Lab – Using Digital Signatures (Instructor Version)

Instructor Note: Have students pair up for this lab.

Objectives

Understand the concepts behind digital signature.

Part 1: Demonstrate the use of digital signatures.

Part 2: Demonstrate the verification of a digital signature.

Background / Scenario

A digital signature is a mathematical technique used to validate the authenticity and integrity of a digital message. A digital signature is the equivalent of a handwritten signature. Digital signatures can actually be far more secure. The purpose of a digital signature is to prevent the tampering and impersonation in digital communications. In many countries, including the United States, digital signatures have the same legal significance as traditional forms of signed documents. The United States Government now publishes electronic versions of budgets, laws, and congressional bills with digital signatures.

Required Resources

- PC or mobile device with Internet access

Part 1: Using Digital Signatures

In this part, you will use a website to verify a document signature between Alice and Bob. Alice and Bob share a pair of private and public RSA keys. Each of them uses their private key to sign a legal document. They then send the documents to each other. Both Alice and Bob can verify each other's signature with the public key. They must also agree on a shared public exponent for calculation.

Table 1 - RSA Public and Private Keys

Public RSA Key	d94d889e88853dd89769a18015a0a2e6bf82bf356fe14f251fb4f5e2df0d9f9a94a68a3 0c428b39e3362fb3779a497eceaea37100f264d7fb9fb1a97fbf621133de55fdcb9b1ad 0d7a31b379216d79252f5c527b9bc63d83d4ecf4d1d45cbf843e8474babc655e9bb67 99cba77a47eafa838296474afc24beb9c825b73ebf549
Private RSA Key	47b9cfde843176b88741d68cf096952e950813151058ce46f2b048791a26e507a1095 793c12bae1e09d82213ad9326928cf7c2350acb19c98f19d32d577d666cd7bb8b2b5b a629d25ccf72a5ceb8a8da038906c84dcdb1fe677dffb2c029fd8926318eede1b58272 af22bda5c5232be066839398e42f5352df58848adad11a1
Public Exponent	10001

Step 1:   Sign the Document.

Alice signs a legal document and send it to Bob using the RSA public and private keys shown in the table above. Now Bob will have to verify Alice's digital signature in order to trust the authenticity of the electronic document.
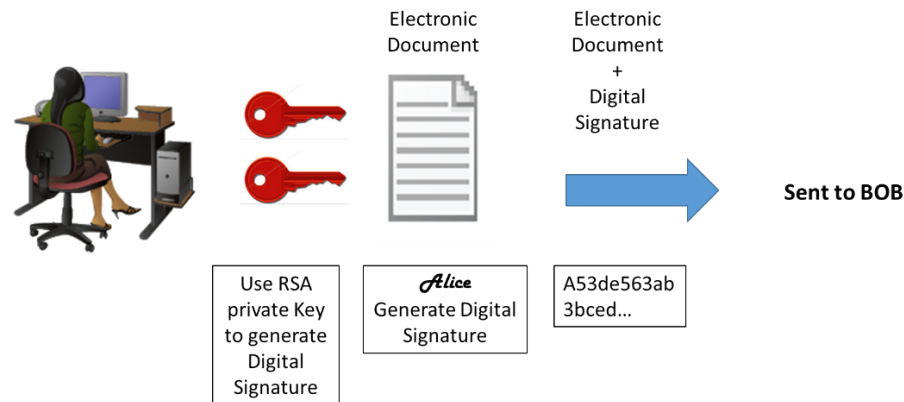
Step 2:   Verify Digital Signature.

Bob receives the document with a digital signature shown in the table below.

Table 2 - Alice's Digital Signature

Alice's Digital Signature
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

Click here to use the online RSA tool to verify the authenticity of Alice's digital signature.

Table 3 - Online Digital Signature Tool

RSA Encryptor/Decryptor/Key Generator/Cracker

Directions are at the bottom.

| Public Modulus (hexadecimal): | d94d889e88853dd89769a18015a0a2e6bf82bf356fe14f251fb4f5e2df0d9f9a94a68a30c428b39e3362fb3779a497eceaea37100f264d7fb9fb1a97fbf621133de55fdcb9b1ad0d7a31b379216d79252f5c527b9bc63d83d4ecf4d1d45cbf843e8474babc655e9bb6799cba77a47eafa838296474afc24beb9c825b73ebf549 |

| Public Exponent (hexadecimal): | 10001 |

| Private Exponent (hexadecimal): | 47b9cfde843176b88741d68cf096952e950813151058ce46f2b048791a26e507a1095793c12bae1e09d82213ad9326928cf7c2350acb19c98f19d32d577d666cd7bb8b2b5ba629d25ccf72a5ceb8a8da038906c84dcdb1fe677dffb2c029fd8926318eede1b58272af22bda5c5232be066839398e42f5352df58848adad11a1 |

```
Text:   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
```

Hexadecimal ●
Character String ○

Encrypt	Sign
Decrypt	Verify
Generate	Crack

a. Copy and paste the **public** and **private** keys from Table 1 above into the **Public Modulus** and **Private Exponent** boxes on the website as shown in the picture above.

b. Make sure the Public Exponent is 10001.

c. Paste Alice's digital signature from Table 2 in the box labeled text on the website as shown above.

d. Now BOB can verify the digital signature by clicking the **Verify** button near the bottom center of the website. Whose signature is identified?

Alice's (ALICE)

Step 3: Generate a Response Signature.

Bob receives and verifies Alice's electronic document and digital signature. Now Bob creates an electronic document and generates his own digital signature using the private RSA Key in Table 1 (Note: Bob's name is in all capital letters).

BOB's Digital Signature
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 sends the electronic document and digital signature to Alice.

Step 4: Verify Digital Signature.

a. Copy and paste the **public** and **private** keys from Table 1 above into the **Public Modulus** and **Private Exponent** boxes on the website as shown in the picture above.

b. Make sure the Public Exponent is 10001.

c. Paste Bob's digital signature from Table 4 in the box labeled text on the website as shown above.

d. Now Alice can verify the digital signature by clicking the **Verify** button near the bottom center of the website. Whose signature is identified?

Bob's (BOB) _____

Part 2: Create Your Own Digital Signature

Now that you see how digital signatures work, you can create your own digital signature.

Step 1: Generate a New Pair of RSA Keys.

Go to the website tool and generate a new set of RSA public and private keys.

a. Delete the contents of the boxes labeled **Public Modulus**, **Private Modulus** and **Text**. Just use your mouse to highlight the text and press the delete key on your keyboard.

b. Make sure the "Public Exponent" box has **10001**.

c. Generate a new set of RSA keys by clicking the **Generate** button near the bottom right of the website.

d. Copy the new keys in Table 5.

Table 5 - New RSA Keys

Public Key	af2143db5819096f7b3e212981c977cec353e1ef7359250bed95d51212863a87ecd78adcba8bd10f 6ce548eb15d46040a81aae6dda7401155ea20b1a179755d4ae86423e87ca7f9a4702d18342a4a477 300ec45dd719ccf5217c9c7f7396ede5b3c3dd4c54dc786824187be31cd596eccf37bf86b3bdaf66 057671ae422a92a7
Private key	195e132b318ea6dc3c18dacadd5ee678cfb855d0ce7f8a2b3925ebf02b38c03fb221e29e68731a3c 46c4cb9429dc5278eb20ba4575503a5bf3123bd372b95c182e2018e91eece79f03613b43f50f0d40 84add2eb3a7dff0fd722bdf61fca58b64537b110d57449076eec9e490e7251971ca270c189c3d206 d886f1953a7c8669

e. Now type in your full name into the box labeled **Text** and click **Sign**.

Table 6 - Personal Digital Signature

Personal Digital Signature	0x1e 0xe1 0xf5 0xc2 0x11 0x61 0x05 0xc5 0x8a 0xd6 0xbe 0x2c 0xe2 0x24 0xa9 0xe9 0x6c 0x53 0x16 0x31 0xac 0xc9 0x0f 0x43 0x2d 0xa8 0xfd 0x22 0x07 0x18 0xa0 0xe2 0x6f 0xd2 0x92 0x9b 0x6c 0x67 0x39 0xb7 0xdd 0x4f 0xb2 0xa2 0xdf 0x97 0x40 0x4d 0x53 0x10 0xf1 0x64 0xdd 0xc8 0x37 0xb4 0x80 0x70 0x21 0xfe 0x67 0xb9 0x5b 0xb3 0xd6 0xed 0xd0 0xd6 0x1e 0x5c 0xef 0x8d 0xc3 0xb8 0x5a 0x04 0xc1 0x3d 0xe0 0x9f 0xd6 0xe0 0xff 0x7b 0x40 0x44 0xad 0x2c 0x72 0x84 0x3f 0x68 0x44 0x58 0x4f 0x61 0xf6 0xf8 0x20 0xe5 0x90 0x24 0x23 0xc8 0x00 0xc6 0xbe 0xac 0x0d 0x84 0x52 0xaa 0x44 0x59 0x1f 0x6b 0x74 0xfc 0x7a 0x30 0x76 0x06 0xf7 0xf5 0xe1 0xa0 0x42 0xc0

Part 3: Exchange and Verify Digital Signatures

Now you can use this digital signature.

Step 1:   Exchange your new public and private keys in Table-5 with your lab partner.

a.   Record your lab partner's public and private RSA keys from their Table-5.

b.   Record both keys in the table below.

Table 7- Lab Partners RSA Keys

Public key	d020d5b8c1809c716a16d75f96f8032645125aef0855465bd31d6251b27d415785cb20c111122310 64f3a5d12a887e3cc1817dc4c26a5a9d36e156b55f4de307d6b1046493f2e71cb52563040dd508eb e368d601a24fa2378465e0ff52b8950a1bec5f61dc5e027a701f27d7872b0c0642bf7e0510728834 f763b9f88f3128c9
Private key	59c8004a0df71c0574bd5bb5199bed47e1fdf40a2f2f1205e481457b76a2bfc030b01a760e962358 1c245ac06b37ac352b485fe7b3f24b1a8ca512517546550bb270b66e3e1a4d223d7455447c4faf99 8ae7202a794d393bd9f7cd73623678950478733f547b415e294a259b291ae7658adf103d3341d31a faafe7c821c61101

c.   Now exchange their digital signature from their Table-6. Record the digital signature in the table below.

Lab Partner's Digital Signature	0x21 0x8b 0x9f 0xf8 0x5b 0xa5 0x1b 0x57 0xc1 0xb0 0x20 0xc7 0x5e 0x11 0xd4 0x2b 0xe3 0x01 0xa0 0xfb 0x91 0xa1 0xa4 0x30 0x3d 0x68 0xee 0x4b 0x79 0x18 0xa2 0x9d 0xdc 0x86 0x9f 0x58 0x1d 0x03 0x84 0x4e 0xb3 0x45 0xd1 0x4c 0x6c 0x7a 0xea 0x06 0x64 0x7e 0x84 0x89 0xb0 0x33 0x5c 0x77 0xaf 0x98 0x55 0x7b 0xb0 0x87 0x24 0xd2 0x40 0x89 0x9c 0xb2 0x27 0x61 0xd9 0xb7 0x41 0x97 0x95 0x29 0xb9 0x9b 0xa6 0x16 0xf3 0xa2 0x7e 0x0d 0x97 0xa1 0x8c 0xe0 0x6e 0x77 0xe5 0x2f 0xf6 0xbe 0xfa 0x46 0x14 0xf3 0x88 0x85 0xd4 0x6e 0x16 0x38 0x58 0xb4 0xcb 0x0f 0xdb 0xd3 0x22 0x22 0x60 0x45 0x28 0x1d 0x38 0xb0 0xf2 0x28 0x77 0x3f 0x66 0x7e 0x24 0xb7 0x22 0x16

Step 2:   Verify Lab Partners Digital Signature

a.   To verify your lab partner's digital signature, paste his or her public and private keys in the appropriate boxes labeled **Public and Private modulus** on the website.

b.   Now paste the digital signature in the box labeled **Text**.

c.   Now verify his or her digital signature by clicking the button labeled verify.

    d.   What shows up in the Text box?

      Jay Tejada