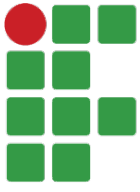
Segurança Computacional

RSA

Ricardo de la Rocha Ladeira
{ricardo.ladeira@ifc.edu.br}



INSTITUTO FEDERAL
Catarinense
Campus Blumenau

RSA

- Algoritmo de **criptografia assimétrica**.

RSA

- Algoritmo de **criptografia assimétrica**.
- **Criptografia assimétrica** (ou de **chave pública**) é aquela que exige um par de chaves para cifragem e decifragem da informação. Uma chave é distribuída livremente (chamada *pública*) e outra é mantida sob sigilo (a chave *privada*). As chaves são unidas matematicamente, de forma que todo conteúdo cifrado por uma é decifrado somente pela outra e vice-versa.

RSA

- Ronald **R**ivest, Adi **S**hamir e Leonard **A**dleman.
- Primeiro algoritmo a permitir criptografia e assinatura digital.

RSA

- Utilizado em funções de criptografia e assinatura digital em diversos protocolos.
  - SSH
  - OpenPGP
  - SSL/TLS
  - ...
- Navegadores utilizam para estabelecer conexões seguras em uma rede insegura (Internet) e validar assinaturas digitais.

RSA

- Está fundamentado na teoria dos números.
- Decifragem depende da fatoração de números, e costuma-se usar números **muito grandes**.
- O cálculo utiliza números primos e módulo (%).

RSA

1. Escolha 2 números primos p e q.
2. Calcule $n = p \times q$.
3. Compute $\varphi(n) = (p-1)(q-1)$.
4. Escolha $e \mid 1 < e < \varphi(n)$, e e $\varphi(n)$ coprimos[1].
5. Compute $d \mid (d \times e) \% \varphi(n) = 1$
6. Chave pública = (e,n)
7. Chave privada = (d,n)
8. Mensagem = $x \rightarrow$ MensagemC = $x^e \% n = y$
9. MensagemC = $y \rightarrow$ Mensagem = $y^d \% n = x$

Note que de Mensagem é possível obter MensagemC e vice versa.
As chaves pública e privada são relacionadas matematicamente.

[1] Dois números naturais a e b são ditos *coprimos*, ou *primos entre si*, se $mdc(a, b) = 1$.

RSA

Tabela: Exemplo de Codificação.

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
10	11	12	13	14	15	16	17	18	19	20	21	22
N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
23	24	25	26	27	28	29	30	31	32	33	34	35

*99 = Espaço em branco.

RSA

- $p = 3$
- $q = 11$

- Quanto vale n?
- Quanto vale $\varphi\ (n)$?

RSA

- $p = 3$
- $q = 11$

- Quanto vale n?
- Quanto vale $\varphi\ (n)$?
- Quanto vale d, se foi escolhido $e = 7$? E por que 7?

RSA

- $p = 3$
- $q = 11$

- Quanto vale n?
- Quanto vale $\varphi\ (n)$?
- Quanto vale d, se foi escolhido $e = 7$? E por que 7?
- Qual é a chave pública?

RSA

- $p = 3$
- $q = 11$

- Quanto vale n?
- Quanto vale $\varphi\ (n)$?
- Quanto vale d, se foi escolhido $e = 7$? E por que 7?
- Qual é a chave pública?
- Qual é a chave privada?

RSA

- $p = 3$
- $q = 11$

- Quanto vale n?
- Quanto vale $\varphi\ (n)$?
- Quanto vale d, se foi escolhido $e = 7$? E por que 7?
- Qual é a chave pública?
- Qual é a chave privada?
- Como cifrar a mensagem “10” com a chave pública?

RSA

- $p = 3$
- $q = 11$

- Quanto vale n?
- Quanto vale $\varphi\ (n)$?
- Quanto vale d, se foi escolhido $e = 7$? E por que 7?
- Qual é a chave pública?
- Qual é a chave privada?
- Como cifrar a mensagem “10” com a chave pública?
- Como decifrar a mensagem “29” com a chave privada?

RSA

- $p = 3$
- $q = 11$
- $n = 33$
- $\varphi(n) = 20$
- $e = 7$
- $d = 3$
- $pub = (7,33)$
- $pri = (3,33)$

RSA

- $M = 10 \rightarrow C = ?$
- $M = 6 \rightarrow C = ?$
- $M = 2 \rightarrow C = ?$
- $M = 4 \rightarrow C = ?$

RSA

- $p = 11$
- $q = 13$
- $n = 143$
- $\varphi\,(n) = 120$
- $e = 7$
- $d = 103$
- $pub = ?$
- $pri = ?$

- Mensagem criptografada: 64 – 119 – 6 – 119 – 102 – 36 – 130 – 36 – 27 – 79 – 23 – 117 – 10. Obter a original!

RSA

- Mensagem criptografada: 64 – 119 – 6 – 119 – 102 – 36 – 130 – 36 – 27 – 79 – 23 – 117 – 10.
- Mensagem original: 25 – 102 – 7 – 102 – 93 – 49 – 91 – 49 – 92 – 118 – 23 – 13 – 10
- Olhando na tabela...

RSA

- Mensagem criptografada: 64 – 119 – 6 – 119 – 102 – 36 – 130 – 36 – 27 – 79 – 23 – 117 – 10.
- Mensagem original: 25 – 102 – 7 – 102 – 93 – 49 – 91 – 49 – 92 – 118 – 23 – 13 – 10
- Olhando na tabela... PARATY É LINDA.

RSA

1. Complete:
   - $e = 7085$
   - $n = 9047$
   - $p = 83$
   - $q = ?$
   - $\varphi(n) = ?$
   - $d = ?$
2. Decifrar a mensagem criptografada: 8655 – 1969 – 1563.

RSA

1. Complete:
   - $e = 7085$
   - $n = 9047$
   - $p = 83$
   - $q = n/p = 9047/83 = 109$
   - $\varphi(n) = ?$
   - $d = ?$

RSA

1. Complete:
   - $e = 7085$
   - $n = 9047$
   - $p = 83$
   - $q = n/p = 9047/83 = 109$
   - $\varphi(n) = 82 * 108 = 8856$
   - $d = ?$

RSA

1. Complete:
   - $e = 7085$
   - $n = 9047$
   - $p = 83$
   - $q = n/p = 9047/83 = 109$
   - $\varphi(n) = 82 * 108 = 8856$
   - $d = 5$ (`rsad.py 7085 8856`)

RSA

1. Complete:
   - $e = 7085$
   - $n = 9047$
   - $p = 83$
   - $q = n/p = 9047/83 = 109$
   - $\varphi(n) = 82 * 108 = 8856$
   - $d = 5$ (`rsad.py 7085 8856`)
2. Decifrar a mensagem criptografada: 8655 – 1969 – 1563.
   - $8655^5 \ \% \ 9047 = 2930 =$ TU
   - $1969^5 \ \% \ 9047 = 1220 =$ CK
   - $1563^5 \ \% \ 9047 = 1427 =$ ER
   - TUCKER

RSA

1. Complete:
   - $p = 127$
   - $q = 211$
   - $e = 4811$
   - $n = 26797$
   - $\varphi(n) = 26460$
   - $d = ?$
2. Decifrar a mensagem criptografada: 17523 – 9183

RSA

1. Complete:
   - $p = 127$
   - $q = 211$
   - $e = 4811$
   - $n = 26797$
   - $\varphi(n) = 26460$
   - $d = 11$ (`rsad.py 4811 26460`)
2. Decifrar a mensagem criptografada: 17523 – 9183
   - 17523^{11} % $26797 = 272$
   - 9183^{11} % $26797 = 810$
   - $272810 \rightarrow 27 - 28 - 10 \rightarrow$ RSA

RSA

- Quando o RSA não é seguro?

RSA

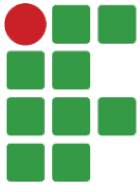
- Quando o RSA não é seguro?
  - Quando n é pequeno.
  - Quando d é pequeno (e é, tipicamente, 3 ou **65537**).
  - Quando e e d são iguais.

- Link interessante: `https://en.wikipedia.org/wiki/RSA_Factoring_Challenge`

Segurança Computacional

RSA

Ricardo de la Rocha Ladeira
{ricardo.ladeira@ifc.edu.br}



INSTITUTO FEDERAL
Catarinense
Campus Blumenau