ALGEBRA E CRIPTOGRAFIA

NICOLE & WENDELL

ATAQUES AO RSA

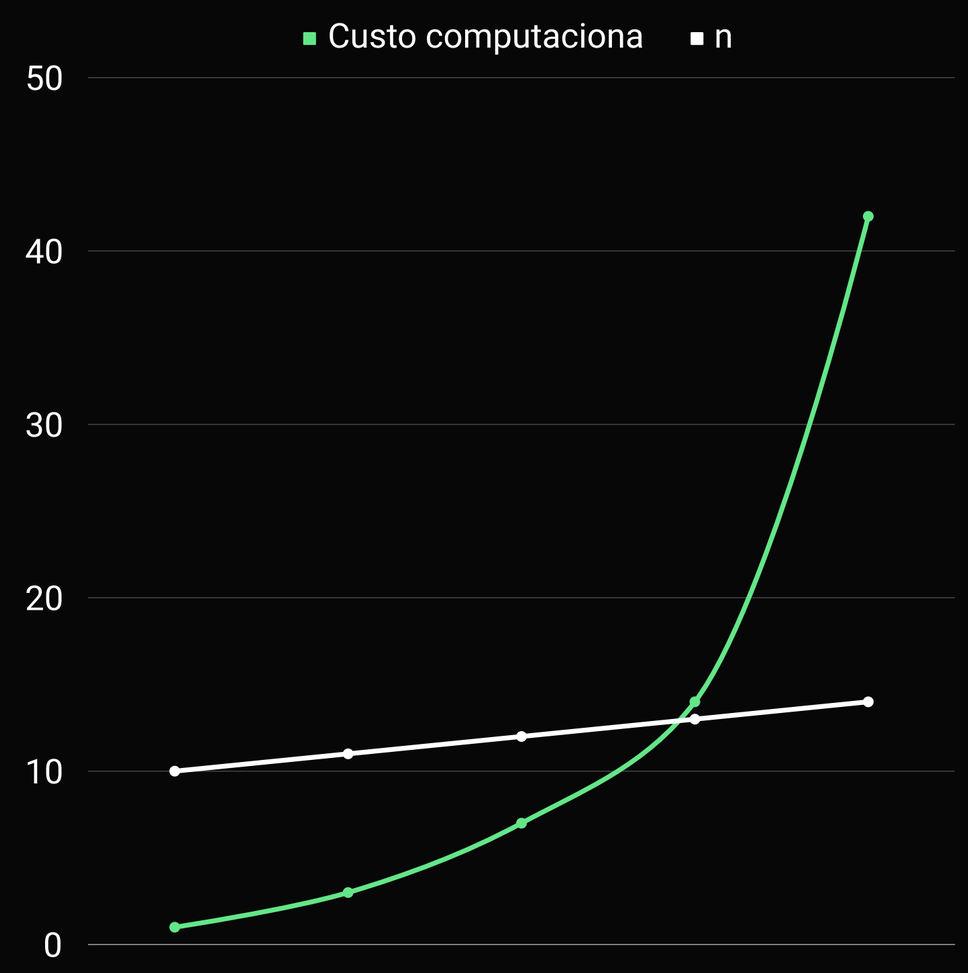
Explorando vulnerabilidades do sistema
e o problema da fatoração

Introdução

- A segurança do sistema RSA
- O problema da fatoração da chave pública
- **Custo computacional.**
- O que é um ataque?
- **“Uma corrente não é mais forte que seu elo mais fraco”**
- Busca por vulnerabilidades

Força bruta!

Ataques baseados em tentativa e erro: tentam explorar todas as possíveis combinações de chaves até encontrar uma que funcione

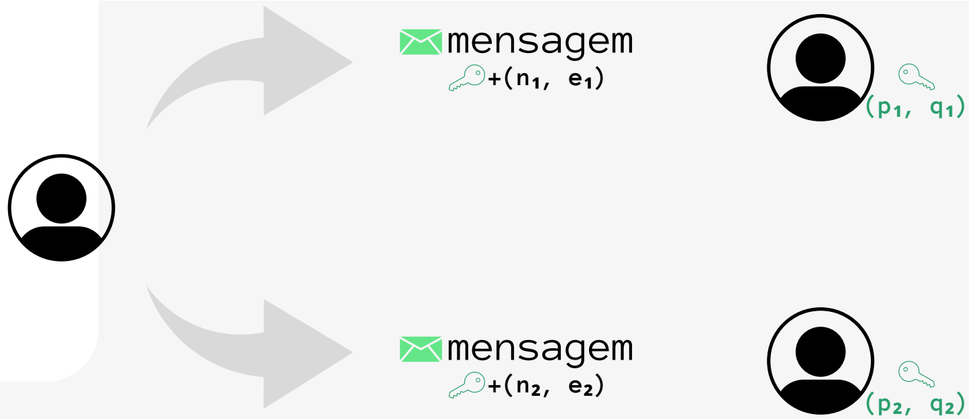


Ataques Matemáticos

1. Fatorar N para que possamos calcular $\varphi(N) = (p-1) \cdot (q-1)$ e em seguida $d \equiv e^{-1} \pmod{\varphi(N)}$.

2. Tentar determinar $\varphi(N)$ sem precisar achar p e q que compõem N, e com ele determinar d.

3. Encontrar d diretamente sem calcular $\phi(N)$.



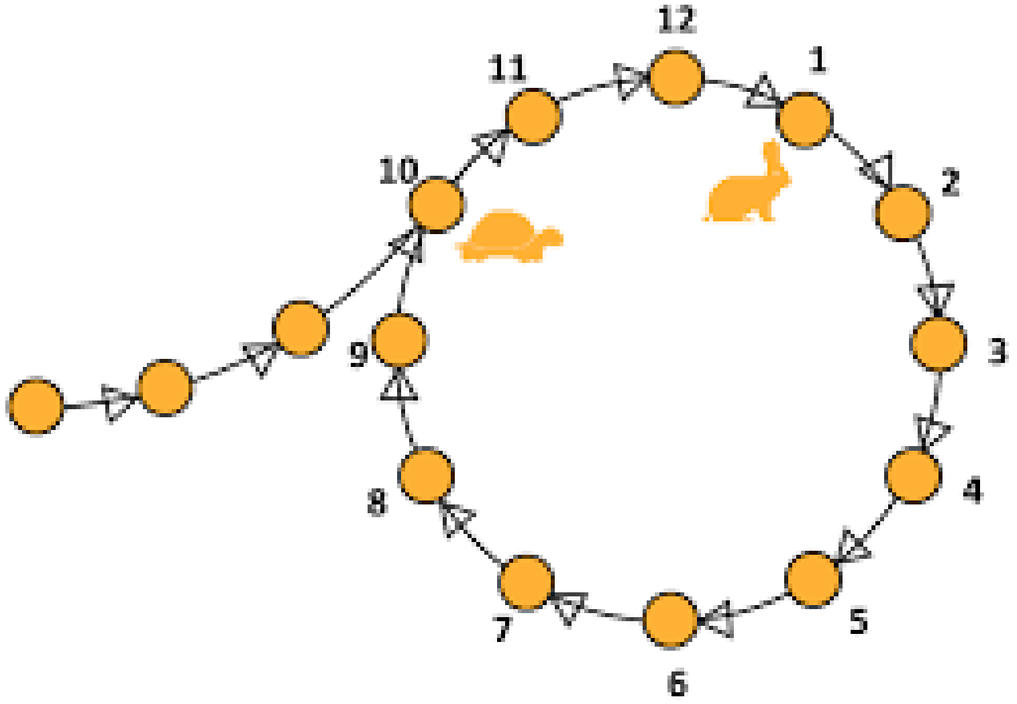
Ataques Temporais

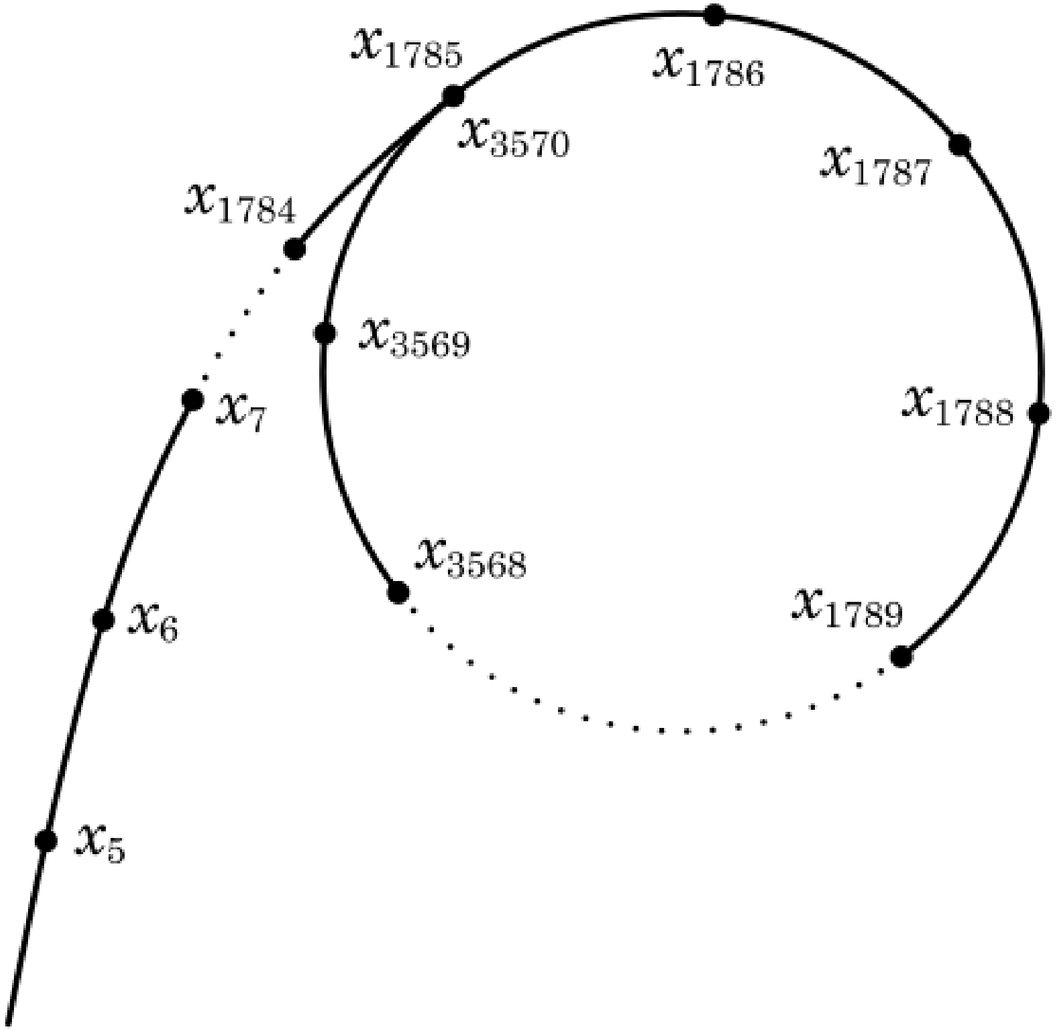
- Buscam vulnerabilidades na implementação computacional
- Visam obter informações sensíveis ao medir variações temporais:
  - Consumo de Energia
  - Tempo de execução


Exemplos de ataques ao RSA

Problema da Fatoração

- Algoritmo de fatorização de Fermat
- Algoritmo rho de Pollard


12
1
2
3
4
5
6
7
8
9
10
11


x_{1785}
x_{1786}
x_{3570}
x_{1787}
x_{1784}
x_{3569}
x_7
x_{1788}
x_{3568}
x_{1789}
x_6
x_5

Vulnerabilidades do sistema

- Módulo Comum
- Ataque de Hastad

$$C_1 \equiv m^3 \bmod N_1$$
$$C_2 \equiv m^3 \bmod N_2$$
$$C_3 \equiv m^3 \bmod N_3$$

$$M = C_1^x \times (C_2^{-1})^y$$

Mais ataques matemáticos

- Ataque de Wiener
- Ataque cíclico

ATACANDO E-MAILS!

~~(Ezequiel e Darlan)~~

119_231_61_86_119_567_32_61_650_32_119_557_248_650_567_174_114_86_114

Caixa de entrada ×

[redacted]

3 de dez. de 2023, 23:11 (há 16 horas)

para mim

306_678_8_557_174_114_306_32_480_32_14_231_86_686_567_32_678_557_8_306_678 --- (779, 37)

Responder Encaminhar

Como computadores quânticos quebram o RSA?

Conclusão

- Vulnerabilidades atreladas ao mal uso
- Problema da Fatoração
- Futuro da Criptografia

```
[2]                                                                    Python

...  Mensagem criptografada: 695311358495398420122652038887068477639374430602798390744134
     Expoente e1: 65537
     Expoente e2: 587
     Ataque bem sucedido!
     Mensagem descriptografada: minha senha do banco é 1234
```