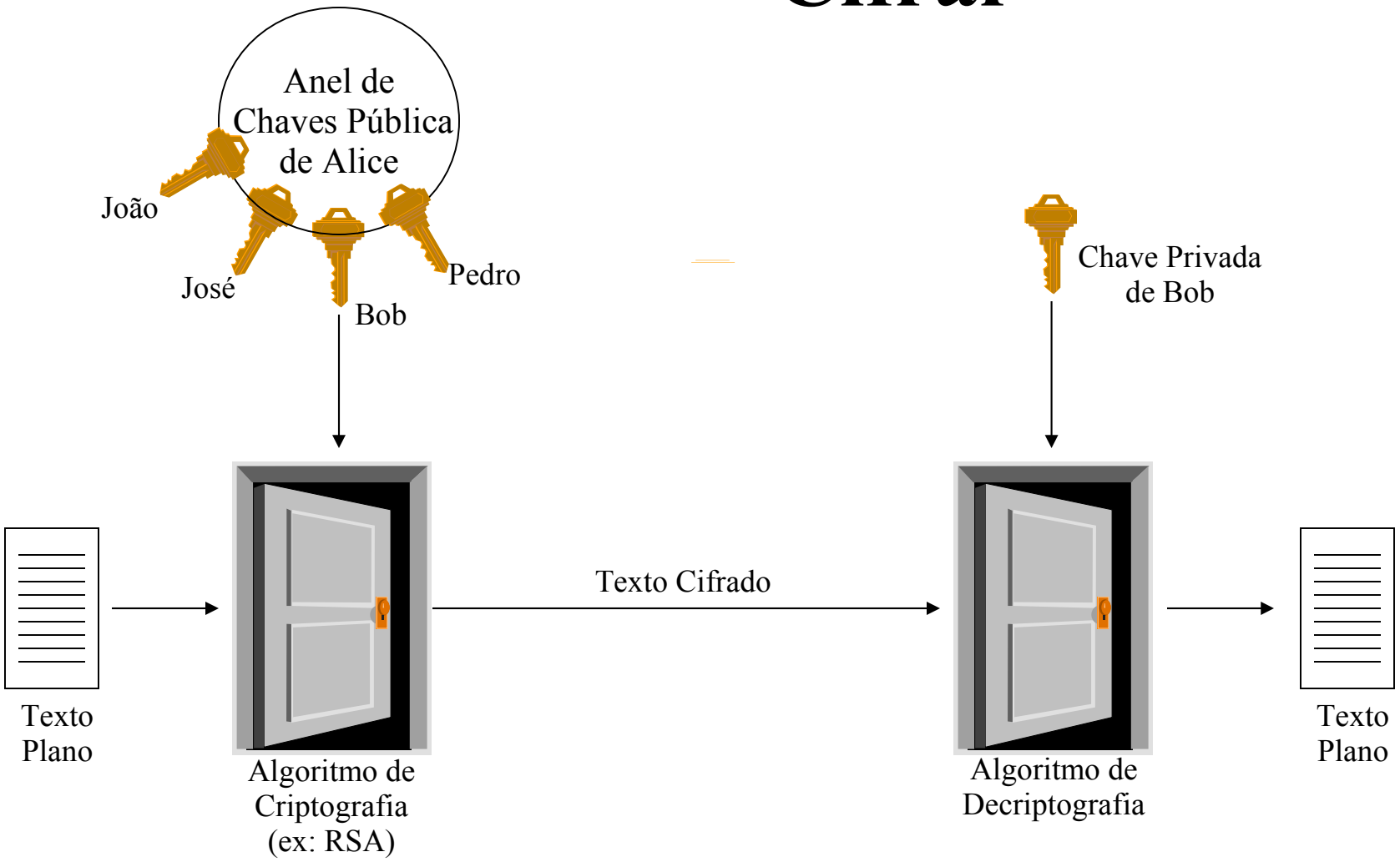
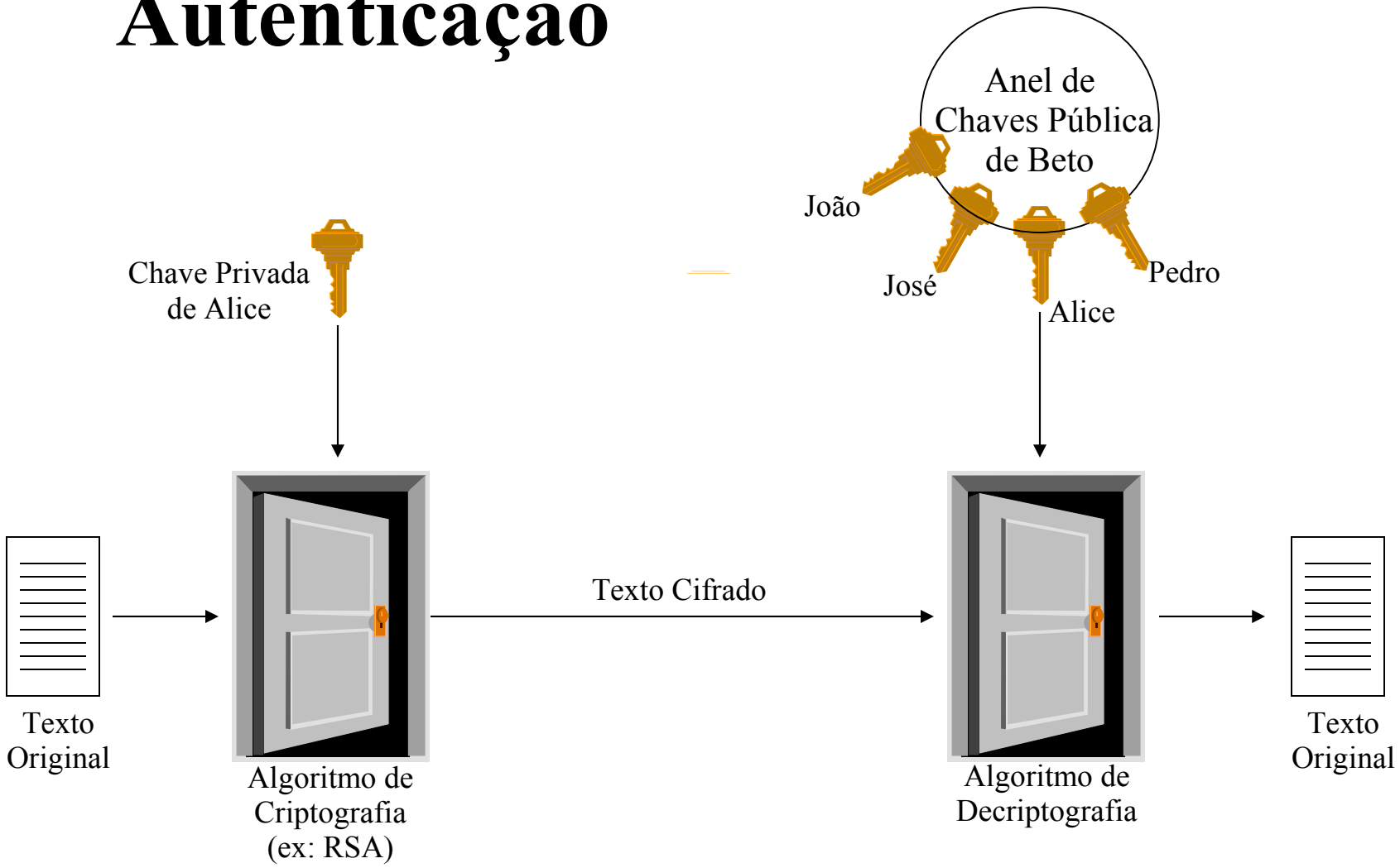
Criptografia
por
Chave Pública
Algoritmo RSA

Prof. Ricardo Felipe Custódio, D.Sc.
INE-CTC-UFSC

Cifrar


Anel de
Chaves Pública
de Alice
João
José
Bob
Pedro
Chave Privada
de Bob
Texto
Plano
Algoritmo de
Criptografia
(ex: RSA)
Texto Cifrado
Algoritmo de
Decriptografia
Texto
Plano

Autenticação



1978

Ron Rivest, Adi Shamir e Len Adleman

Blocos com valores binários menores que **n**
Tamanho do Bloco é k bits, onde $2^k < \mathbf{n} \leq 2^{k+1}$

Texto Cifrado

$C = M^e \bmod n$

$M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n$

Texto Plano

KU = {e,n}
KR = {d,n}

Requisitos do Algoritmo

- É possível encontrar **e**, **d**, **n** tal que $\mathbf{M^{ed} = M \bmod n}$ para todo **M < n**
- É relativamente fácil calcular $\mathbf{M^e}$ e $\mathbf{C^d}$ para todos os valores de **M < n**
- É improvável determinar **d** dado **e**, **n**

Detalhes Matemáticos

Dados **p** e **q** primos,
n e **m** inteiros tal que **n = pq**, **0 < m < n**
e um **k** arbitrário

$m^{k\phi(n)+1} = m^{k(p-1)(q-1)+1} \equiv m \bmod n$ (Eq. 7.8 - Corolário do Teor. Euler)

- $\phi(n)$ é a função totiente de Euler
  Número de Inteiros Positivos menor do que **n** e relativamente primos a **n**
- $\phi(pq) = (p-1)(q-1)$

$M^{ed} = M \bmod n$
$ed = k\,\phi(n) + 1$
$ed \equiv 1 \bmod \phi(n)$
$d \equiv e^{-1} \bmod \phi(n)$

Relativamente primos a $\phi(n)$

Algoritmo RSA

Geração da Chave

Selecione **p**,**q**	**p** e **q** primos
Calcular **n** = **p** x **q**	
Calcular $\phi(n) = (p-1)(q-1)$	
Selecionar **e** inteiro	$\gcd(\phi(n),e) = 1;\ 1 < e < \phi(n)$
Calcular **d**	$d = e^{-1} \bmod \phi(n)$
Chave Pública	**KU={e,n}**
Chave Privada	**KR={d,n}**

Cifrar

Texto Plano:	$M < n$
Texto Cifrado:	$C = M^e \pmod n$

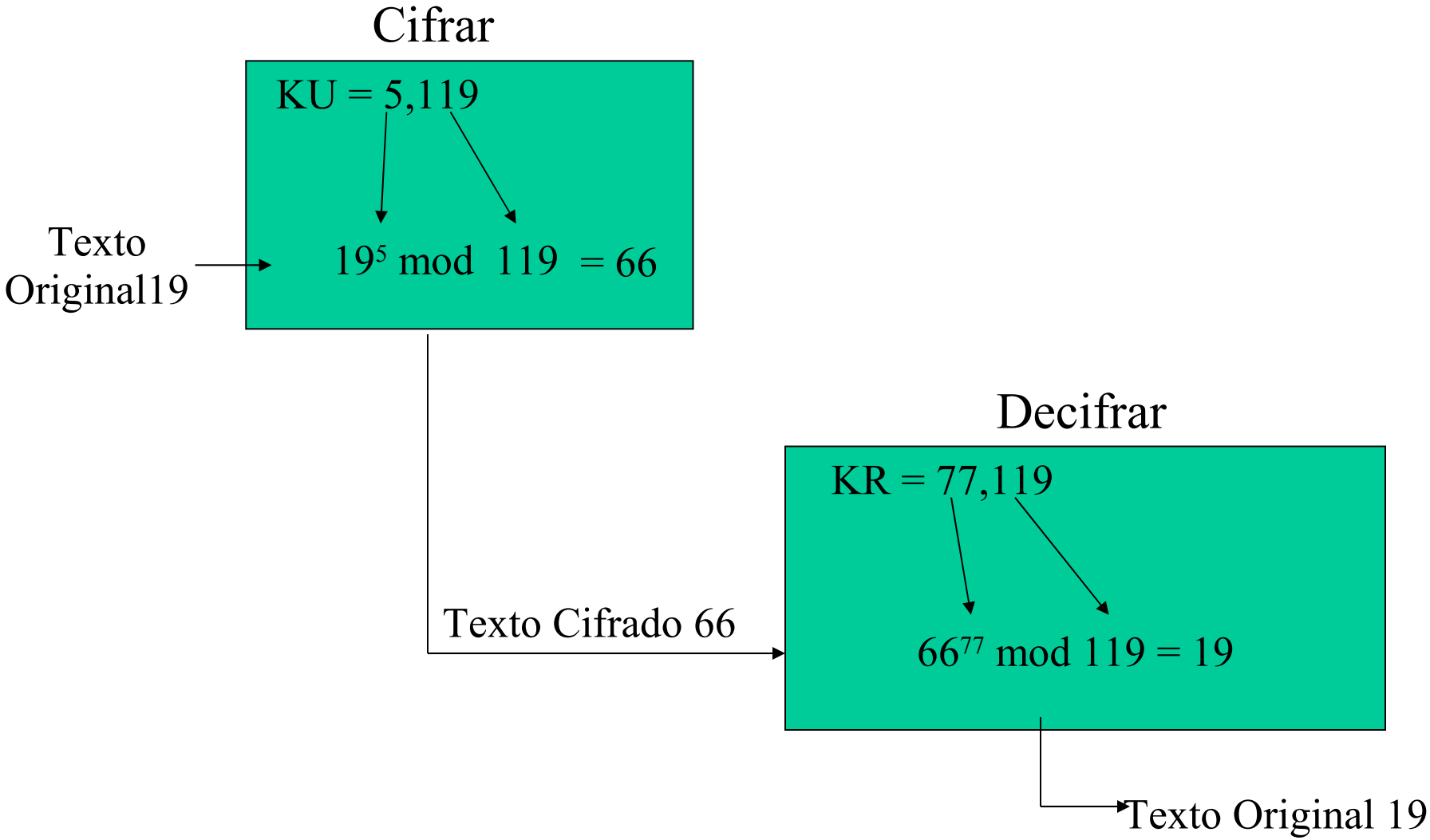
Decifrar

Texto Plano:	C
Texto Cifrado:	$M = C^d \pmod n$

Exemplo

- Selecionar dois números primos: $p = 7$ e $q = 17$
- Calcular $n = pq = 7 \times 17 = 119$
- Calcular $\phi(n) = (p-1)(q-1) = 96$
- Selecionar **e** tal que **e** é relativamente primo a $\phi(n)$ e menor que $\phi(n)$; $e = 5$
- Determinar d tal que $de = 1 \bmod 96$ e $d < 96$; $d = 77$, pois $77 \times 5 = 385 = 4 \times 96 + 1$
- $KU = \{5,119\}$ e $KR = \{77,119\}$

Continuação do Exemplo



Aspectos Computacionais E/D

$[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$

Seja $m = b_k b_{k-1} \ldots b_0$

$$m = \sum_{b_i \neq 0} 2^i$$

$$a^m = a^{\sum_{b_i \neq 0} 2^i} = \prod_{b_i \neq 0} a^{2^i}$$

$$a^m \bmod n = \left[\prod_{b_i \neq 0} a^{2^i} \right] \bmod n = \prod_{b_i \neq 0} a^{2^i} \bmod n$$

$d = a^m \bmod n$

```
d = 1
para i = k passo -1 até 0 faça
      d = (d x d) mod n
      se b_i = 1 então
            d = (d x a) mod n
      fim se
fim para
retorna d
```

[CORM 90]

Aspectos Computacionais Chaves

- Determinar dois primos **p** e **q**
  - n = pq é conhecido
    - **r** randômico ($\approx 2^{200} \rightarrow$ tentativas = $\ln(2^{200})/2 = 70$
    - **a < r** randômico
    - Testa r para primalidade
    - Se r passa em vários testes, aceita-se r
- Selecionar **e** ou **d** e calcular o outro
  - Algoritmo Extendido de Euclides

Segurança do RSA

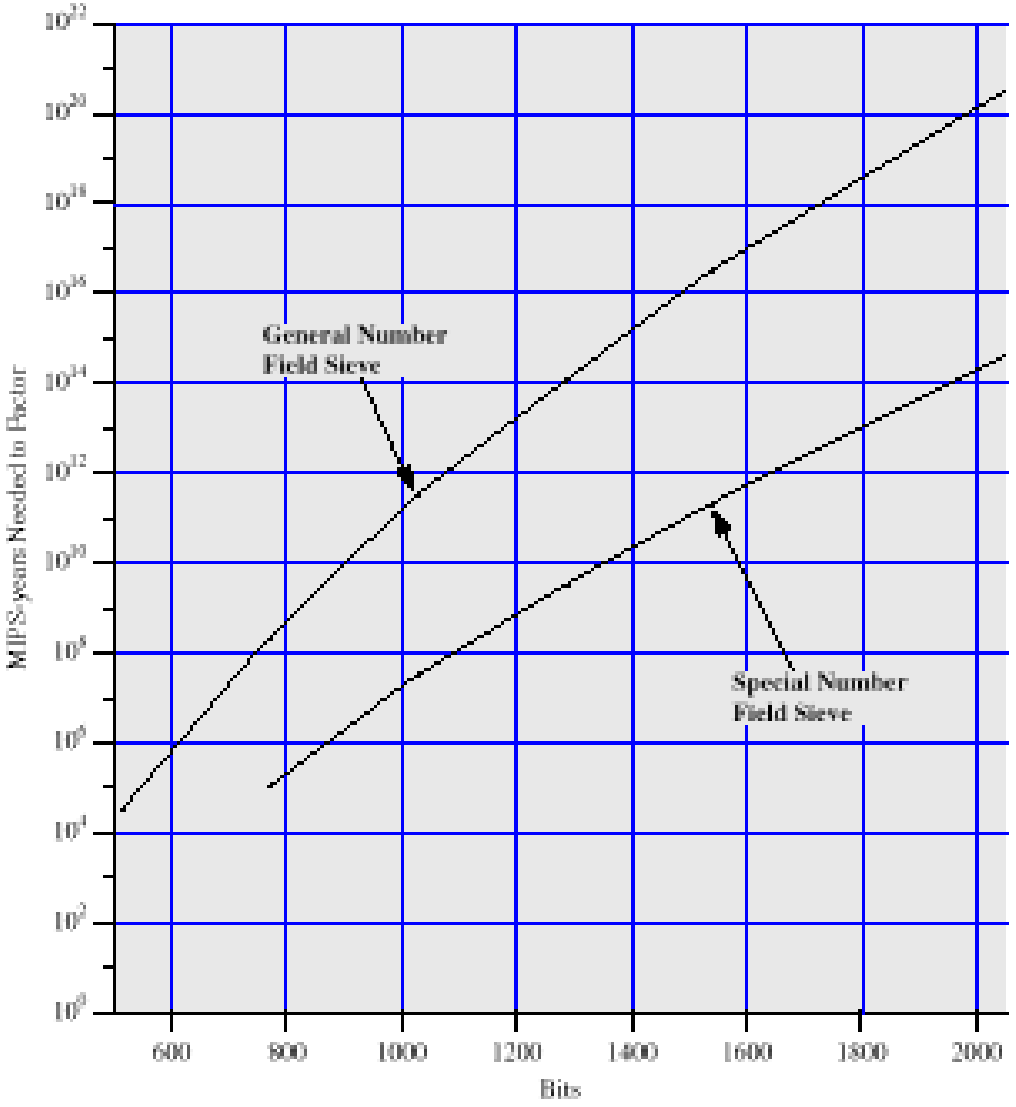
- Força Bruta
- Ataques Matemáticos
  - Fatorar Números Primos
  - Determinar $\phi(n)$ diretamente
  - Determinar d diretamente
- Ataques temporais

Fatoração

Número de dígitos Dec.	Aproximado de bits	Data	MIPS - Ano	Algoritmo
100	332	04/1991	7	sieve quadrático
110	365	04/1992	75	sieve quadrático
120	398	06/1993	830	sieve quadrático
129	428	04/1994	5000	sieve quadrático
130	431	04/1996	500	No. de campo sieve generalizado

Pentium 200 MHz = 50 MIPS

MIPS ano para fatorar



Prof. Ricardo Felipe Custódio, D.Sc.
INE-CTC-UFSC