Übung – Verwenden von digitalen Signaturen

Zielsetzung

Lernen Sie die Konzepte hinter digitalen Signaturen kennen.

Teil 1: Demonstrieren Sie die Verwendung digitaler Signaturen.

Teil 2: Demonstrieren Sie das Überprüfen einer digitalen Signatur.

Hintergrund/Szenario

Digitale Signaturen sind eine mathematische Methode zum Validieren der Echtheit und Integrität einer digitalen Nachricht. Eine digitale Signatur ist genauso viel wert wie eine handschriftliche Unterschrift. Digitale Signaturen können sogar wesentlich sicherer sein. Mit digitalen Signaturen sollen Manipulationen und betrügerisches Auftreten bei der digitalen Kommunikation verhindert werden. In vielen Ländern sind digitale Signaturen ebenso rechtsgültig wie herkömmliche Unterschriften auf Dokumenten. Die US-Behörden veröffentlichen inzwischen elektronische Versionen von Budgets, Gesetzen und Gesetzesentwürfen mit digitalen Signaturen.

Erforderliche Ressourcen

- PC oder Mobilgerät mit Internetzugang

Teil 1: Verwenden von digitalen Signaturen

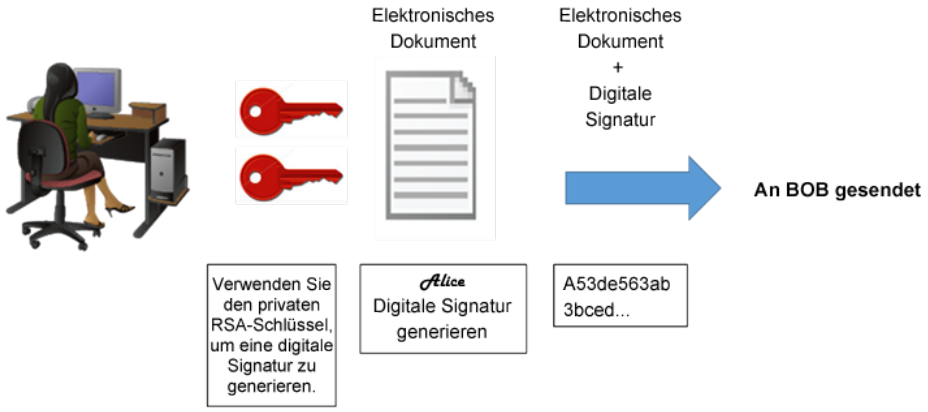
In diesem Teil der Übung verwenden Sie eine Website zum Überprüfen einer Dokumentsignatur in der Kommunikation zwischen Alice und Bob. Alice und Bob teilen sich ein Paar aus privaten und öffentlichen RSA-Schlüsseln. Jeder von ihnen verwendet seinen eigenen privaten Schlüssel zum Unterzeichnen eines rechtlichen Dokuments. Dann senden sie einander die Dokumente. Beide können die Signatur des jeweils anderen mithilfe des öffentlichen Schlüssels überprüfen. Außerdem müssen sie einen gemeinsamen öffentlichen Exponenten für die Berechnung vereinbaren.

Tabelle 1: Öffentlicher und privater RSA-Schlüssel

Öffentlicher RSA-Schlüssel	d94d889e88853dd89769a18015a0a2e6bf82bf356fe14f251fb4f5e2df0d9f9a94a68a30c428b39e3362fb3779a497eceaea37100f264d7fb9fb1a97fbf621133de55fdcb9b1ad0d7a31b379216d79252f5c527b9bc63d83d4ecf4d1d45cbf843e8474babc655e9bb6799cba77a47eafa838296474afc24beb9c825b73ebf549
Privater RSA-Schlüssel	47b9cfde843176b88741d68cf096952e950813151058ce46f2b048791a26e507a1095793c12bae1e09d82213ad9326928cf7c2350acb19c98f19d32d577d666cd7bb8b2b5ba629d25ccf72a5ceb8a8da038906c84dcdb1fe677dffb2c029fd8926318eede1b58272af22bda5c5232be066839398e42f5352df58848adad11a1
Öffentlicher Exponent	10001

Schritt 1: Unterzeichnen Sie das Dokument.

Unter Verwendung des öffentlichen und des privaten RSA-Schlüssels aus der Tabelle oben signiert Alice ein rechtliches Dokument und sendet es an Bob. Bob muss nun Alices digitale Signatur überprüfen, um sich der Echtheit des elektronischen Dokuments zu vergewissern.



Schritt 2: Überprüfen Sie die digitale Signatur.

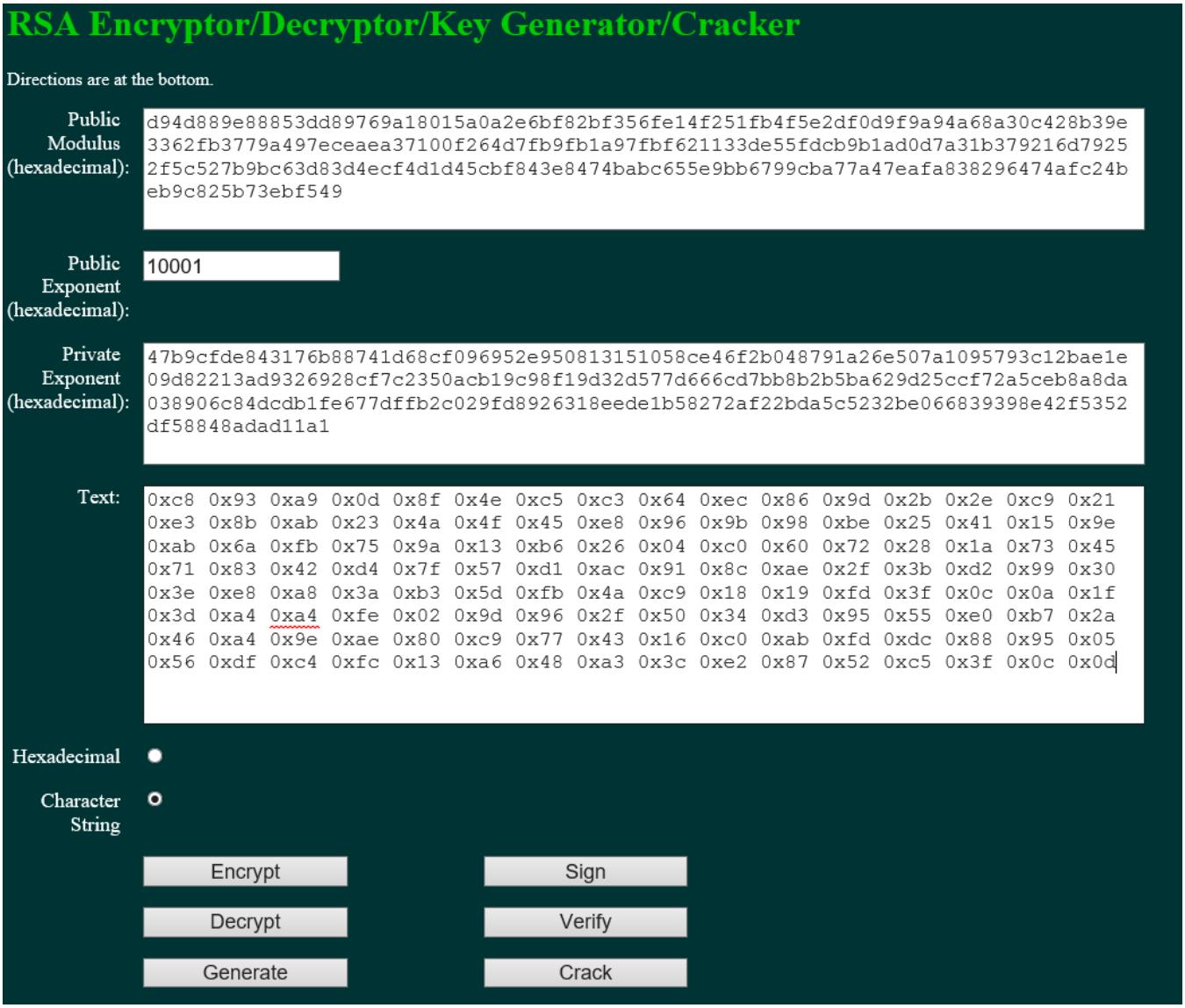
Bob erhält das Dokument mit der in der Tabelle unten angegebenen digitalen Signatur.

Tabelle 2: Alices digitale Signatur

Alices digitale Signatur
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 0x83 0x42 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

Klicken Sie hier, um die Echtheit von Alices digitaler Signatur mit dem RSA-Online-Tool zu überprüfen.

Tabelle 3: Online-Tool für digitale Signaturen



a. Kopieren Sie den **öffentlichen** und den **privaten** Schlüssel aus Tabelle 1 oben, und fügen Sie sie auf der Website wie oben im Bild gezeigt in den Feldern **Public Modulus** (Öffentlicher Modulo) und **Private Exponent** (Privater Exponent) ein.

b. Der öffentliche Exponent muss 10001 sein.

c. Fügen Sie Alices Signatur aus Tabelle 2 auf der Website wie oben im Bild gezeigt im Feld "Text" ein.

d. Bob kann die digitale Signatur jetzt überprüfen, indem er im unteren mittleren Bereich der Website auf die Schaltfläche **Verify** (Überprüfen) klickt. Wessen Signatur wird identifiziert?

Schritt 3: Generieren Sie eine Signatur für die Antwort.

Bob empfängt und überprüft das elektronische Dokument von Alice mit ihrer digitalen Signatur. Daraufhin erstellt Bob ein eigenes elektronisches Dokument und generiert seine eigene digitale Signatur mit dem privaten RSA-Schlüssel aus Tabelle 1. (Hinweis: Bobs Name ist in Großbuchstaben angegeben.)

Tabelle 4: Digitale Signatur von BOB

Digitale Signatur von 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 sendet das elektronische Dokument mit der digitalen Signatur an Alice.

Schritt 4: Überprüfen Sie die digitale Signatur.

a. Kopieren Sie den **öffentlichen** und den **privaten** Schlüssel aus Tabelle 1 oben, und fügen Sie sie auf der Website wie oben im Bild gezeigt in den Feldern **Public Modulus** (Öffentlicher Modulo) und **Private Exponent** (Privater Exponent) ein.

b. Der öffentliche Exponent muss 10001 sein.

c. Fügen Sie Bobs Signatur aus Tabelle 4 auf der Website wie oben im Bild gezeigt im Feld "Text" ein.

d. Alice kann die digitale Signatur jetzt überprüfen, indem sie im unteren mittleren Bereich der Website auf die Schaltfläche **Verify** (Überprüfen) klickt. Wessen Signatur wird identifiziert?

Teil 2: Erstellen einer eigenen digitalen Signatur

Sie wissen jetzt, wie digitale Signaturen funktionieren, und können nun eine eigene erstellen.

Schritt 1: Generieren Sie ein neues Paar RSA-Schlüssel.

Generieren Sie mit dem Tool auf der Website einen neuen Satz aus einem öffentlichen und einem privaten RSA-Schlüssel.

a. Löschen Sie die Inhalte der Felder **Public Modulus** (Öffentlicher Modulo), **Private Modulus** (Privater Modulo) und **Text**. Markieren Sie den Text einfach mit der Maus, und drücken Sie die Taste "Entfernen" auf der Tastatur.

b. Im Feld "Public Exponent" (Öffentlicher Exponent) muss der Wert **10001** angegeben sein.

c. Generieren Sie einen neuen Satz RSA-Schlüssel, indem Sie im unteren rechten Bereich der Website auf die Schaltfläche **Generate** (Generieren) klicken.

d. Kopieren Sie die neuen Schlüssel, und fügen Sie sie in Tabelle 5 ein.

Tabelle 5: Neue RSA-Schlüssel

Öffentlicher Schlüssel	
Privater Schlüssel	

e. Geben Sie jetzt im Feld **Text** Ihren vollständigen Namen ein, und klicken Sie auf **Sign** (Signieren).

Tabelle 6: Persönliche digitale Signatur

Persönliche digitale Signatur	

Teil 3: Austauschen und Überprüfen von digitalen Signaturen

Sie können die digitale Signatur jetzt verwenden.

Schritt 1: Tauschen Sie den neuen öffentlichen und privaten Schlüssel aus Tabelle 5 mit Ihrem Übungspartner aus.

a. Notieren Sie den öffentlichen und den privaten RSA-Schlüssel Ihres Übungspartners aus dessen Tabelle 5.

b. Halten Sie beide Schlüssel in der Tabelle unten fest.

Tabelle 7: RSA-Schlüssel des Übungspartners

Öffentlicher Schlüssel	
Privater Schlüssel	

c. Tauschen Sie jetzt die digitale Signatur aus Tabelle 6 mit Ihrem Übungspartner aus. Notieren Sie die digitale Signatur in der Tabelle unten.

Digitale Signatur des Übungspartners	

Schritt 2: Überprüfen Sie die digitale Signatur Ihres Übungspartners.

a. Um die digitale Signatur Ihres Übungspartners zu überprüfen, fügen Sie seinen öffentlichen und privaten Schlüssel auf der Website in den Feldern **Public Modulus** (Öffentlicher Modulo) und **Private Modulus** (Privater Modulo) ein.

b. Fügen Sie dann im Feld **Text** die digitale Signatur ein.

c. Überprüfen Sie die digitale Signatur, indem Sie auf die Schaltfläche "Verify" (Überprüfen) klicken.

d. Was wird im Feld "Text" angezeigt?