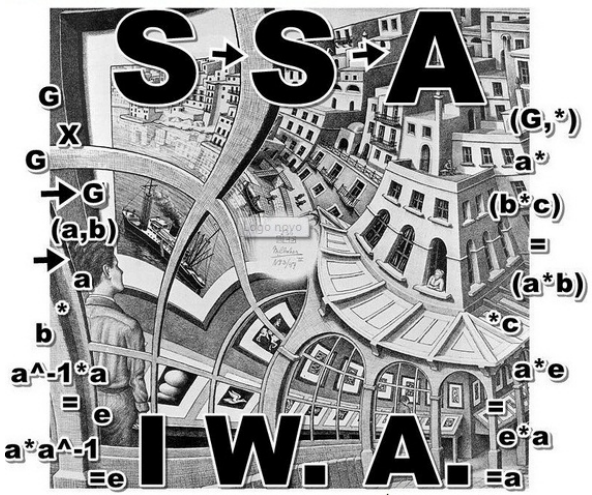
Desvendando os mistérios do criptossistema RSA

Grasiele Cristiane Jorge

Pós-Doc - IMECC - UNICAMP



- A internet tornou-se indispensável no nosso dia a dia (emails, redes sociais, fotos, compras, transações bancárias, ...)

- Como garantir a privacidade das informações trocadas via internet?

- Como garantir a privacidade das informações trocadas via internet?

- O objetivo deste minicurso é entender um método criptográfico que atualmente vem sendo utilizado para proteger informações.

Um pouco de história...

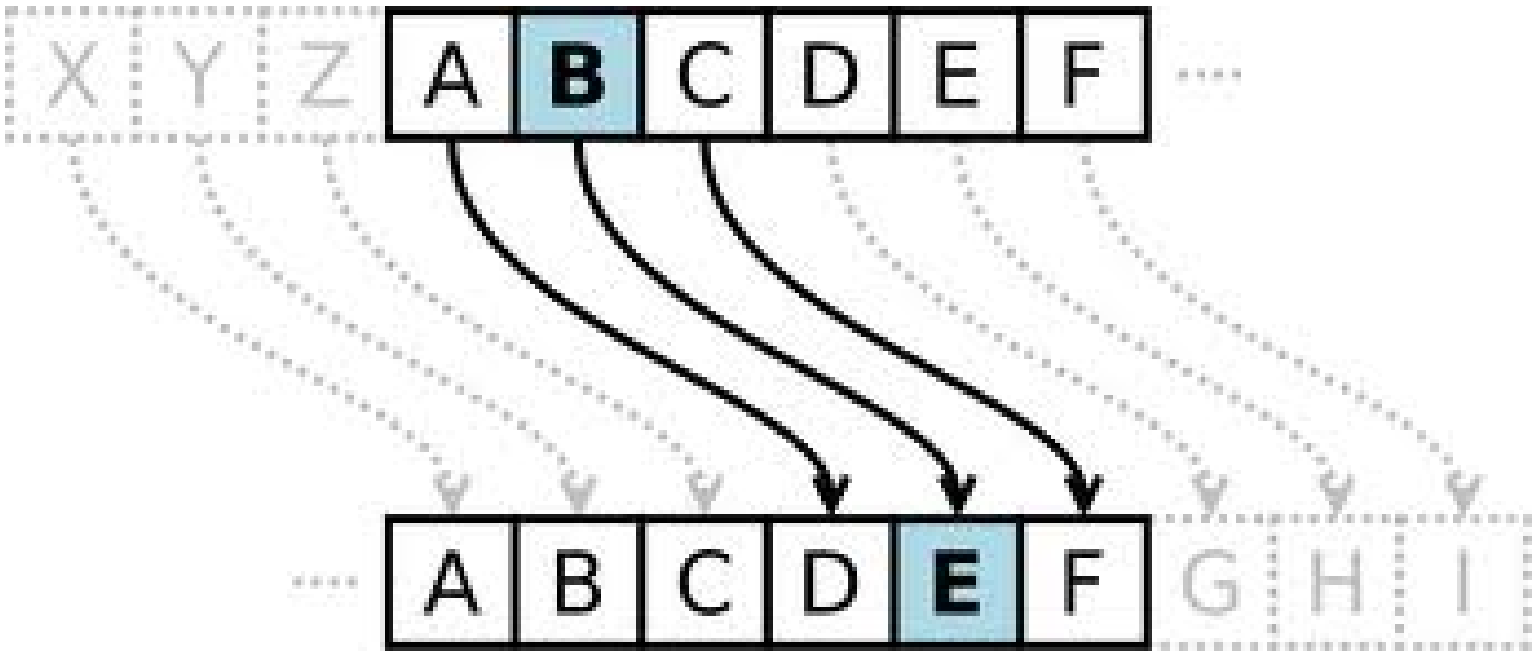
- Desde os tempos remotos o homem vem desenvolvendo e utilizando técnicas que possibilitam a troca de mensagens secretas que podem ser facilmente interpretadas e lidas pelo receptor autorizado mas dificilmente por aqueles que a interceptam sem autorização do remetente ou destinatário.

Um pouco de história...

- Desde os tempos remotos o homem vem desenvolvendo e utilizando técnicas que possibilitam a troca de mensagens secretas que podem ser facilmente interpretadas e lidas pelo receptor autorizado mas dificilmente por aqueles que a interceptam sem autorização do remetente ou destinatário.
- Muitos **amantes** e **revolucionários** perderam a vida por usarem métodos que se mostraram muito **frágeis**, permitindo a fácil **decodificação** das mensagens por **pessoas não autorizadas**.

Alguns exemplos

- **Cifrário de César**: Júlio César utilizava um código para se comunicar com seus generais.



Alguns exemplos

a	b	c	d	e	f	g	h	i	j	k	l	m
$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$
D	E	F	G	H	I	J	K	L	M	N	O	P

n	o	p	q	r	s	t	u	v	w	x	y	z
$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$
Q	R	S	T	U	V	W	X	Y	Z	A	B	C

- criptografia $\Leftrightarrow$ FULSWRJUDLD
- Os generais tinham pré conhecimento do código e conseguiam decodificar facilmente as mensagens.

Alguns exemplos

- Utilizando permutações das letras do alfabeto conseguimos obter $26! = 403.291.461.126.605.635.584.000.000$ códigos.

Alguns exemplos

- Utilizando permutações das letras do alfabeto conseguimos obter $26! = 403.291.461.126.605.635.584.000.000$ códigos.
- A desvantagem em utilizar essa forma de criptossistema é que o código deve ser previamente combinado entre as partes.

Alguns exemplos

- **Enigma**: Máquina utilizada na segunda guerra mundial pelos alemães que podia ser configurada de 15.896.255.521.782.636.000 maneiras diferentes.

Alguns exemplos

- Durante a Segunda Guerra Mundial, as máquinas Enigma foram usadas por praticamente todas as comunicações de rádio alemãs.
- O fim da guerra se deu devido a descoberta de como eram gerados os códigos da Enigma.

Alguns exemplos

- Não bastava, no entanto, decifrar todas as comunicações secretas do inimigo: era necessário fazê-lo de forma a que ele o ignorasse.
- A destruição de cada navio alemão do qual a posição fosse conhecida era precedida do envio de um avião de reconhecimento que sobrevoava o local de forma que parecesse acidental. Este fazia-se ver com nitidez, e o ataque podia então ser feito sem alertar o inimigo.

A matemática oculta da cifra de César

- Seja f uma função que leva cada letra do alfabeto na letra codificada:

$$\boxed{f(a) = D,\ f(b) = E,\ \ldots,\ f(w) = Z,\ f(x) = A \text{ e } f(z) = C.}$$

A matemática oculta da cifra de César

- Seja f uma função que leva cada letra do alfabeto na letra codificada:

$$f(a) = D,\ f(b) = E,\ \ldots,\ f(w) = Z,\ f(x) = A \text{ e } f(z) = C.$$

- Para cada letra associamos um número:

a	b	c	d	$\cdots$	w	x	y	z
$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\vdots$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$
0	1	2	3	$\cdots$	22	23	24	25

A matemática oculta da cifra de César

a	b	c	d	$\cdots$	w	x	y	z
$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\vdots$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$
0	1	2	3	$\cdots$	22	23	24	25

A matemática oculta da cifra de César

a	b	c	d	$\cdots$	w	x	y	z
$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\vdots$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$
0	1	2	3	$\cdots$	22	23	24	25

$f(0) = 0 + 3$

A matemática oculta da cifra de César

a	b	c	d	$\cdots$	w	x	y	z
$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\vdots$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$
0	1	2	3	$\cdots$	22	23	24	25

$f(0) = 0 + 3$

$f(1) = 1 + 3 = 4$

A matemática oculta da cifra de César

a	b	c	d	$\cdots$	w	x	y	z
$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\vdots$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$
0	1	2	3	$\cdots$	22	23	24	25

$f(0) = 0 + 3$

$f(1) = 1 + 3 = 4$

$\vdots$

A matemática oculta da cifra de César

a	b	c	d	$\cdots$	w	x	y	z
$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\vdots$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$
0	1	2	3	$\cdots$	22	23	24	25

$$f(0) = 0 + 3$$

$$f(1) = 1 + 3 = 4$$

$$\vdots$$

$$f(22) = 22 + 3 = 25$$

A matemática oculta da cifra de César

a	b	c	d	$\cdots$	w	x	y	z
$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\vdots$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$
0	1	2	3	$\cdots$	22	23	24	25

$f(0) = 0 + 3$

$f(1) = 1 + 3 = 4$

$\vdots$

$f(22) = 22 + 3 = 25$

$f(23) = 23 + 3 = 26?$

A matemática oculta da cifra de César

a	b	c	d	$\cdots$	w	x	y	z
$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\vdots$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$
0	1	2	3	$\cdots$	22	23	24	25

$$f(0) = 0 + 3$$

$$f(1) = 1 + 3 = 4$$

$$\vdots$$

$$f(22) = 22 + 3 = 25$$

$$f(23) = 23 + 3 = 26 - 26 = 0$$

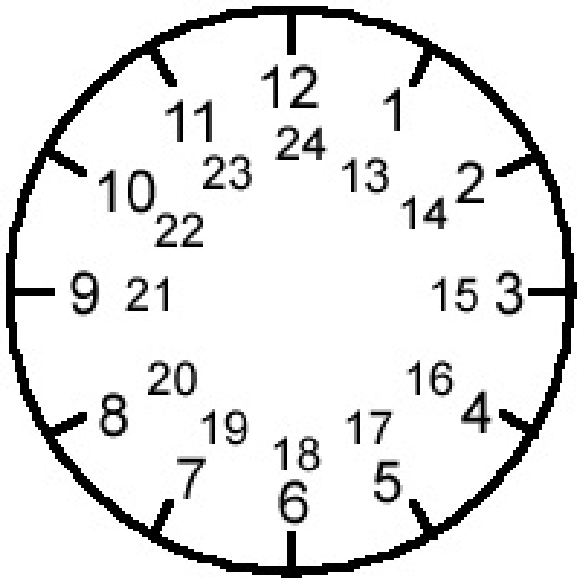
A matemática oculta da cifra de César

$$f(x) = x + 3 \ (mod\ 26)$$

$$\Downarrow$$

$$\mathbb{Z}_{26} = \{\overline{0}, \overline{1}, \cdots, \overline{25}\}$$

Exemplos do dia a dia



1986

	JULHO	AGOSTO	SETEMBRO
S	7 14 21 28	4 11 18 25	1 8 15 22 29
T	1 8 15 22 29	5 12 19 26	2 9 16 23 30
Q	2 9 16 23 30	6 13 20 27	3 10 17 24
Q	3 10 17 24 31	7 14 21 29	4 11 18 25
S	4 11 18 25	1 8 F 22 29	5 12 19 26
S	5 12 19 26	2 9 16 23 30	6 13 20 27
D	6 13 20 27	3 10 17 24 31	7 14 21 28

	OUTUBRO	NOVEMBRO	DEZEMBRO
S	6 13 20 27	3 10 17 24	F F 15 22 29
T	7 14 21 28	4 11 18 25	2 9 16 23 30
Q	1 8 15 22 29	5 12 19 26	3 10 17 24 31
Q	2 9 16 23 30	6 13 20 27	4 11 18 N
S	3 10 17 24 31	7 14 21 28	5 12 19 26
S	4 11 18 25	F 8 15 22 29	6 13 20 27
D	F 12 19 26	2 9 16 23 30	7 14 21 28

Nosso ambiente de trabalho

Anel dos inteiros módulo n

$$\boxed{\mathbb{Z}_n = \{\overline{0}, \overline{1}, \cdots, \overline{n-1}\}}$$

- $\overline{a} \equiv \overline{b}\,(mod\ n)$ se, e somente se, $a = b + qn$ para algum $q \in \mathbb{Z}$.
- Por exemplo $\overline{14} \equiv \overline{6} \equiv \overline{2}\,(mod\ 4)$

Anel dos inteiros módulo n

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \cdots, \overline{n-1}\}$$

Soma e produto de classes

Anel dos inteiros módulo n

$$\boxed{\mathbb{Z}_n = \{\overline{0}, \overline{1}, \cdots, \overline{n-1}\}}$$

- Adição: $\overline{a} + \overline{b} = \overline{a+b}$
- Multiplicação: $\overline{a}.\overline{b} = \overline{a.b}$

$\mathbb{Z}_5$

$+$	**0**	**1**	**2**	**3**	**4**
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$*$	**0**	**1**	**2**	**3**	**4**
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Grupo aditivo abeliano

$$\boxed{\mathbb{Z}_n = \{\overline{0}, \overline{1}, \cdots, \overline{n-1}\}}$$

- Elemento neutro: $\overline{0}$
- Associativa: $(\overline{a} + \overline{b}) + \overline{c} = \overline{a} + (\overline{b} + \overline{c})$
- Elemento inverso: $-\overline{a} = \overline{n - a}$
- Comutativa: $\overline{a} + \overline{b} = \overline{b} + \overline{a}$

Inverso Multiplicativo

$$\boxed{\mathbb{Z}_n = \{\overline{0}, \overline{1}, \cdots, \overline{n-1}\}}$$

- Elemento neutro da multiplicação: $\overline{1}$
- Associativa: $(\overline{a}.\overline{b}).\overline{c} = \overline{a}.(\overline{b}.\overline{c})$

Inverso Multiplicativo

$$\boxed{\mathbb{Z}_n = \{\overline{0}, \overline{1}, \cdots, \overline{n-1}\}}$$

- Elemento neutro da multiplicação: $\overline{1}$
- Associativa: $(\overline{a}.\overline{b}).\overline{c} = \overline{a}.(\overline{b}.\overline{c})$
- Pergunta: Dado $\overline{a} \in \mathbb{Z}_n$, existe $\overline{b} \in \mathbb{Z}_n$ tal que $\overline{a}.\overline{b} = \overline{1}$?

Inverso Multiplicativo

$$\boxed{\mathbb{Z}_n = \{\overline{0}, \overline{1}, \cdots, \overline{n-1}\}}$$

- Elemento neutro da multiplicação: $\overline{1}$
- Associativa: $(\overline{a}.\overline{b}).\overline{c} = \overline{a}.(\overline{b}.\overline{c})$
- Pergunta: Dado $\overline{a} \in \mathbb{Z}_n$, existe $\overline{b} \in \mathbb{Z}_n$ tal que $\overline{a}.\overline{b} = \overline{1}$?
- Exemplo: Em $\mathbb{Z}_6$, qual é o inverso multiplicativo de $\overline{3}$?

Inverso Multiplicativo

$$\boxed{\mathbb{Z}_n = \{\overline{0}, \overline{1}, \cdots, \overline{n-1}\}}$$

- Elemento neutro da multiplicação: $\overline{1}$
- Associativa: $(\overline{a}.\overline{b}).\overline{c} = \overline{a}.(\overline{b}.\overline{c})$
- Pergunta: Dado $\overline{a} \in \mathbb{Z}_n$, existe $\overline{b} \in \mathbb{Z}_n$ tal que $\overline{a}.\overline{b} = \overline{1}$?
- Exemplo: Em $\mathbb{Z}_6$, qual é o inverso multiplicativo de $\overline{3}$?
- $\overline{3}.\overline{0} = \overline{0}$, $\overline{3}.\overline{1} = \overline{3}$, $\overline{3}.\overline{2} = \overline{0}$, $\overline{3}.\overline{3} = \overline{3}$, $\overline{3}.\overline{4} = \overline{0}$ e $\overline{3}.\overline{5} = \overline{3}$.
- $\overline{3}$ não possui inverso multiplicativo em $\mathbb{Z}_6$.

Inverso Multiplicativo

- Exemplo: Em $\mathbb{Z}_{10}$, qual é o inverso multiplicativo de $\overline{3}$?

Inverso Multiplicativo

- Exemplo: Em $\mathbb{Z}_{10}$, qual é o inverso multiplicativo de $\overline{3}$?
- $\overline{3}.\overline{2} = \overline{6}$, $\overline{3}.\overline{3} = \overline{9}$, $\overline{3}.\overline{4} = \overline{2}$, $\overline{3}.\overline{5} = \overline{5}$, $\overline{3}.\overline{6} = \overline{8}$, $\overline{3}.\overline{7} = \overline{1}$
- $\overline{7}$ é o inverso multiplicativo de $\overline{3}$ em $\mathbb{Z}_{10}$.

Inverso Multiplicativo

- Exemplo: Em $\mathbb{Z}_{10}$, qual é o inverso multiplicativo de $\overline{3}$?
- $\overline{3}.\overline{2} = \overline{6}$, $\overline{3}.\overline{3} = \overline{9}$, $\overline{3}.\overline{4} = \overline{2}$, $\overline{3}.\overline{5} = \overline{5}$, $\overline{3}.\overline{6} = \overline{8}$, $\overline{3}.\overline{7} = \overline{1}$
- $\overline{7}$ é o inverso multiplicativo de $\overline{3}$ em $\mathbb{Z}_{10}$.

- Exemplo: Em $\mathbb{Z}_7$, qual é o inverso multiplicativo de $\overline{3}$?

Inverso Multiplicativo

- Exemplo: Em $\mathbb{Z}_{10}$, qual é o inverso multiplicativo de $\overline{3}$?
- $\overline{3}.\overline{2} = \overline{6}$, $\overline{3}.\overline{3} = \overline{9}$, $\overline{3}.\overline{4} = \overline{2}$, $\overline{3}.\overline{5} = \overline{5}$, $\overline{3}.\overline{6} = \overline{8}$, $\overline{3}.\overline{7} = \overline{1}$
- $\overline{7}$ é o inverso multiplicativo de $\overline{3}$ em $\mathbb{Z}_{10}$.

- Exemplo: Em $\mathbb{Z}_7$, qual é o inverso multiplicativo de $\overline{3}$?
- $\overline{3}.\overline{2} = \overline{6}$, $\overline{3}.\overline{3} = \overline{2}$, $\overline{3}.\overline{4} = \overline{5}$, $\overline{3}.\overline{5} = \overline{1}$
- $\overline{5}$ é o inverso multiplicativo de $\overline{3}$ em $\mathbb{Z}_7$.

Inverso Multiplicativo

Proposição

Um elemento $\overline{a} \in \mathbb{Z}_n$ possui inverso multiplicativo se, e somente se,

$mdc(a, n) = 1$.

Inverso Multiplicativo

Proposição

Um elemento $\overline{a} \in \mathbb{Z}_n$ possui inverso multiplicativo se, e somente se, $mdc(a, n) = 1$.

$$\mathbb{Z}_n{}^* = \{\overline{x} \in \mathbb{Z}_n \text{ tal que } mdc(x, n) = 1\}$$

Inverso Multiplicativo

Proposição

Um elemento $\overline{a} \in \mathbb{Z}_n$ possui inverso multiplicativo se, e somente se,

$mdc(a, n) = 1$.

$$\mathbb{Z}_n{}^* = \{\overline{x} \in \mathbb{Z}_n \text{ tal que } mdc(x, n) = 1\}$$

Exemplo

$$\mathbb{Z}_{12} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}, \overline{10}, \overline{11}\}$$

Inverso Multiplicativo

Proposição

Um elemento $\overline{a} \in \mathbb{Z}_n$ possui inverso multiplicativo se, e somente se,

$mdc(a, n) = 1$.

$$\mathbb{Z}_n{}^* = \{\overline{x} \in \mathbb{Z}_n \text{ tal que } mdc(x, n) = 1\}$$

Exemplo

$$\mathbb{Z}_{12} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}, \overline{10}, \overline{11}\}$$

Inverso Multiplicativo

Proposição

Um elemento $\overline{a} \in \mathbb{Z}_n$ possui inverso multiplicativo se, e somente se,

$mdc(a, n) = 1$.

$$\mathbb{Z}_n{}^* = \{\overline{x} \in \mathbb{Z}_n \text{ tal que } mdc(x, n) = 1\}$$

Exemplo

$$\mathbb{Z}_{12}{}^* = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}$$

Proposição

$\mathbb{Z}_n{}^*$ é um grupo abeliano multiplicativo.

$$\mathbb{Z}_p{}^* = \{\overline{1}, \overline{2}, \cdots, \overline{p-1}\}$$

A função ϕ de Euler

Seja $\phi(n)$ a função que conta o número de inteiros entre 1 e $n-1$ que são primos com n.

A função ϕ de Euler

Seja $\phi(n)$ a função que conta o número de inteiros entre 1 e $n-1$ que são primos com n.

$$\boxed{\phi(n) = |\mathbb{Z}_n{}^*|}$$

A função ϕ de Euler

Seja $\phi(n)$ a função que conta o número de inteiros entre 1 e $n-1$ que são primos com n.

$$\boxed{\phi(n) = |\mathbb{Z}_n{}^*|}$$

Proposição

Se p é primo, então

$$\phi(p) = |\mathbb{Z}_p{}^*| = p - 1$$

Teorema de Fermat

Seja p um número primo e a um inteiro, então

$$\overline{a}^{(p-1)} \equiv \overline{1} \ (mod\ p)$$

Pierre de Fermat

Teorema de Fermat

Exemplo

$\mathbb{Z}_7{}^* = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}$

Teorema de Fermat

Exemplo

$\mathbb{Z}_7{}^* = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}$

$\overline{1}^6 = \overline{1} \equiv \overline{1}\ (mod\ 7)$

$\overline{2}^6 = \overline{64} \equiv \overline{1}\ (mod\ 7)$

$\overline{3}^6 = \overline{729} \equiv \overline{1}\ (mod\ 7)$

$\overline{4}^6 = \overline{4096} \equiv \overline{1}\ (mod\ 7)$

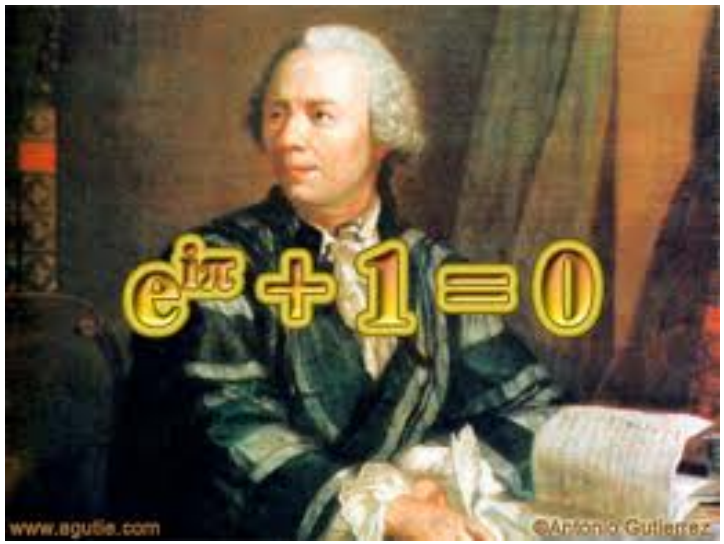
$\overline{5}^6 = \overline{15625} \equiv \overline{1}\ (mod\ 7)$

$\overline{6}^6 = \overline{46656} \equiv \overline{1}\ (mod\ 7)$

Teorema de Euler

Sejam n e a inteiros. Se $mdc(a, n) = 1$, então

$$\overline{a}^{\phi(n)} \equiv \overline{1} \ (mod\ n)$$



Teorema de Euler

Exemplo

$\mathbb{Z}_{12}{}^{*} = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}$

Teorema de Euler

Exemplo

$\mathbb{Z}_{12}{}^{*} = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}$

$\overline{1}^{4} \equiv \overline{1}\ (mod\ 12)$

$\overline{5}^{4} \equiv \overline{1}\ (mod\ 12)$

$\overline{7}^{4} \equiv \overline{1}\ (mod\ 12)$

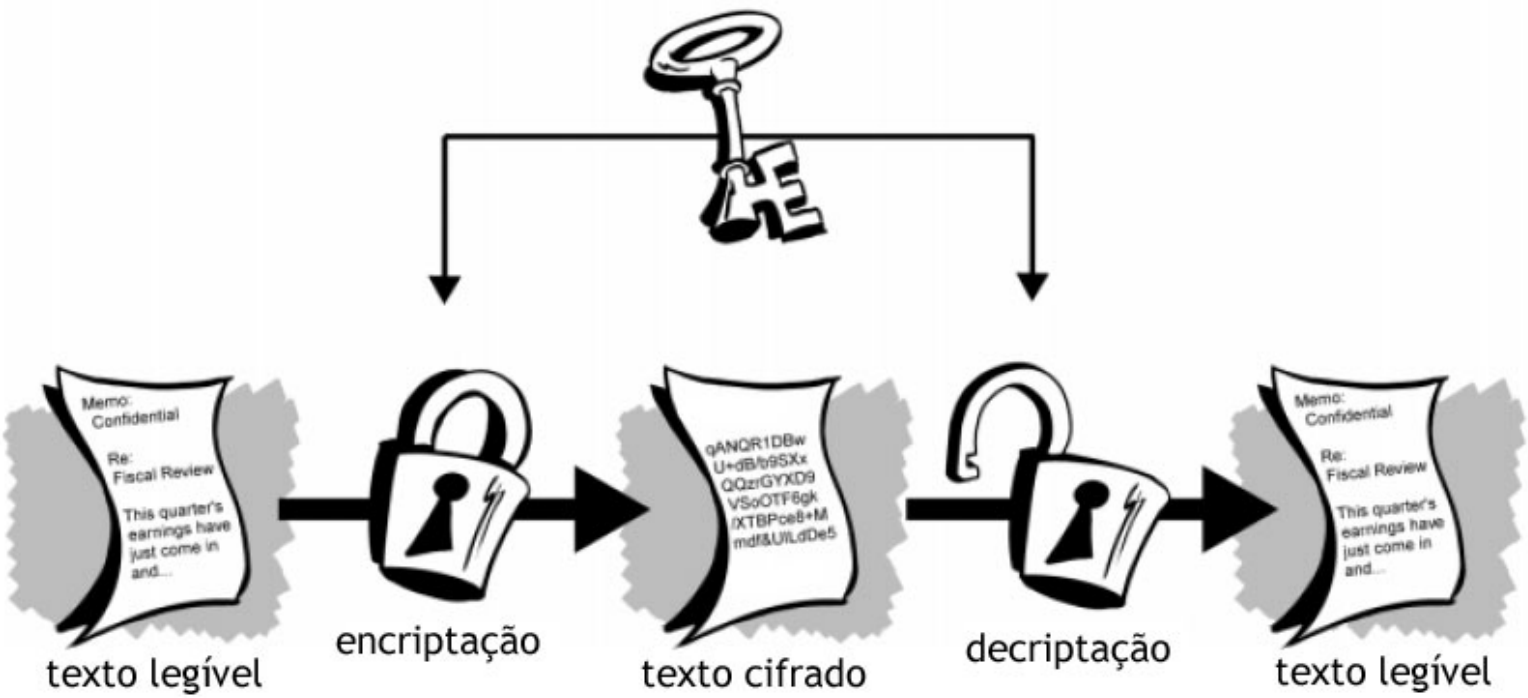
$\overline{11}^{4} \equiv \overline{1}\ (mod\ 12)$

Criptografia de Chave publica

Criptografia de Chave publica

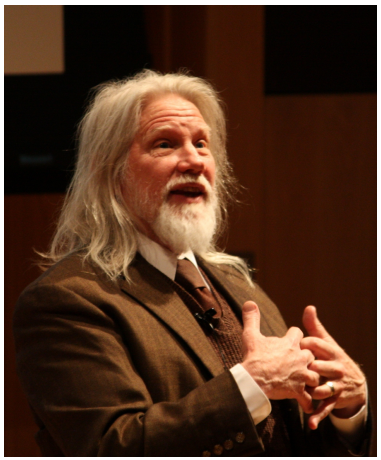
- A segunda guerra mundial terminou em 1945.
- A partir daí começam a surgir os primeiros computadores.
- A década de 70 foi um marco na história da criptografia.

Criptossistemas simétricos

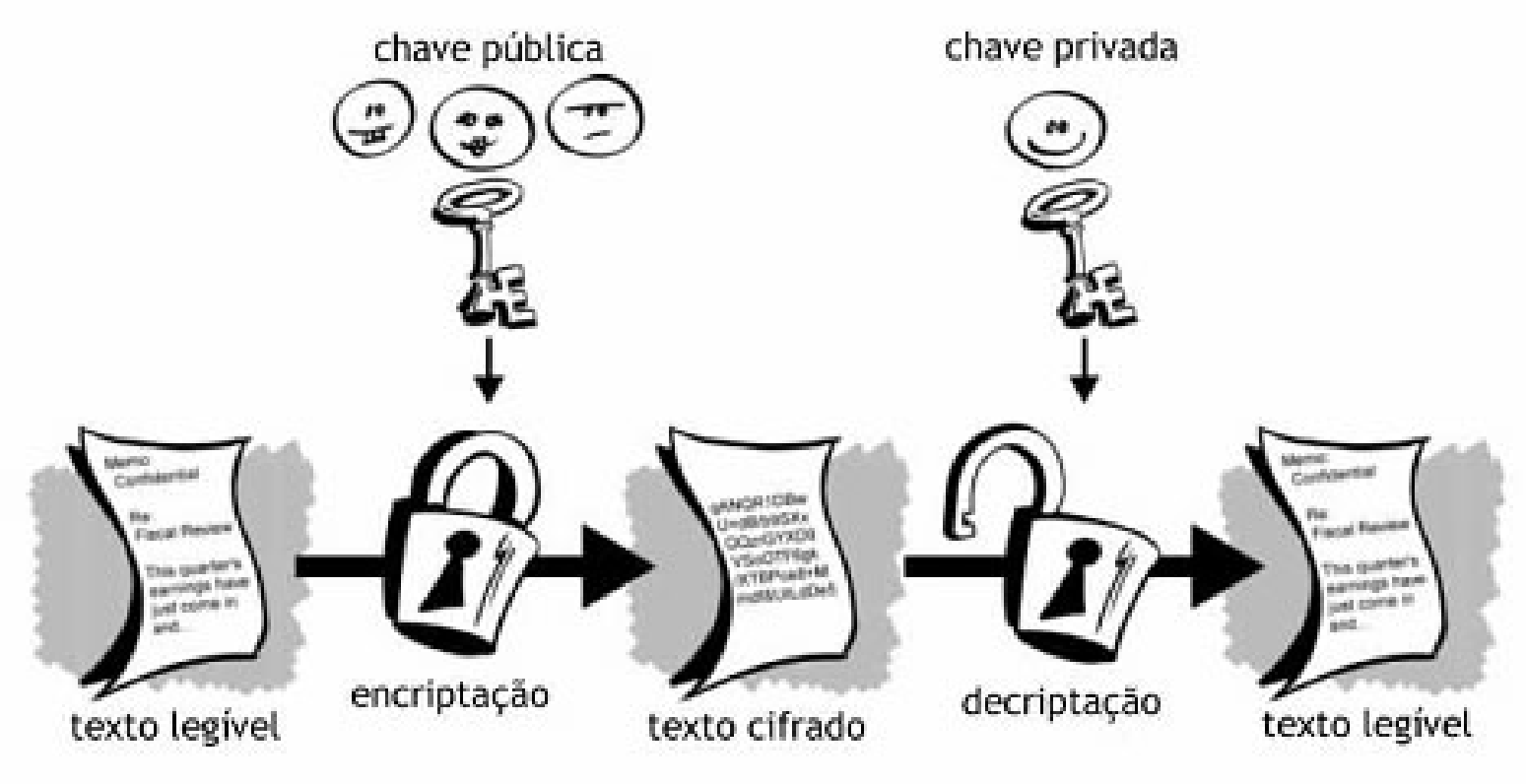


Criptografia de Chave publica

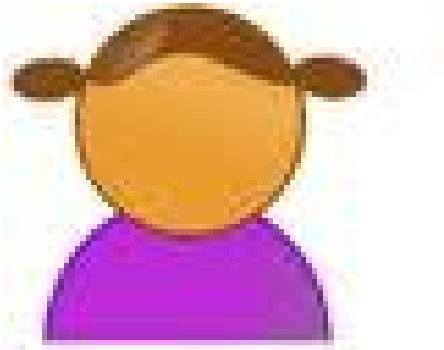
- Em 1975, Whitfied Diffie pensou um modelo de criptossistema em que as partes não precisassem combinar o código antes.
- Tal sistema criptográfico se baseia em um par de chaves:
  - uma chave para embaralhar um texto claro
  - uma chave para desembaralhar o texto cifrado.

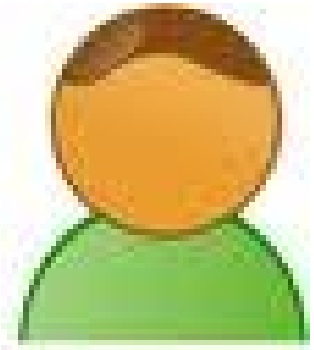


Criptossistemas assisimétricos



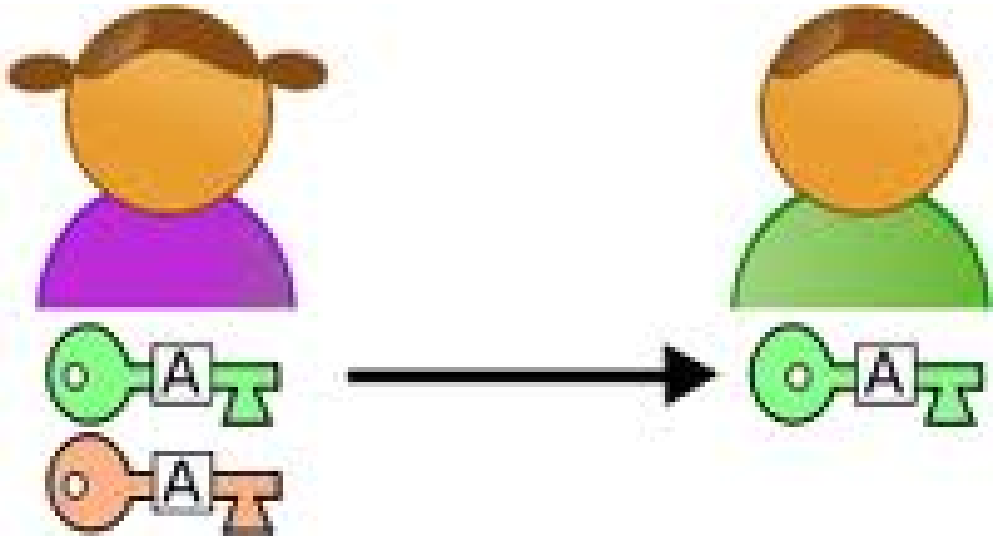
Criptografia de Chave pública

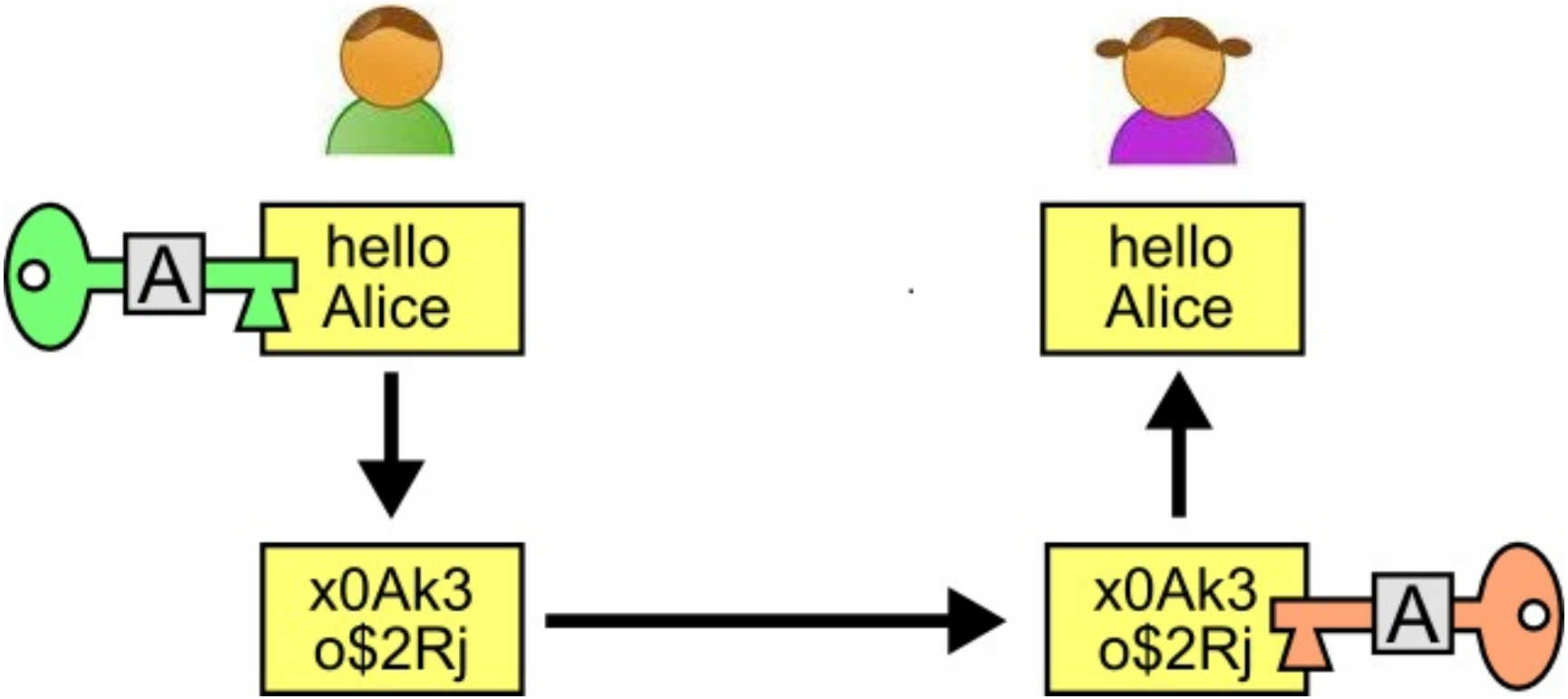




Alice	Bob
C_A = chave pública de Alice	C_B = chave pública de Bob
D_A = chave privada de Alice	D_B = chave privada de Bob

As chaves públicas são divulgadas de um para outro (e pra quem mais quiser saber).



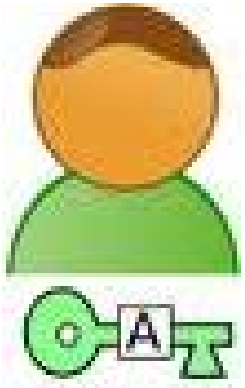

A
hello
Alice
hello
Alice
x0Ak3
o$2Rj
x0Ak3
o$2Rj
A

Transmissão de Informações

- Bob quer enviar a mensagem P para Alice

Transmissão de Informações

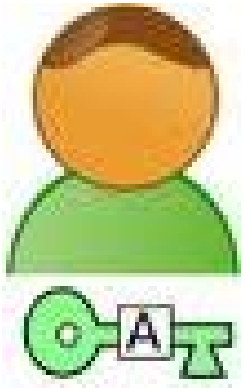
- Bob quer enviar a mensagem P para Alice
- Bob vai utilizar a chave pública C_A de Alice



e com ela vai cifrar a mensagem, enviando para Alice a mensagem cifrada

Transmissão de Informações

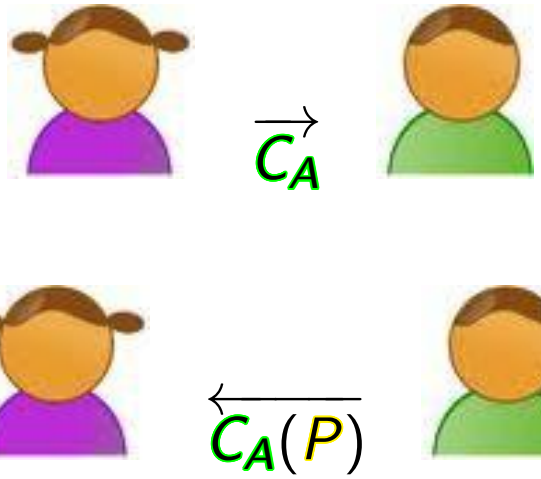
- Bob quer enviar a mensagem P para Alice
- Bob vai utilizar a chave pública C_A de Alice



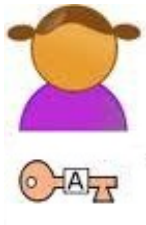
e com ela vai cifrar a mensagem, enviando para Alice a mensagem cifrada

$$C_A(P)$$

Transmissão de Informações



Alice utiliza sua chave privada para decodificar a mensagem



$$D_A(C_A(P)) = P$$

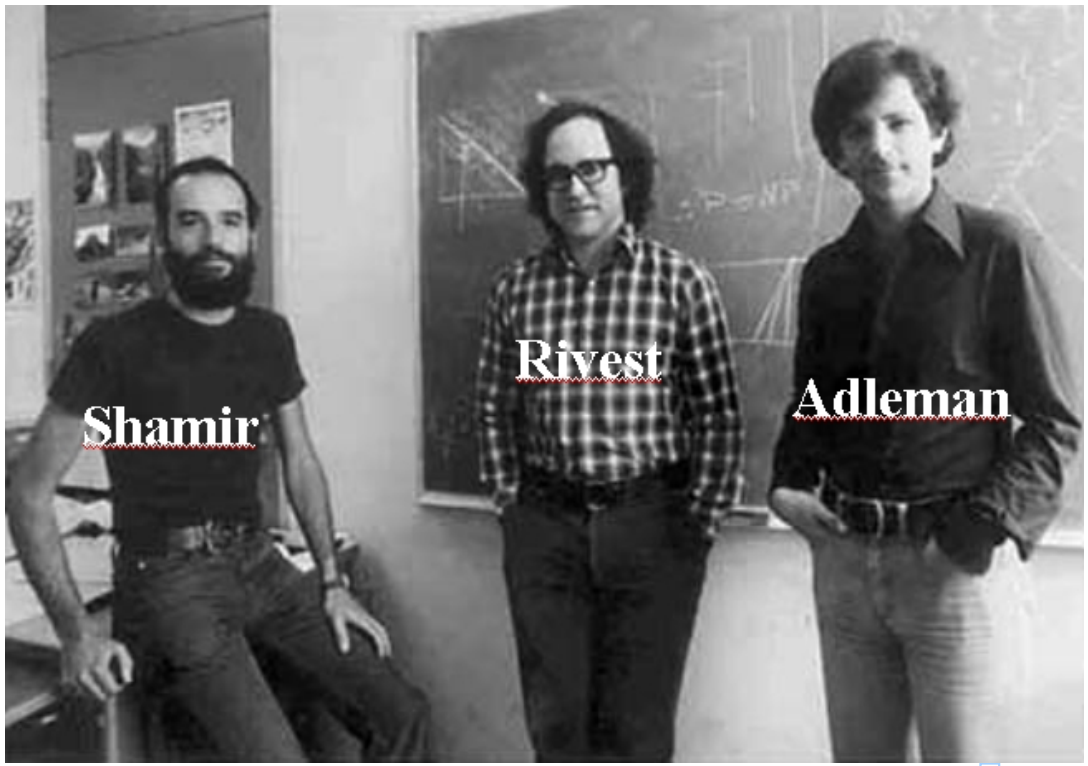
O que seriam essas chaves? Quais códigos devemos usar?

O que seriam essas chaves? Quais códigos devemos usar?

- Diffie expôs suas ideias em 1975.
- Somente em 1977 , três pesquisadores do MIT criaram um esquema que implementa um sistema criptográfico assimétrico, o **RSA**.

O que seriam essas chaves? Quais códigos devemos usar?

- Diffie expôs suas ideias em 1975.
- Somente em 1977 , três pesquisadores do MIT criaram um esquema que implementa um sistema criptográfico assimétrico, o **RSA**.



De $D_A(C_A(P)) = P$ percebemos que a ideia é encontrar duas funções tais que uma seja o inverso da outra e de tal forma que conhecendo uma não se conheça a outra.

Na verdade, vamos precisar de uma família de funções pois cada pessoa vai ter o seu par de chaves.

RSA

Geração de Chaves

- Escolha aleatoriamente dois primos distintos e grandes $p \neq q$

RSA

Geração de Chaves

- Escolha aleatoriamente dois primos distintos e grandes $p \neq q$
- Calcule $n = pq$

RSA

Geração de Chaves

- Escolha aleatoriamente dois primos distintos e grandes $p \neq q$
- Calcule $n = pq$
- Calcule $\phi(n) = \phi(p)\phi(q) = (p-1)(q-1)$

RSA

Geração de Chaves

- Escolha aleatoriamente dois primos distintos e grandes $p \neq q$
- Calcule $n = pq$
- Calcule $\phi(n) = \phi(p)\phi(q) = (p-1)(q-1)$
- Escolha um inteiro e tal que $1 < \text{e} < \phi(n)$ e mdc(e,$\phi(n)$)=1.

RSA

Geração de Chaves

- Escolha aleatoriamente dois primos distintos e grandes $p \neq q$
- Calcule $n = pq$
- Calcule $\phi(n) = \phi(p)\phi(q) = (p-1)(q-1)$
- Escolha um inteiro e tal que $1 < \text{e} < \phi(n)$ e mdc(e,$\phi(n)$)=1.

  (isto significa que $\text{e} \in \mathbb{Z}^*_{\phi(n)}$)

RSA

Geração de Chaves

- Escolha aleatoriamente dois primos distintos e grandes $p \neq q$
- Calcule $n = pq$
- Calcule $\phi(n) = \phi(p)\phi(q) = (p-1)(q-1)$
- Escolha um inteiro e tal que $1 < \text{e} < \phi(n)$ e mdc(e,$\phi(n)$)=1.

  (isto significa que $\text{e} \in \mathbb{Z}^*_{\phi(n)}$)
- Calcule o inteiro d tal que $1 < d < \phi(n)$ e $\text{de} \equiv 1 \ (mod\ \phi(n))$

RSA

Geração de Chaves

- Escolha aleatoriamente dois primos distintos e grandes $p \neq q$
- Calcule $n = pq$
- Calcule $\phi(n) = \phi(p)\phi(q) = (p-1)(q-1)$
- Escolha um inteiro e tal que $1 < e < \phi(n)$ e mdc(e,$\phi(n)$)=1.

  (isto significa que $e \in \mathbb{Z}^*_{\phi(n)}$)
- Calcule o inteiro d tal que $1 < d < \phi(n)$ e $de \equiv 1 \ (mod\ \phi(n))$

$$\mathbb{Z}^*_{\phi(n)} = \{\overline{1}, \cdots, \overline{e}, \cdots, \overline{d}, \cdots\}$$

RSA

- Chave Pública: O par (e,n)
- Chave Privada: O par (d,n)

RSA

- Suponha que Bob quer enviar a mensagem P para Alice.

RSA

- Suponha que Bob quer enviar a mensagem P para Alice.
- Alice envia sua chave pública $C_A = (e, n)$

RSA

- Suponha que Bob quer enviar a mensagem P para Alice.
- Alice envia sua chave pública $C_A = (e, n)$
- Bob calcula

$$C \equiv P^e \ (mod\ n)$$

e envia C.

RSA

Alice quando recebe a mensagem, calcula

$$C^d \equiv (P^e)^d \equiv P^{ed}$$

RSA

Alice quando recebe a mensagem, calcula

$$C^d \equiv (P^e)^d \equiv P^{ed}$$

Mas,

$$\boxed{de \equiv 1 \ (mod\ \phi(n)) \text{ se, e somente se, } de = 1 + k\phi(n)}$$

RSA

Alice quando recebe a mensagem, calcula

$$C^d \equiv (P^e)^d \equiv P^{ed}$$

Mas,

$$\boxed{de \equiv 1 \ (mod\ \phi(n)) \text{ se, e somente se, } de = 1 + k\phi(n)}$$

Daí,

$$C^d \equiv (P^e)^d \equiv P^{ed} \equiv P^{1+k\phi(n)}$$

RSA

Alice quando recebe a mensagem, calcula

$$C^d \equiv (P^e)^d \equiv P^{ed}$$

Mas,

$$\boxed{de \equiv 1 \ (mod\ \phi(n)) \text{ se, e somente se, } de = 1 + k\phi(n)}$$

Daí,

$$C^d \equiv (P^e)^d \equiv P^{ed} \equiv P^{1+k\phi(n)}$$

Pelo Teorema de Euler:

$$\boxed{\text{se mdc(P,n)=1, então } P^{\phi(n)} \equiv 1 \text{ (mod n)}}$$

RSA

Alice quando recebe a mensagem, calcula

$$C^d \equiv (P^e)^d \equiv P^{ed}$$

Mas,

$$\boxed{de \equiv 1 \ (mod\ \phi(n)) \text{ se, e somente se, } de = 1 + k\phi(n)}$$

Daí,

$$C^d \equiv (P^e)^d \equiv P^{ed} \equiv P^{1+k\phi(n)}$$

Pelo Teorema de Euler:

$$\boxed{\text{se mdc(P,n)=1, então } P^{\phi(n)} \equiv 1 \text{ (mod n)}}$$

Portanto,

$$C^d \equiv P^{ed} \equiv P^{1+k\phi(n)} \equiv P, \text{ se } mdc(P, n) = 1$$

Antes de iniciarmos a geração de chaves já conhecemos os tamanhos possíveis de P e tomamos n maior do que o maior P possível.

$mdc(P, n) \neq 1$ se, e somente se, $P = p$ ou $P = q$, o que é muito difícil de acontecer.

- Fatorando n como produto de dois primos distintos, obtém-se $\phi(n) = (p-1)(q-1)$ e com essa fatoração e a chave pública e é possível obter a chave privada $d = e^{-1}, (mod\, \phi(n))$.
- Dado um inteiro n, até o momento NÃO existe um algoritmo computacional capaz de fatorar n como um produto de primos em tempo polinomial.

Encifrando mensagens

- Dado uma mensagem de texto, dividimos a mensagem em blocos de mesmo tamanho.
- O espaço entre as palavras é contado também.
- Cada um destes blocos é transformado em um vetor.
- Aplicamos o RSA neste vetor

Exemplo

- Escolhemos $p = 61$ e $q = 71$

Exemplo

- Escolhemos $p = 61$ e $q = 71$
- $n = p.q = 4331$

Exemplo

- Escolhemos $p = 61$ e $q = 71$
- $n = p.q = 4331$
- $\phi(n) = 60.70 = 4200$

Exemplo

- Escolhemos $p = 61$ e $q = 71$
- $n = p.q = 4331$
- $\phi(n) = 60.70 = 4200$
- Escolhemos e=23 e nossa chave pública fica (23,4331).

Exemplo

- Escolhemos $p = 61$ e $q = 71$
- $n = p.q = 4331$
- $\phi(n) = 60.70 = 4200$
- Escolhemos e=23 e nossa chave pública fica (23,4331).
- Calculamos d = 3287 o inverso de 23 módulo $\phi(n) = 4200$ e nossa chave privada fica (3287,4331).

Exemplo

- Escolhemos $p = 61$ e $q = 71$
- $n = p.q = 4331$
- $\phi(n) = 60.70 = 4200$
- Escolhemos e=23 e nossa chave pública fica (23,4331).
- Calculamos d = 3287 o inverso de 23 módulo $\phi(n) = 4200$ e nossa chave privada fica (3287,4331).
- Seja P=20 um vetor (mensagem encriptada)

Exemplo

- Escolhemos $p = 61$ e $q = 71$
- $n = p.q = 4331$
- $\phi(n) = 60.70 = 4200$
- Escolhemos e=23 e nossa chave pública fica (23,4331).
- Calculamos d = 3287 o inverso de 23 módulo $\phi(n) = 4200$ e nossa chave privada fica (3287,4331).
- Seja P=20 um vetor (mensagem encriptada)
- Bob envia $20^{23}\,(mod\,4331) \equiv 2388\,(mod 4331)$

Exemplo

- Escolhemos $p = 61$ e $q = 71$
- $n = p.q = 4331$
- $\phi(n) = 60.70 = 4200$
- Escolhemos e=23 e nossa chave pública fica (23,4331).
- Calculamos d = 3287 o inverso de 23 módulo $\phi(n) = 4200$ e nossa chave privada fica (3287,4331).
- Seja P=20 um vetor (mensagem encriptada)
- Bob envia $20^{23}\,(mod\,4331) \equiv 2388\,(mod 4331)$
- Fazemos $2388^{3287}\,(mod\,4331) \equiv 20\,(mod\,4331)$ e recuperamos a mensagem inicial.

Segurança

- A tendência, com o passar dos anos, é o aumento do tamanho das chaves.
- Existe um algoritmo AKS para saber se um dado número natural é primo que opera em tempo polinomial.

- Na década de 90, Peter Shor descreveu um algoritmo, que se utilizado em computadores quânticos é capaz de fatorar um inteiro n como produto de números primos em tempo polinomial.

O algoritmo RSA sozinho é seguro?

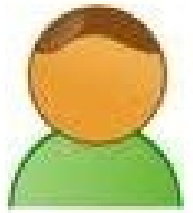
O algoritmo RSA sozinho é seguro?

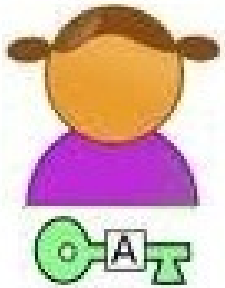
Infelizmente não!

Autenticidade

- Matematicamente falando: o RSA é seguro.
- No entanto, um invasor pode ter acesso a uma mensagem sem quebrar o sistema criptográfico, falsificando a chave pública de uma das partes.

Autenticidade





Autenticidade

- O invasor pode enviar uma chave pública fingindo ser Alice.
- Bob saudoso de sua amiga Alice, manda a mensagem codificada para o invasor.
- O invasor sabe decodificar pois foi ele quem gerou as chaves.

Autenticidade

Como Bob deve proceder para se certificar a chave pública que dizem ser de Alice é de fato de Alice?

Assinatura digital

- Se Bob quer se certificar que a chave C_A é de fato de Alice, ele pede para Alice lhe enviar uma mensagem.

Assinatura digital

- Se Bob quer se certificar que a chave C_A é de fato de Alice, ele pede para Alice lhe enviar uma mensagem.
- Alice envia o par

$$(C_B(P), D_A(S))$$

Assinatura digital

- Se Bob quer se certificar que a chave C_A é de fato de Alice, ele pede para Alice lhe enviar uma mensagem.
- Alice envia o par

$$(C_B(P), D_A(S))$$

- Ao receber este par, Bob usa sua chave secreta D_B para recuperar o texto claro

$$P = D_B(C_B(P))$$

Assinatura digital

- e usa a chave pública de Alice para conferir a assinatura:

$$S = C_A(D_A(S))$$

.

Assinatura digital

- e usa a chave pública de Alice para conferir a assinatura:

$$S = C_A(D_A(S))$$

.

- S e P estão relacionados por uma função conhecida como função de Hash. Se $S = H(P)$, então a assinatura de Alice está correta.

Funções de Hash

- As funções de Hash são funções quase sempre injetoras
- é impossível obter P a partir de $H(P)$.

Obrigada pela atenção!

- S.C. Coutinho, *Números Inteiros e Criptografia RSA*, IMPA, 2011.
- M. Lemos, *Criptografia, Números Primos e Algoritmos*, IMPA, 2010.
- A. C. Faleiros, *Criptografia*, SBMAC, 2010, disponível em *http : //www.sbmac.org.br/arquivos/notas/livro*$_{52}$*.pdf*


UNICAMP


CNPq
Conselho Nacional de Desenvolvimento
Científico e Tecnológico