

Trabalho 3

Gerador\Verificador de Assinaturas

Lucas Resende Silveira Reis, 18/0144421

¹Dep. Ciência da Computação – Universidade de Brasília (UnB)
CiC 0201 - SEGURANÇA COMPUTACIONAL

toy.lcdv@hotmail.com

Abstract. *This corresponds to project 3, on encryption, decipherment with RSA.*

Resumo. *Este corresponde ao trabalho 3, sobre cifração, decifração com a RSA.*

1. Introdução

O RSA (Rivest–Shamir–Adleman) é um dos algoritmos mais amplamente utilizados em criptografia assimétrica. Desenvolvido por Ron Rivest, Adi Shamir e Leonard Adleman em 1977, o RSA é fundamental para a segurança da comunicação digital e transações online. Baseado na dificuldade computacional de fatorar grandes números primos, o RSA utiliza um par de chaves, pública e privada, para cifrar e decifrar informações. A segurança do algoritmo repousa na complexidade de se determinar os fatores primos de um grande número, tornando o RSA uma escolha robusta para a implementação de assinaturas digitais, troca segura de chaves e autenticação em sistemas de segurança informática.

1.1. Funcionalidade

O algoritmo RSA, concebido por Ron Rivest, Adi Shamir e Leonard Adleman em 1977, é um dos pilares da criptografia assimétrica. Essa técnica utiliza um par de chaves, uma pública, conhecida por todos, e outra privada, mantida em segredo. A geração das chaves envolve a escolha aleatória de dois números primos grandes, p e q , e o cálculo de $n = pq$ e $\phi(n) = (p - 1)(q - 1)$. A partir desses valores, são determinados e e d de maneira que $ed \equiv 1 \pmod{\phi(n)}$.

A criptografia RSA é amplamente empregada na internet, sendo aplicada em diversos contextos, como e-mails e transações online. O processo de encriptação envolve elevar a mensagem à potência de e módulo n , enquanto a deciptação utiliza a potência de d módulo n . A segurança do RSA baseia-se na dificuldade computacional de fatorar números primos grandes, garantindo a confidencialidade e autenticidade das comunicações digitais.

A assinatura em RSA é um processo essencial para garantir a autenticidade e integridade das mensagens. Para assinar uma mensagem, utiliza-se a biblioteca de hash, como o hashlib, para criar um resumo criptográfico da mensagem. Em seguida, esse resumo é cifrado utilizando a chave privada do remetente e a função de encriptação RSA.

Na fase de verificação, o destinatário realiza a deciptação da assinatura utilizando a chave pública do remetente. O resultado é comparado com o resumo criptográfico

original, obtido a partir da mensagem recebida. Se as duas informações coincidirem, a assinatura é considerada válida, atestando a origem da mensagem e sua integridade. Esse processo confere confiança nas transmissões digitais, assegurando que as mensagens não foram adulteradas e foram realmente enviadas pelo remetente autenticado.

2. Resultados

Se o código é executado com os inputs presentes no README estes serão os resultados:

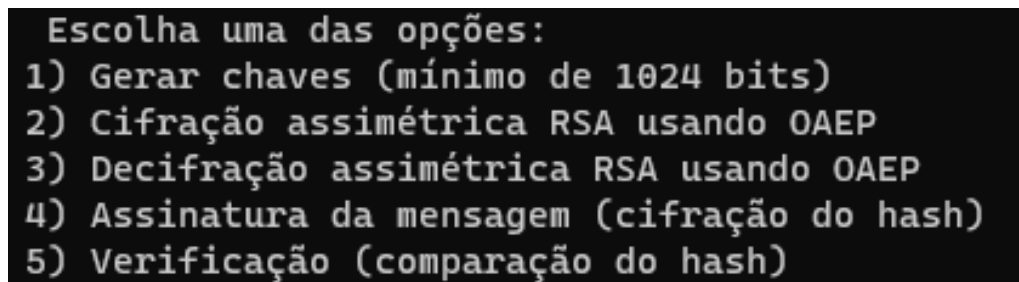


Figura 1. Menu de escolhas

```
Chave Pública: (94543881106804675877867688201464902085842706092032620683596593093536809544541418994357931302330443226495
996865805990610659887244894973849311827082577163685769084295123305337289885914964870639829525759498037729004134747456507
829098070143953336613476094257231703246503132115320707117632672803437998769257667569, 7075054892844811217506426272742349
0123186200165696096735817372355923761883383405700842023383672807495316926885485902677811347177857332535982052297400160
323098741542216449719367978181271745597442364319476901740431771605779488730188302055607179178188295919582046073829590384
9854669400062293362687790815521509)

Chave Privada: (94543881106804675877867688201464902085842706092032620683596593093536809544541418994357931302330443226495
996865805990610659887244894973849311827082577163685769084295123305337289885914964870639829525759498037729004134747456507
829098070143953336613476094257231703246503132115320707117632672803437998769257667569, 3654167163929023550409003206884694
827414621205342729154909012435968655085641975800195431511271796031047054819908173588241586776526043347943358089838500676
39076073778212867035353114368116289821551066285318489791881240860238194245091484517472798336353792189424595263166623666
7388564030077520132077846658330269)
```

Figura 2. Resultado 1

```
Digite:
Mensagem a ser criptografada: O que eu bebi por você dá pra encher um navio
Chave Pública: 945438811068046758778676882014649020858427060920326206835965930935368095445414189943579313023304432264959
968658059906106598872448949738493118270825771636857690842951233053372898859149648706398295257594980377290041347474565078
29098070143953336613476094257231703246503132115320707117632672803437998769257667569, 70750548928448112175064262727423490
1231862001656960967358173723559237618833834057008420233836728074953169268854859026778113471778573325359820522974001603
230987415422164497193679781812717455974423643194769017404317716057794887301883020556071791781882959195820460738295903849
854669400062293362687790815521509

Mensagem criptografada: PFP67f540tuSFG+AFxMQuJ6NqwyCQqW0RRUnlvkmOACDGQ3lLa9HLdFG0IGwRKSHdnv4IpdJpX10PUA39KImKnQhIfwIdVc
nupGA95x7ys+XV70rmE81z2LkFvIR8SDYIoI/34HbVjCjGnDth723Z5uwyE3Desjvuo9suLzYSU=
```

Figura 3. Resultado 2

```
Digite:
Mensagem criptografada: PFP67f540tuSFG+AFxMQuJ6NqwyCQqW0RRUnlvkmOACDGQ3lLa9HLdFG0IGwRKSHdnv4IpdJpX10PUA39KImKnQhIfwIdVc
nupGA95x7ys+XV70rmE81z2LkFvIR8SDYIoI/34HbVjCjGnDth723Z5uwyE3Desjvuo9suLzYSU=

Mensagem descryptografada: O que eu bebi por você dá pra encher um navio
```

Figura 4. Resultado 3

```

Digite:
Mensagem a ser assinada: O que eu bebi por você dá pra encher um navio
Chave Privada: 945438811068046758778676882014649020858427060920326206835965930935368095445414189943579313023304432264959
968658059906106598872448949738493118270825771636857690842951233053372898859149648706398295257594980377290041347474565078
29098070143953336613476094257231703246503132115320707117632672803437998769257667569, 36541671639290235504090032068846948
274146212053427291549090124359686550856419758001954315112717960310470548199081735882415867765260433479433580898385006763
907607377821286703535311143681162898215510662853184897918812408602381942450914845174727983363537921894245952631666236667
388564030877520132077846658330269
Assinatura: X+cply5eIrVA5mfj/MQLmoX+eLO/rgW8JaAh3f8SEAvL+0f6a7gLVuvUUhqhmF00/px4X4TjarJFRgK80rb99/anR0ejV2UCxITXy3r+P2L
cXP6Djpeh+f/zmgls19ZwxCBGSMASVG2qYKG7cNldfqsqJve+gzz7om7swG/wL4=

```

Figura 5. Resultado 4

```

Digite:
Mensagem original: O que eu bebi por você dá pra encher um navio

Assinatura: X+cply5eIrVA5mfj/MQLmoX+eLO/rgW8JaAh3f8SEAvL+0f6a7gLVuvUUhqhmF00/px4X4TjarJFRgK80rb99/anR0ejV2UCxITXy3r+P2L
cXP6Djpeh+f/zmgls19ZwxCBGSMASVG2qYKG7cNldfqsqJve+gzz7om7swG/wL4=
Chave Pública: 945438811068046758778676882014649020858427060920326206835965930935368095445414189943579313023304432264959
968658059906106598872448949738493118270825771636857690842951233053372898859149648706398295257594980377290041347474565078
29098070143953336613476094257231703246503132115320707117632672803437998769257667569, 70750548928448112175064262727423490
123186208165696096735817372355923761883338340570084202338367280749531692688548590267781134717785733253359820522974801603
2309874154221644977193679781812717455974423643194769017404317716057794887301883020556071791781882959195820460738295903849
854669400062293362687790815521509

A assinatura é
válida.

```

Figura 6. Resultado 5

3. Conclusão

Em conclusão, o algoritmo RSA, combinando técnicas de criptografia assimétrica e assinatura digital, desempenha um papel crucial na segurança da comunicação digital. Ao utilizar pares de chaves pública e privada, o RSA possibilita a transmissão segura de informações, garantindo autenticidade e integridade. A assinatura digital, baseada em hash e encriptação RSA, oferece uma robusta verificação de autenticidade das mensagens. Dessa forma, o RSA se torna uma peça fundamental na arquitetura de segurança online, protegendo transações, comunicações e dados sensíveis contra ameaças cibernéticas.

Referências

- [1] Criptografia - Criptografia RSA - Fábrica de Noobs
https://www.youtube.com/watch?v=GAR1Ur_2IGk
- [2] RSA (sistema criptográfico)
[https://pt.wikipedia.org/wiki/RSA_\(sistema_criptogr%C3%Alfico\)](https://pt.wikipedia.org/wiki/RSA_(sistema_criptogr%C3%Alfico))
- [3] Optimal asymmetric encryption padding
https://en.wikipedia.org/wiki/Optimal_asymmetric_encryption_padding
- [4] Teste de primalidade de Miller-Rabin https://pt.wikipedia.org/wiki/Teste_de_primalidade_de_Miller-Rabin
- [5] <https://docs.python.org/3/library/hashlib.html>
<https://docs.python.org/3/library/hashlib.html>