Criptografia de chave pública, RSA

André Gustavo dos Santos[1]

[1] Departamento de Informática
Universidade Federal de Viçosa

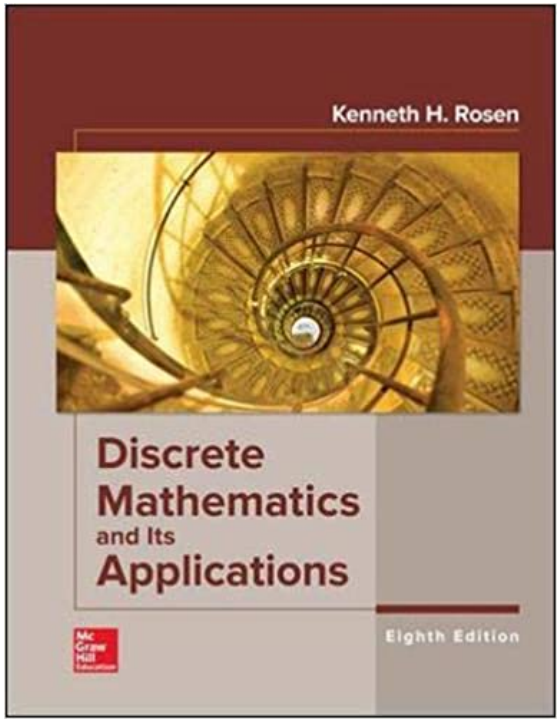
INF230 - 2021/1

UFV

Conteúdo

UFV

Os slides seguintes são baseados nas seções 4.6.3 a 4.6.8 do livro texto da disciplina:



ROSEN, Kenneth H.
Discrete mathematics and its applications.
McGraw-Hill Education, 8th edition, 2018

Criptografia de chave privada

- Os métodos vistos anteriormente são sistemas de criptografia de chave privada
- Sabendo-se a chave usada na codificação, é fácil descobrir a de decodificação
- Saber como codificar com uma certa chave permite decodificar com essa chave
- Por exemplo, na cifra de deslocamento com chave k
  - Um inteiro p é criptografado deslocando-se k, $c = (p + k) \text{mod } 26$
  - É descriptografado deslocando-se $-k$, $p = (c - k) \text{mod } 26$
- Quem envia e quem recebe a mensagem precisam combinar uma chave secreta
- Cada par de pessoas que se comunica precisa decidir e compartilhar uma chave
- Para evitar isso, nos anos 70 foi criada a criptografia de chave pública

UFV

Criptografia de chave pública

- Na criptografia de chave pública, saber como codificar uma mensagem não ajuda a saber como decodificá-la
- Nesse sistema, cada um tem uma chave de codificação conhecida publicamente
- E uma chave de decodificação mantida secreta
- Assim, qualquer um pode codificar uma mensagem para certo destinatário, mas somente o destinatário da mensagem pode decifrá-la
- Para isto funcionar deve existir alguma relação entre as chaves pública e secreta
- Isto é seguro se o fato de se conhecer a chave pública não permitir decifrar a mensagem, a não ser com uma quantidade extraordinária de trabalho
- O primeiro sistema foi criado nos anos 70 e muitos criados depois
- O mais usado atualmente é o RSA, que veremos em detalhes
- Outros serão usados futuramente, quando o RSA se tornar obsoleto

UFV

Criptografia de chave pública *vs.* de chave privada

- A grande vantagem dos sistemas de chave pública é que duas pessoas não precisam combinar uma chave para se comunicarem
- Uma desvantagem é que codificar/decodificar pode ser extremamente demorado
- Para muitas aplicações, isso torna a criptografia de chave pública impraticável
- Em tais situações, a criptografia de chave privada é usada
- Entretanto, a criptografia de chave pública ainda pode ser usada no processo de troca de chave

UFV

Criação do RSA

- O sistema foi apresentado em 1976 por Ronald Rivest, Adi Shamir, and Leonard Adleman, pesquisadores do MIT
- O nome RSA vem dos sobrenomes dos autores
- O sistema foi criado anos antes, em 1973, por Clifford Cocks, em uma pesquisa secreta do governo do Reino Unido, mantida como informação confidencial
- Isso só se tornou conhecido no final da década de 90, quando ele pode finalmente compartilhar a informação
- A ideia de Cocks, fundamental para segurança do RSA, é baseada no fato que é extremamente difícil reverter o processo de multiplicação de dois primos grandes
  - Dados dois primos grandes p e q, é fácil calcular $n = pq$
  - Mas dado n, é difícil encontrar p e q

UFV

Chaves do RSA

- No sistema RSA, cada indivíduo possui uma chave de codificação (n, e)
- n é o módulo, com $n = pq$, sendo p e q dois primos grandes
- e é o expoente, um valor coprimo com $(p - 1)(q - 1)$

- Se p e q tem cerca de 300 dígitos, n terá 600, facilmente computado a partir deles
- Fatorar n, no entanto, não pode ser feito com o conhecimento e recursos atuais
- Veremos que esse é o motivo de não ser possível, hoje, decifrar uma mensagem

UFV

Codificação RSA

- Para codificar uma mensagem M usando a chave pública (n, e), a mensagem é transformada em uma sequência de números inteiros de dois dígitos
  - A = 00, B = 01, ..., Z = 25
- Esses números são agrupados em blocos formando inteiros grandes $m_1, \ldots, m_k$
  - O tamanho desses blocos blocos deve ser o maior tal que 2525...25 não ultrapassa n
- A mensagem $M = m_1 m_2 \ldots m_k$ é então codificada[1] em $C = c_1 c_2 \ldots c_k$
  - $c_i = m_i^e \bmod n$
- A mensagem codificada C é enviada ao destinatário

[1] Esse cálculo pode ser feito pelo método de potenciação modular rápida visto anteriormente

Codificação RSA

Codificar STOP com a chave pública (2537, 13)

- STOP = 18 19 14 15
- $2525 < 2537 < 252525$ então os blocos terão tamanho 4
- A mensagem é então 1819 1415
- Esses números são codificados com $c = m^e \bmod n$
  - $1819^{13} \bmod 2537 = 2081$
  - $1415^{13} \bmod 2537 = 2182$

- Essa chave foi gerada com $p = 43$ e $q = 59$
- Assim, $n = pq = 43 \cdot 59 = 2537$
- Note que $\text{mdc}(e, (p-1)(q-1)) = \text{mdc}(13, 42 \cdot 58) = 1$

UFV

Decodificação RSA

- A decodificação é feita com uma chave secreta d que é o inverso de e módulo $(p-q)(q-1)$
  - Este inverso existe porque $\text{mdc}(e, (p-1)(q-1)) = 1$
- Se $de \equiv 1 (\text{mod } (p - 1(q-1))$ então existe inteiro k tal que $de = 1 + k(p-1)(q-1)$
  - $c^d \equiv (m^e)^d = m^{de} = m^{1+k(p-1)(q-1)} \text{ mod } n$
- Se $\text{mdc}(m, p) = 1$, temos, pelo pequeno teorema de Fermat, que $m^{p-1} \equiv 1 (\text{mod } p)$
  - E então $c^d \equiv m^{1+k(p-1)(q-1)} = m \cdot (m^{p-1})^{k(q-1)} \equiv m \cdot 1 = m \text{ mod } p$
- Pelo mesmo motivo[2], se $\text{mdc}(m, q) = 1$, temos
  - $c^d \equiv m \text{ mod } q$
- Como $\text{mdc}(p, q) = 1$, pelo teorema chinês do resto, esses dois resultados implicam que
  - $c^d \equiv m \text{ mod } pq$
- Portanto, $m \equiv c^d \text{ mod } n$, a mensagem é decifrada corretamente

[2] Quase sempre $\text{mdc}(m, p) = 1$ e $\text{mdc}(m, q) = 1$, mas funciona mesmo se não for

UFV

Decodificação RSA

Decodificar a mensagem 0981 0641, que foi codificada com a chave pública (2537, 13)

- $n = 2537 = 43 \cdot 59$, então $p = 43$ e $q = 59$
- $d = 937$ é um inverso de $e = 13$ módulo $(p-1)(q-1) = 42 \cdot 58 = 2436$
- A mensagem pode ser decodificada com $m = c^d \bmod n$
  - $0981^{937} \bmod 2537 = 0704$
  - $0641^{937} \bmod 2537 = 1115$
- 0704 1115 = 07 04 11 15 = HELP

- A chave pública do destinatário, conhecida por todos, é $(n, e) = (2637, 13)$
- A chave $d = 937$ é a chave secreta do destinatário do destinatário
- É possível calculá-la sabendo-se $p = 43$ e $q = 59$ pois é o inverso de e módulo $42 \cdot 58$
- Não se conhece outro método de calculá-la e não se conhece método eficiente para fatorar n

UFV

Assinatura digital

- No sistema RSA, Alice tem uma chave pública (n, e) e uma chave secreta d
  - Uma mensagem enviada para Alice é codificada com $c = m^e \pmod{n}$
  - Alice decodifica a mensagem com $m = c^d \pmod{n}$
  - Qualquer um pode enviar mensagem codificada para Alice, pois (n, e) é público
  - Mas só Alice pode decifrá-la, poid d é mantido secreto

- Mas como ter certeza da fonte de uma mensagem?
- Bob recebe uma mensagem de Alice, como se certificar que é mesmo de Alice?

- Suponha que Alice queira enviar uma mensagem assinada para Bob
  - Alice "assina" a mensagem codificando-a com $c = m^d \pmod{n}$
  - Quando Bob recebe a mensagem ele pode decodificá-la com $m = c^e \pmod{n}$
  - Bob pode ler m porque (n, e), de Alice, é conhecida publicamente
  - Mas só Alice pode ter gerado a mensagem c, pois só ela conhece d

UFV

Assinatura digital

Alice usa $(n, e) = (2537, 13)$ e $d = 937$. Como enviar a mensagem MEET AT NOON para suas amigas de forma que elas tenham certeza que foi enviada por ela?

- MEET AT NOON = 1204 0419 0019 1314 1413
- Alice calcula $m^{937} (\text{mod } 2537)$ para cada bloco: 0817 0555 1310 2173 1026
- Quando uma de suas amigas recebe essa mensagem, pode calcular $c^{13} (\text{mod } 2537)$ para cada bloco, chegando a MEET AT NOON
- Isto funciona se a mensagem recebida foi criada com $d = 937$, secreta de Alice

UFV

Assinatura digital

Alice usa $(n, e) = (2537, 13)$ e $d = 937$. Como enviar a mensagem MEET AT NOON para suas amigas de forma que elas tenham certeza que foi enviada por ela?

- MEET AT NOON = 1204 0419 0019 1314 1413
- Alice calcula $m^{937} \pmod{2537}$ para cada bloco: 0817 0555 1310 2173 1026
- Quando uma de suas amigas recebe essa mensagem, pode calcular $c^{13} \pmod{2537}$ para cada bloco, chegando a MEET AT NOON
- Isto funciona se a mensagem recebida foi criada com $d = 937$, secreta de Alice

- No exemplo de antes, qualquer um pode ler a mensagem de Alice, não apenas Bob.
- Como Alice pode mandar uma mensagem assinada que só Bob por ler?
  - Assinando com sua chave secreta e codificando com a chave pública de Bob

UFV

Protocolo para decidir chave privada

- Alice e Bob querem conversar por criptografia de chave privada, já que por chave pública é custoso computacionalmente
- Para isso precisam combinar uma chave secreta que só eles devem conhecer
- Como combinar uma chave secreta comum sem se encontrarem secretamente?
- Uma forma é usar o protocolo de troca de chaves descrito pelos americanos Whitfield Diffie e Martin Hellman in 1976
- O protocolo, na verdade, foi criado anos antes pelo britânico Malcolm Williamson, mas isso só foi tornado público no final dos anos 90

UFV

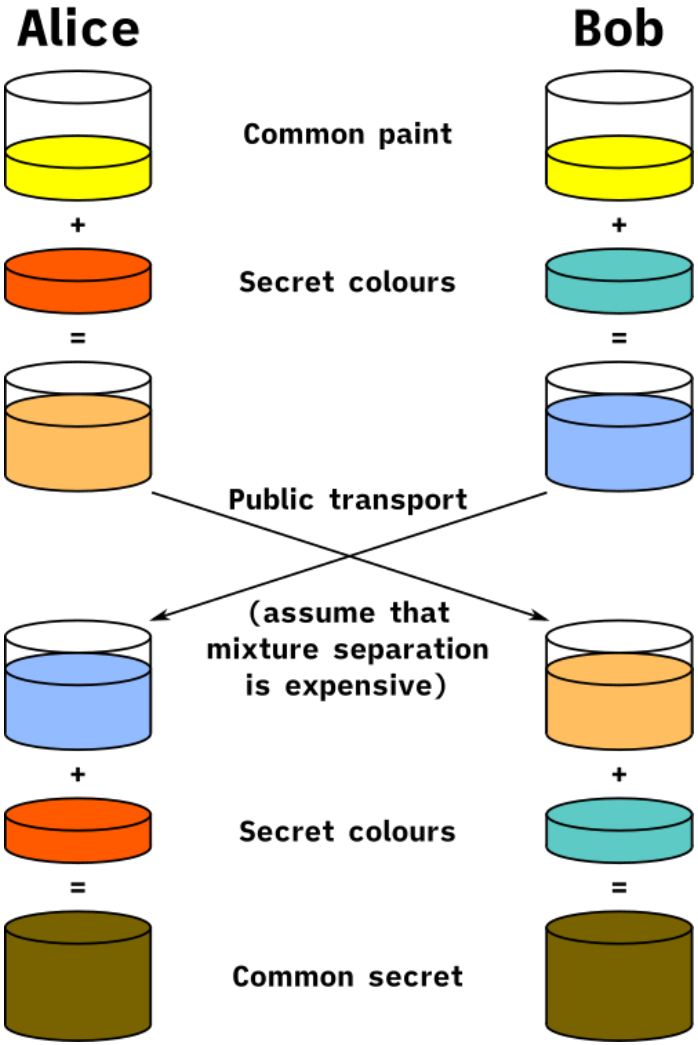
Troca de chaves de Diffie-Hellman

- Suponha que Alice e Bob querem decidir uma chave comum
- O protocolo de troca de chaves de Diffie-Hellman segue os passos em $\mathbb{Z}_p$
  1. Alice e Bob decidem usar um primo p e uma base a (raiz primitiva de p)
  2. Alice escolhe um inteiro secreto k_1 e envia $a^{k_1} \mod p$ para Bob
  3. Bob escolhe um inteiro secreto k_2 e envia $a^{k_2} \mod p$ para Alice
  4. Alice calcula $(a^{k_2})^{k_1} \mod p$
  5. Boba calcula $(a^{k_1})^{k_2} \mod p$
  6. Alice e Bob agora possuem uma chave secreta em comum $a^{k_2\,k_1} = a^{k_1\,k_2} \mod p$

- Segurança do protocolo
  - As mensagens enviadas nos passos 1, 2 e 3 podem ser interceptadas
  - Então alguém pode saber p, a, $a^{k_1} \mod p$ e $a^{k_2} \mod p$
  - Mas a forma conhecida de calcular k_1, k_2 e $a^{k_1\,k_2}$ com isso é resolver logaritmo discreto
  - Isso é inviável se p e a são suficientemente grandes
  - Considerado inquebrável se p tem mais de 300 dígitos e k_1 e k_2 mais de 100

UFV

Troca de chaves de Diffie-Hellman - analogia com cores



Fonte: wikipedia

Segurança

"*Can the reader say what two numbers multiplied together will produce the number 8616460799? I think it unlikely that anyone but myself will ever know.*" - William Stanley Jevons, The Principles of Science, 1874

- Com o aumento do poder computacional, cresceu o tamanho recomendado de p e q
- Mas o aumento do tamanho de n aumenta o tempo de codificar e decodificar
- Deve-se fazer um balanço entre esses fatores de acordo com o número de anos que uma mensagem precisa permanecer secreta
- Pois uma vez que o poder computacional aumenta, pode-se decodificar mensagens antigas
- ⚠ Existem propostas de algoritmos rápidos de fatoração para computação quântica, então quando se tornar prática, outros sistemas de chave pública deverão ser usados

UFV