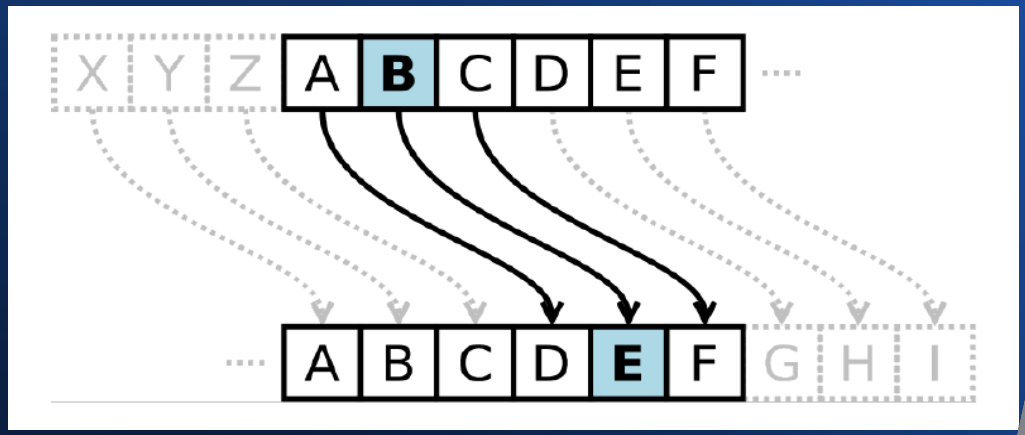
Criptografia e o Algoritmo RSA

Wedson F R Noronha – Licenciado em Matemática
Universidade Regional do Cariri - URCA

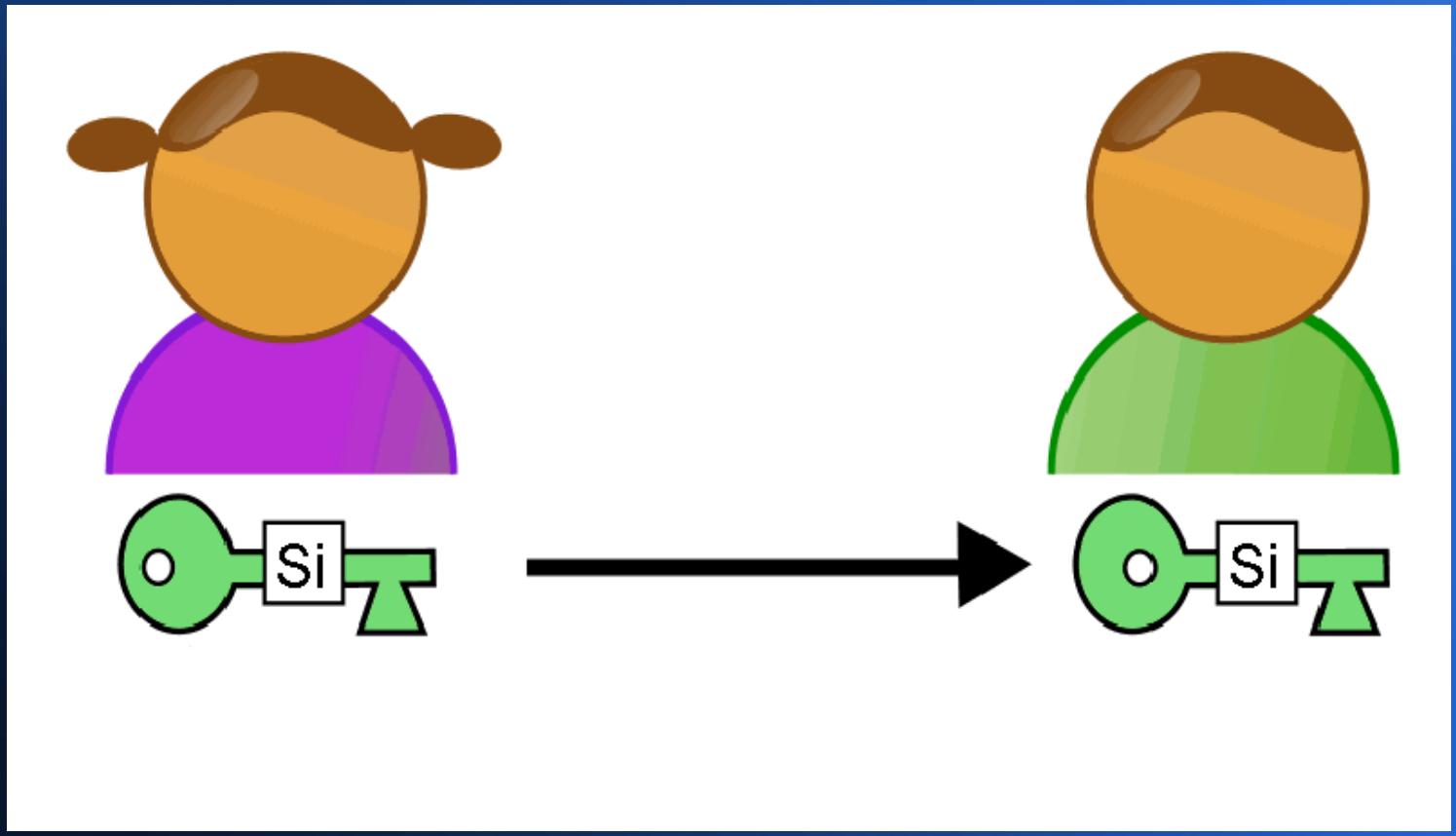
Criptografia e o Algoritmo RSA

- De César a 2º Guerra Mundia



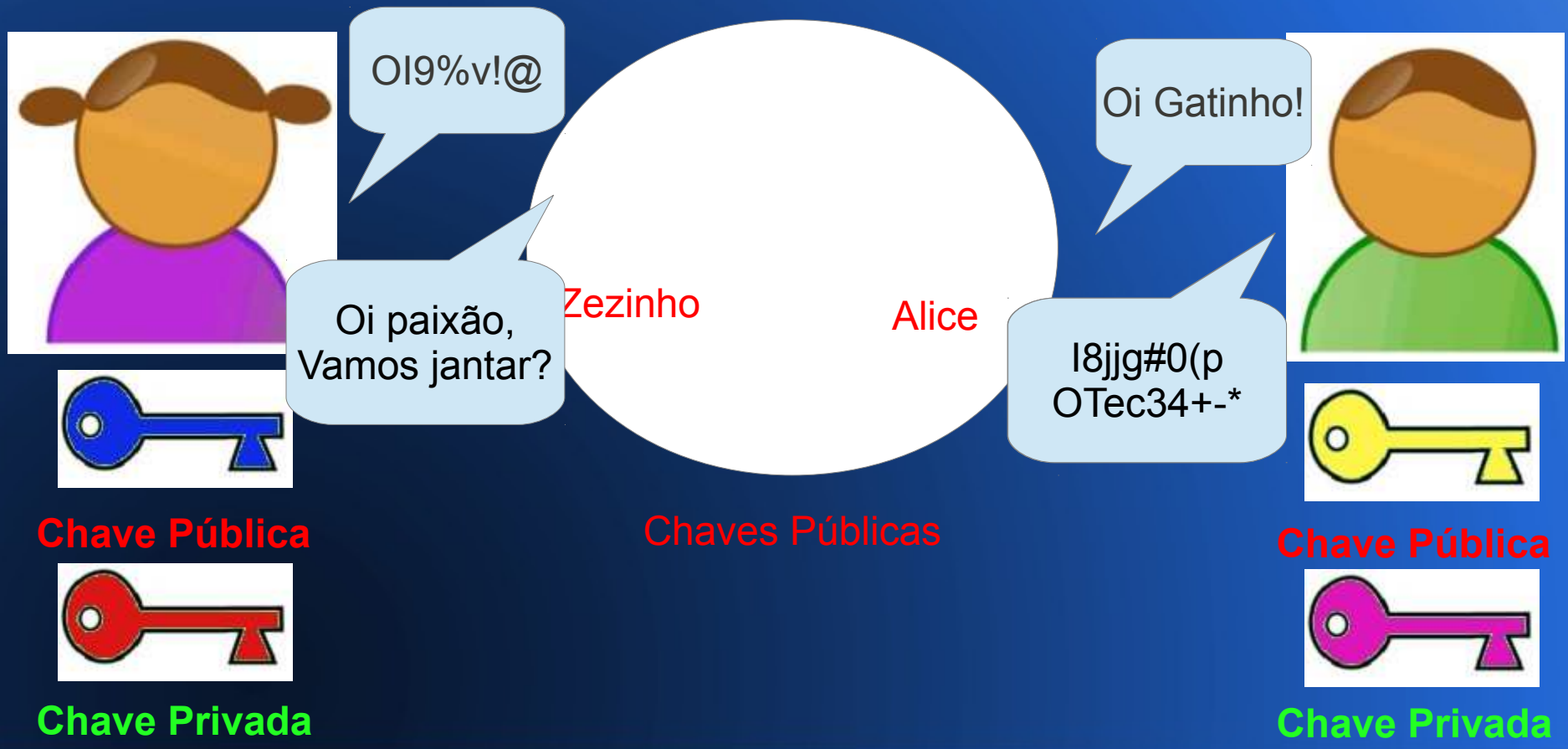
Criptografia e o Algoritmo RSA

- Chaves Simétrica



Criptografia e o Algoritmo RSA

- Chave Assimétrica – Pública/ Privada ⁉



Criptografia e o Algoritmo RSA

- Fatoração de Números Compostos
  - Alguns algoritmos usados;
  - Números compostos GRANDES;
    - Complexidade de algoritmos;
    - Quantos passos possui o algoritmo da soma?

Criptografia e o Algoritmo RSA

Suponha que cada operação elementar seja realizado em t=0,001s por um computador

n	T(n)=n	T(n)=nlog(n)	$T(n)=n^2$	$T(n)=n^3$	T(n)=2^n
10	0,01 s	0,01 s	0,1 s	1 s	1 s
100	0,1 s	0,02 s	10 s	16 min e 40 s	4 x 10^19 anos
200	0,2 s	0,46 s	40 s	2h 13min 20 s	5 x 10^49 anos
400	0,4 s	1,04 s	160 s	2 anos e 20 dias	8 x 10^109 anos

Criptografia e o Algoritmo RSA

- Um pouco de Teoria dos Números...
  - Dizemos que um inteito *m* divide um inteiro *a* se existir um único inteiro *k* tal que *mk=a*
  - Dizemos que dois inteiros *a* e *b* são congruêntes módulo *m* se *m|(a-b)*, com *m>0*;
    - Escrevemos a≡b mod(m)

Criptografia e o Algoritmo RSA

- Resultados importantes:
  - Teorema: *Sejam a, b e m inteiros tais que m>0 e (a,m)=d.Se d|b, a congruência ax≡b mod(m) possui exatamente d soluções incongruentes em x.*
  - *Corolário: Se (a,m)=1, então ax≡1 mod(m) possui apenas uma solução, chamada de inverso de a módulo m.*

Criptografia e o Algoritmo RSA

- Resultados importantes:
  - *Teorema(Fermat): Se p é primo e "a" é um inteiro positivo, então* $a^p \equiv a \bmod(p)$
  - *Fução Totiene de Euler: Definimos a função* $\Phi(n)$ *como o número de valores inteiros menores ou iguais a n que são primos relativos a n.*

    $\Phi(n)=\#\{x \in \mathbb{Z};\ x \leq n \ \ e \ \ (n,x)=1\}$

Criptografia e o Algoritmo RSA

- *Resultados importantes:*
  - *Teorema(Euler): Se m é um inteiro positivo e (a,m)=1, então vale:*

$$a^{\Phi(m)} \equiv 1 \bmod(m);$$

Criptografia e o Algoritmo RSA

- **Algoritmo Rivest-Shamir-Adleman- RSA.**

  O processo de geração das chaves pública e privada é o seguinte:

  - Escolha dois primos p e q da ordem de no mínimo 10^{150}, ou seja, que tenham pelo menos 150 dígitos
  - Faça n=pq

Criptografia e o Algoritmo RSA

- **Algoritmo Rivest-Shamir-Adleman- RSA.**
  - Escolha um intero c tal que $1<c<\Phi(n)$ e $(c,\Phi(n))=1$;
  - Ache um inteiro d tal que

    $dc=1 \bmod(\Phi(n))$;

Criptografia e o Algoritmo RSA

- **Algoritmo Rivest-Shamir-Adleman- RSA.**
  - Chave Pública: os inteiros n e c;
  - Chave Privada: os inteiros n e d;

Criptografia e o Algoritmo RSA

- **Algoritmo Rivest-Shamir-Adleman- RSA.**
  - Como Funciona?
  - Por exemplo, a mensagem: “ola alunos!”
  - Primeiro, vamos transformar a mensagem em um código numérico.

Criptografia e o Algoritmo RSA

a 01	b 02	c 03	d 04	e 05	f 06	g 07	h 08
i 09	j 10	k 11	l 12	m 13	n 14	o 15	p 16
q 17	r 18	s 19	t 20	u 21	v 22	w 23	x 24
y 25	z 26	. 27	, 28	; 29	! 30	? 31	 32

Criptografia e o Algoritmo RSA

- **Algoritmo Rivest-Shamir-Adleman- RSA.**
  - ola alunos = 15 12 01 32 01 12 21 14 15 19 30
  - Criptografar: $x=X(b)=b^c \bmod (n)$
  - Descriptografar: $Y(x)=x^d \bmod (n)$

Criptografia e o Algoritmo RSA

- **Algoritmo Rivest-Shamir-Adleman- RSA.**
  - Porque é seguro?

MUITO OBRIGADO!!!!!