Lab – Using Digital Signatures

1. Objectives

Understand the concepts behind digital signature.

Part 1: Demonstrate the use of digital signatures.

Part 2: Demonstrate the verification of a digital signature.

1. 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.

1. Required Resources

* PC or mobile device with Internet access

1. Using Digital Signatures

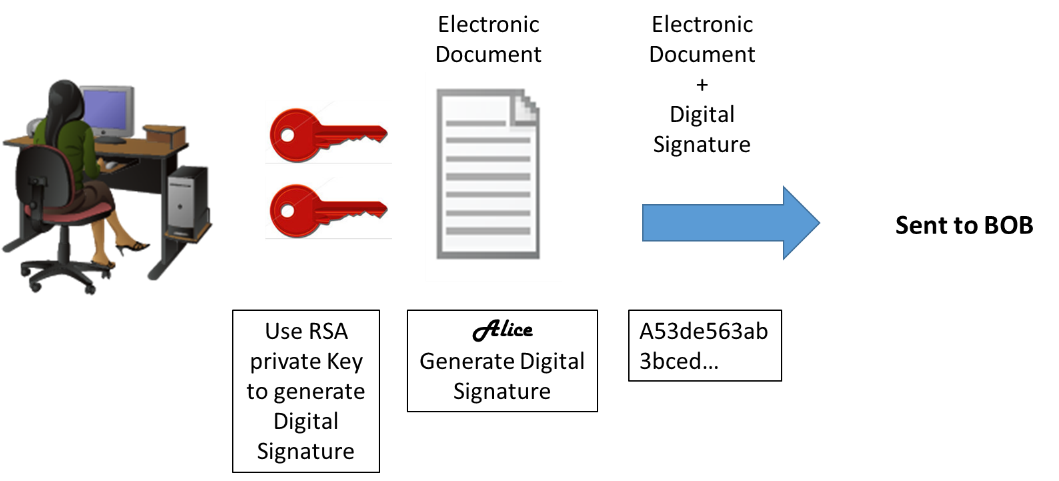
In this part, you will use a website to verify a document signature between Alice and Bob. Alice and Bob share a pair of private and public RSA keys. Each of them uses their private key to sign a legal document. They then send the documents to each other. Both Alice and Bob can verify each other’s signature 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 | d94d889e88853dd89769a18015a0a2e6bf82bf356fe14f251fb4f5e2df0d9f9a94a68a30c428b39e3362fb3779a497eceaea37100f264d7fb9fb1a97fbf621133de55fdcb9b1ad0d7a31b379216d79252f5c527b9bc63d83d4ecf4d1d45cbf843e8474babc655e9bb6799cba77a47eafa838296474afc24beb9c825b73ebf549 |
| Private RSA Key | 47b9cfde843176b88741d68cf096952e950813151058ce46f2b048791a26e507a1095793c12bae1e09d82213ad9326928cf7c2350acb19c98f19d32d577d666cd7bb8b2b5ba629d25ccf72a5ceb8a8da038906c84dcdb1fe677dffb2c029fd8926318eede1b58272af22bda5c5232be066839398e42f5352df58848adad11a1 |
| Public Exponent | 10001 |

* 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.



* 1. Verify Digital Signature.

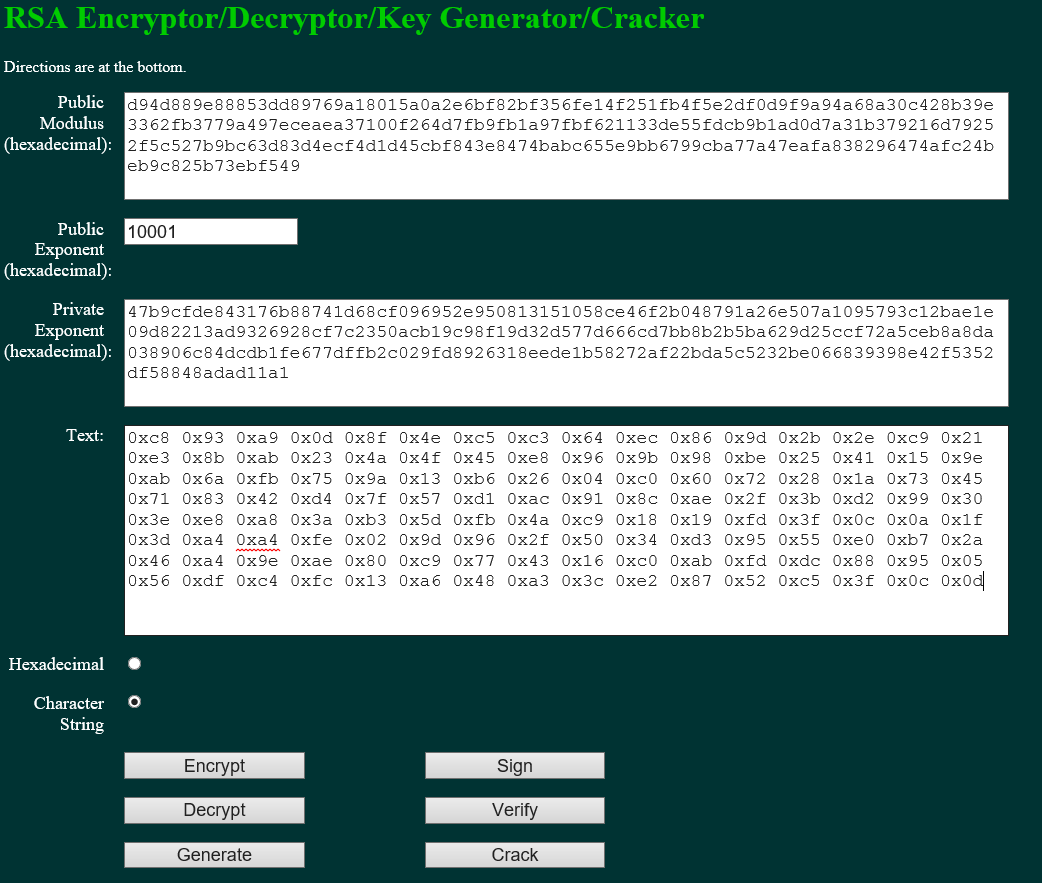
Bob receives the document with a digital signature shown in the table below.

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](http://nmichaels.org/rsa.py) to use the online RSA tool to verify the authenticity of Alice’s digital signature.

Table 3 - Online Digital Signature Tool



* + 1. 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.
    2. Make sure the Public Exponent is 10001.
    3. Paste Alice’s digital signature from Table 2 in the box labeled text on the website as shown above.
    4. Now BOB can verify the digital signature by clicking the **Verify** button near the bottom center of the website. Whose signature is identified?

***Trả lời:*** *Alice*

* 1. 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).

Table 4 - BOB Digital Signature

|  |
| --- |
| 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.

* 1. Verify Digital Signature.
     1. 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.
     2. Make sure the Public Exponent is 10001.
     3. Paste Bob’s digital signature from Table 4 in the box labeled text on the website as shown above.
     4. Now Alice can verify the digital signature by clicking the **Verify** button near the bottom center of the website. Whose signature is identified?

***Trả lời:*** *Bob*

1. Create Your Own Digital Signature

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

* 1. Generate a New Pair of RSA Keys.

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

* + 1. 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.
    2. Make sure the “Public Exponent” box has **10001**.
    3. Generate a new set of RSA keys by clicking the **Generate** button near the bottom right of the website.
    4. Copy the new keys in Table 5.

Table 5 - New RSA Keys

|  |  |
| --- | --- |
| Public Key | cce43f853944b052c1371c770d9d1203ed83e6b96e5a13d5379f16c2cdf8d709e8e062b586  43ab195940c1b81987664616d2b330786f78d0fa35d11fda4e2c4dcc6c4a66dbd334f7e34d  e14fdb67344ca5671dd815d19357e3b638499d5b6bcd8ce8623a201a2cf8c991b067b46d8a  e9addf33a2b606040d820a023a7bb95ea3a |
| Private key | 66c68f7e5a4db44cae92e07a6f9fbc6baff69c03a3f11745bad2d86dfb37b9564534590f493c  245560c9f4e24e1bf7176d575f7f0eca8bc5f7dc8afbf95b8128d70e3e569cb36eff7f9f3fdf42  e1cfc38c69d8d2895354614fb175735f794e9e3c4d6b591d76deeecb4e9fae12513356f6b16  2449ad6d4ee580bb339180cb751. |

* + 1. Now type in your full name into the box labeled **Text** and click **Sign**.

Table 6 - Personal Digital Signature

|  |  |
| --- | --- |
| Personal Digital Signature | 0xc3 0x16 0x4e 0xf9 0xa5 0x0a 0x54 0xd2 0xeb 0xfd 0x3e 0x3d 0xa8 0xde 0xb2 0xc2 0xc3 0xf8 0xc4 0x76 0x91 0x14 0xa3 0x1a 0xbe 0xdd 0x52 0xf9 0xde 0x3e 0xa6 0xb3 0xb6 0x54 0x88 0xc4 0xc2 0xd8 0xd9 0x85 0xd3 0xcf 0x15 0x56 0xbb 0x5d 0x6e 0x33 0x24 0xb5 0xa4 0x7f 0x51 0xb8 0x04 0xee 0x54 0x25 0x85 0xc7 0xf4 0x77 0x64 0x88 0x65 0x8c 0x83 0xf4 0xd0 0x31 0xfc 0x24 0x99 0xd4 0x47 0xa6 0xbd 0x27 0xc6 0xcd 0x31 0x16 0xa3 0x72 0x6d 0x7e 0x2e 0x70 0x01 0x21 0x7f 0x18 0x85 0xcd 0x3c 0x59 0x6d 0x5f 0x02 0xef 0x43 0xe0 0x40 0xe2 0x72 0x54 0x43 0x4a 0xd0 0x39 0x1d 0x47 0x9d 0x2e 0x9d 0xcd 0xbc 0xb7 0x9b 0xde 0xff 0x0c 0x25 0x0f 0x98 0xa0 0x63 0x2e |

1. 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.

* + 1. Record your lab partner’s public and private RSA keys from their Table-5.
    2. Record both keys in the table below.

Table 7- Lab Partners RSA Keys

|  |  |
| --- | --- |
| Public key | bc1cc4e93bb36d3fc1ab9868489370582ce77d4d646558fc3974750882b112f4886a084abe  7b3945867f430dd787141d86f8300b05d2fb1f9862611584404982cf919f9538bc912b8742  2e97608a39baf4c033149f9af613c298e18fa694c03e1b8107f9b9ba2541820335332cec603  2c40b919c4157ef94384352a06bddba1f |
| Private key | 25ff51af23060d4d519b8dbf92d9655a0a4800417fc4110371bf9a5c4bb9e4f04c15cef2fa22  fde09358657d084a1ac0142151e3081c23e9afe83f600f44c51433e3f81d7407322dbf7ab6a  f9ac612ef6d78c647ee145e2a19513ab444117c463369aab3e352c8ce0db14d8680ca9a470  6f3b3dcba58ff29727c76dd32ba57f1 |

* + 1. Now exchange their digital signature from their Table-6. Record the digital signature in the table below.

|  |  |
| --- | --- |
| Lab Partner’s Digital Signature | 0x37 0x79 0xc3 0x80 0x3e 0xb6 0x57 0xc1 0x2f 0xf6 0x5b 0xec 0xf4 0x5b 0x44 0x5e 0xa0 0x6e 0x05 0x40 0x13 0x51 0xb2 0xea 0x5c 0x55 0x15 0xc3 0xcc 0x5b 0xca 0xc2 0x3f 0x41 0xc5 0x60 0x39 0x41 0x43 0x22 0x8e 0x00 0xc9 0x22 0xf2 0xd7 0x8a 0xce 0xf8 0xdb 0x49 0xb5 0xbe 0x76 0x83 0x84 0x3a 0x3b 0x51 0x09 0xbf 0x0d 0xaa 0x6c 0x3a 0xf9 0xc0 0x06 0x25 0x48 0xc3 0x30 0xbe 0xe5 0x50 0x13 0xd0 0xc2 0x6f 0xb7 0xf9 0xe8 0x5c 0x61 0x7d 0x97 0xa7 0xf7 0x74 0x8d 0xea 0xed 0x01 0xcb 0xe1 0xd7 0x3a 0x2c 0x89 0x72 0x0b 0x1c 0x1b 0x87 0xe5 0x27 0x8d 0x5e 0xb9 0xa4 0xe6 0xa0 0xf2 0xaa 0xd7 0xbd 0xcd 0x0b 0x84 0x42 0x23 0x2f 0xbe 0x09 0x04 0x89 0x3f 0x0 |

Step 2: Verify Lab Partners Digital Signature

* + 1. 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.
    2. Now paste the digital signature in the box labeled **Text**.
    3. Now verify his or her digital signature by clicking the button labeled verify.
    4. What shows up in the Text box?

***Trả lời:*** *Aki*