Laboratório - Uso de assinaturas digitais

Objetivos

Entenda os conceitos por trás da assinatura digital.

Parte 1: Demonstre o uso de assinaturas digitais.

Parte 2: Demonstre a verificação de uma assinatura digital.

Histórico/Cenário

Uma assinatura digital é uma técnica matemática usada para validar a autenticidade e a integridade de uma mensagem digital. Uma assinatura digital é o equivalente de uma assinatura feita à mão. As assinaturas digitais podem, na realidade, ser muito mais seguras. A finalidade de uma assinatura digital é evitar a adulteração das mensagens e a falsificação de identidade na comunicação digital. Em muitos países, incluindo os Estados Unidos, as assinaturas digitais têm o mesmo valor legal que as formas tradicionais de documentos assinados. O governo dos Estados Unidos publica, agora, versões eletrônicas de orçamentos, leis e projetos de leis do congresso com assinaturas digitais.

Recursos necessários

- Computador ou dispositivo móvel com acesso à Internet

Parte 1: Uso de assinaturas digitais

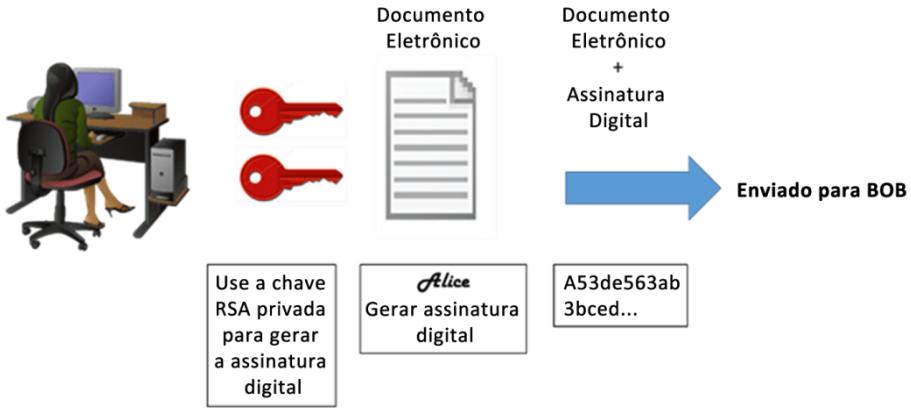
Nesta parte, você usará um site para verificar a assinatura de um documento entre Alice e Bob. Alice e Bob compartilham um par de chaves RSA públicas e privadas. Cada um deles usa sua chave privada para assinar um documento legal. Em seguida, eles enviam os documentos um para o outro. Alice e Bob podem verificar a assinatura um do outro com a chave pública. Eles também devem concordar em um expoente público compartilhado para cálculo.

Tabela 1 - Chaves RSA públicas e privadas

Chave RSA pública	d94d889e88853dd89769a18015a0a2e6bf82bf356fe14f251fb4f5e2df0d9f9a94a68a30c428b39e3362fb3779a497eceaea37100f264d7fb9fb1a97fbf621133de55fdcb9b1ad0d7a31b379216d79252f5c527b9bc63d83d4ecf4d1d45cbf843e8474babc655e9bb6799cba77a47eafa838296474afc24beb9c825b73ebf549
Chave RSA privada	47b9cfde843176b88741d68cf096952e950813151058ce46f2b048791a26e507a1095793c12bae1e09d82213ad9326928cf7c2350acb19c98f19d32d577d666cd7bb8b2b5ba629d25ccf72a5ceb8a8da038906c84dcdb1fe677dffb2c029fd8926318eede1b58272af22bda5c5232be066839398e42f5352df58848adad11a1
Expoente público	10001

Passo 1: Assine o documento.

Alice assina um documento legal e o envia para Bob usando as chaves RSA públicas e privadas mostradas na tabela acima. Agora Bob terá que verificar a assinatura digital da Alice para certificar a autenticidade do documento eletrônico.



Passo 2: Verifique a assinatura digital.

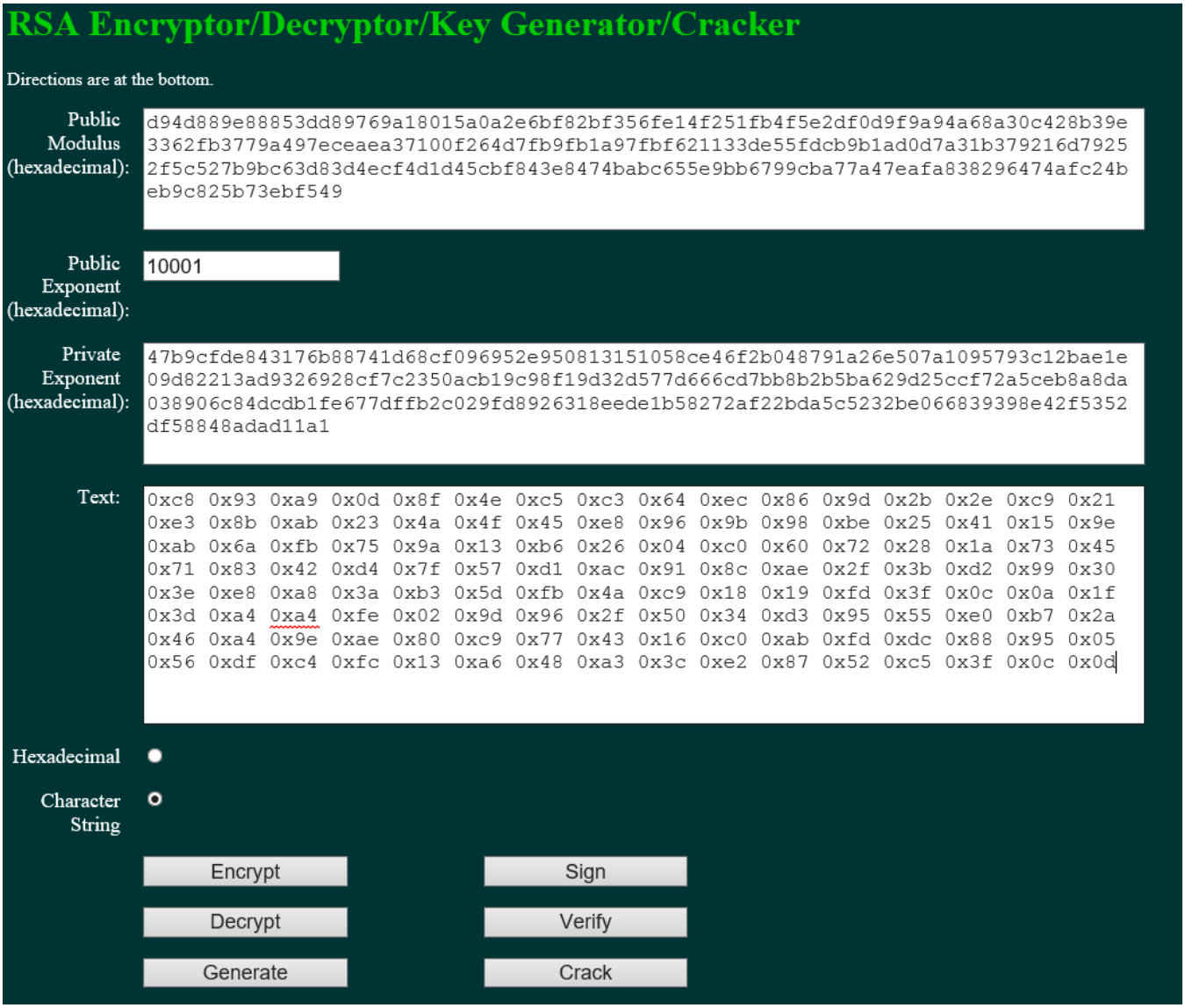
Bob recebe o documento com uma assinatura digital mostrada na tabela a seguir.

Tabela 2 - Assinatura digital da Alice

Assinatura digital da 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 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

Clique aqui para usar a ferramenta RSA on-line para verificar a autenticidade da assinatura digital da Alice.

Tabela 3 - Ferramenta de assinatura digital on-line



a. Copie e cole as chaves **públicas** e **privadas** da Tabela 1 acima nas caixas **Public Modulus** (Módulo público) **Private Exponent** (Expoente privado) no site, conforme mostrado na foto acima.

b. Certifique-se de que o expoente público seja 10001.

c. Cole a assinatura digital da Alice da Tabela 2 na caixa rotulada Text (Texto) no site, conforme mostrado acima.

d. Agora BOB pode verificar a assinatura digital clicando no botão **Verify** (Verificar) ao lado do centro inferior do site. A assinatura de quem é identificada?

Passo 3: Gere uma assinatura de resposta.

Bob recebe e verifica o documento eletrônico e a assinatura digital da Alice. Agora Bob cria um documento eletrônico e gera sua própria assinatura digital usando a chave RSA privada na Tabela 1 (Nota: O nome de Bob tem todas as letras maiúsculas).

Tabela 4 - Assinatura digital de BOB

Assinatura 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 envia o documento eletrônico e a assinatura digital para Alice.

Passo 4: Verifique a assinatura digital.

a. Copie e cole as chaves **públicas** e **privadas** da Tabela 1 acima nas caixas **Public Modulus** (Módulo público) **Private Exponent** (Expoente privado) no site, conforme mostrado na foto acima.

b. Certifique-se de que o expoente público seja 10001.

c. Cole a assinatura digital de Bob da Tabela 4 na caixa rotulada Text (Texto) no site, conforme mostrado acima.

d. Agora Alice pode verificar a assinatura digital clicando no botão **Verify** (Verificar) ao lado do centro inferior do site. A assinatura de quem é identificada?

Parte 2: Criar sua própria assinatura digital

Agora que você sabe como as assinaturas digitais funcionam, você pode criar sua própria assinatura digital.

Passo 1: Gere um novo par de chaves RSA.

Vá para a ferramenta do site e gere um novo conjunto de chaves RSA públicas e privadas.

a. Exclua o conteúdo das caixas rotuladas **Public Modulus** (Módulo público) **Private Modulus (Modo privado)** e **Text** (Texto). Basta usar o mouse para destacar o texto e pressionar a tecla Delete no teclado.

b. Certifique-se de que a caixa “Public Exponent” contenha o valor **10001**.

c. Gere um novo conjunto de chaves RSA clicando no botão **Generate** (Gerar) ao lado do canto direito inferior do site.

d. Copie as novas chaves na Tabela 5.

Tabela 5 - Novas chaves RSA

Chave pública	
Chave privada	

e. Agora, digite seu nome inteiro na caixa rotulada **Text** (Texto) e clique em **Sign (Assinar)**.

Tabela 6 - Assinatura digital pessoal

Assinatura digital pessoal.	

Parte 3: Troque e verifique as assinaturas digitais

Agora você pode usar essa assinatura digital.

Passo 1: Troque suas novas chaves públicas e privadas na Tabela 5 com seu parceiro de laboratório.

a. Registre as chaves RSA publicas e privadas de seu parceiro de laboratório da Tabela 5 dele.

b. Registre as duas chaves na tabela a seguir.

Tabela 7- Chaves RSA de parceiros de laboratório

Chave pública	
Chave privada	

c. Agora troque a assinatura digital dele usando a Tabela 6 de seu parceiro. Registre a assinatura digital na tabela a seguir.

Assinatura digital do parceiro de laboratório	

Passo 2: Verificar a assinatura digital dos parceiros de laboratório

a. Para verificar a assinatura digital do seu parceiro de laboratório, cole as chaves públicas e privadas dele/dela nas caixas adequadas rotuladas **Public and Private modulus** (Módulos público e privado) no site.

b. Agora cole a assinatura digital na caixa rotulada **Text** (Texto).

c. Agora verifique a assinatura digital dele ou dela clicando no botão rotulado Verify (Verificar).

d. O que aparece na caixa de texto?

