 0x27 0x17 0xf1 0x1b 0x62 0x92 0x7f 0x92 0x6d 0x42 0xbd 0xc6 0xd5 0x3e 0x5c 0xe9 0xb5 0xd2 0x96 0xad 0x22 0x5d 0x18 0x64 0xf3 0x89 0x52 0x08 0x62 0xe2 0xa2 0x91 0x47 0x94 0xe8 0x75 0xce 0x02 0xf8 0xe9 0xf8 0x49 0x72 0x20 0x12 0xe2 0xac 0x99 0x25 0x9a 0x27 0xe0 0x99 0x38 0x54 0x54 0x93 0x06 0x97 0x71 0x69 0xb1 0xb6 0x24 0xed 0x1c 0x89 0x62 0x3d 0xd2 0xdf 0xda 0x7a 0x0b 0xd3 0x36 0x37 0xa3 0xcb 0x32 0xbb 0x1d 0x5e 0x13 0xbc 0xca 0x78 0x3e 0xe6 0xfc 0x5a 0x81 0x66 0x4e 0xa0 0x66 0xce 0xb3 0x1b 0x93 0x32 0x2c 0x91 0x4c 0x58 0xbf 0xff 0xd8 0x97 0x2f 0xa8 0x57 0xd7 0x49 0x93 0xb1 0x62

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?

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 el 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.

d. Copie las nuevas claves en la Tabla 5.

Tabla 5: nuevas claves RSA

Clave pública	
Clave privada	

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

Tabla 6: firma digital personal

Firma digital personal	

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.

Tabla 7: claves RSA de sus compañeros

Clave pública	
Clave privada	

c. Ahora intercambie su firma digital de la Tabla-6. Registre lla firma digital en la siguiente tabla.

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?