Avaliação de diferentes implementações do sistema de criptografia RSA

Ana Carla Quallio Rosa[1], Rodrigo Campiolo[1]
[1]Universidade Tecnológica Federal do Paraná (UTFPR)

UTFPR
UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

Introdução

- Os sistemas de criptografia tornam-se essenciais;
- Algoritmo RSA: amplamente adotado no contexto de criptografia assimétrica.

Objetivo principal

O objetivo principal deste trabalho é conduzir uma avaliação das implementações do RSA.

Objetivos específicos

Comparação do RSA para diferentes APIs

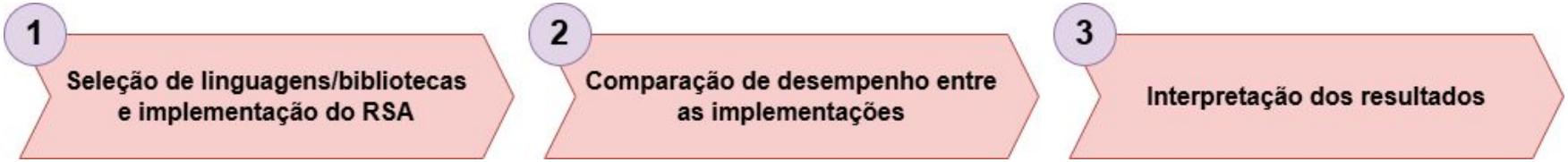
Avaliar a eficiência de ajustes no processo matemático

Analisar estruturas de dados de armazenamento

Trabalhos relacionados

Abordagem	Autores	Proposta do trabalho
Algoritmos híbridos	Gupta e Sharma (2012)	RSA e sistema *Diffie-Hellman*
	Jintcharadze e Iavich (2020)	RSA e *ElGamal*
Alterações matemáticas	Islam *et al.* (2018)	Generalização do RSA para *n* primos
Desempenho	Singh *et al.* (2016)	RSA vs. curvas elípticas

Método de pesquisa



Implementação
do algoritmo com base nas documentações de cada biblioteca.

Linguagens e bibliotecas selecionadas

- **C:** OpenSSL e Libgcrypt;
- **C++:** Crypto++e Botan;
- **Java:** Bouncy Castle;
- **Python:** Cryptography e PyCryptodome;
- **Rust:** rust-crypto e ring;

Avaliação preliminar

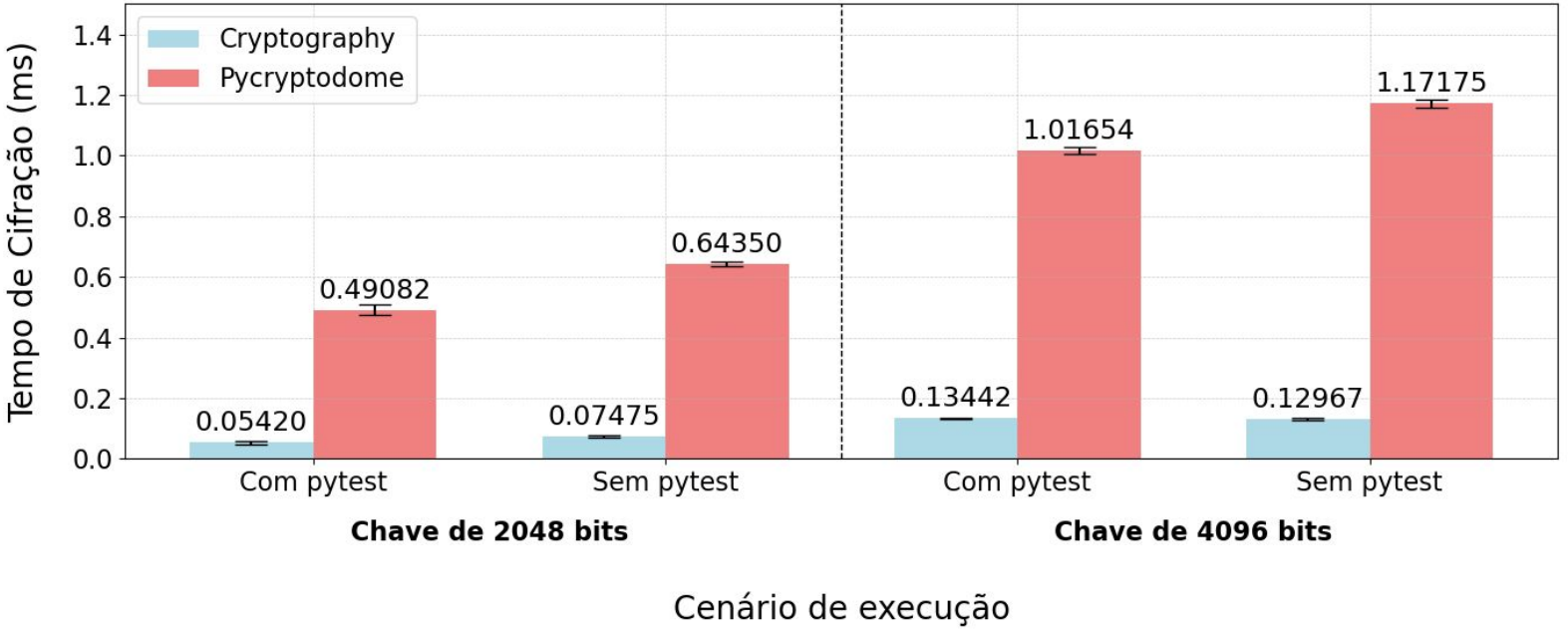
Linguagem selecionada	Python (Cryptography e Pycryptodome)
Contexto de avaliação	Processador: AMD Ryzen 5 (64 bit)
	Memória RAM: 12 GB
	Sistema Operacional: Debian 12 (64 bit)
	Ambiente Gráfico: GNOME
Comparação	Pytest e versão sem ferramenta
Tamanho da mensagem	190 bytes

Resultados preliminares

Tamanho da chave	Biblioteca	Tempo médio (s)	Desvio padrão	Mediana
2048	Cryptography	0,16251	0,08277	0,13970
	Pycryptodome	0,42374	0,22434	0,41536
4096	Cryptography	1,04163	0,59759	0,86004
	Pycryptodome	5,21896	4,39681	4,41156

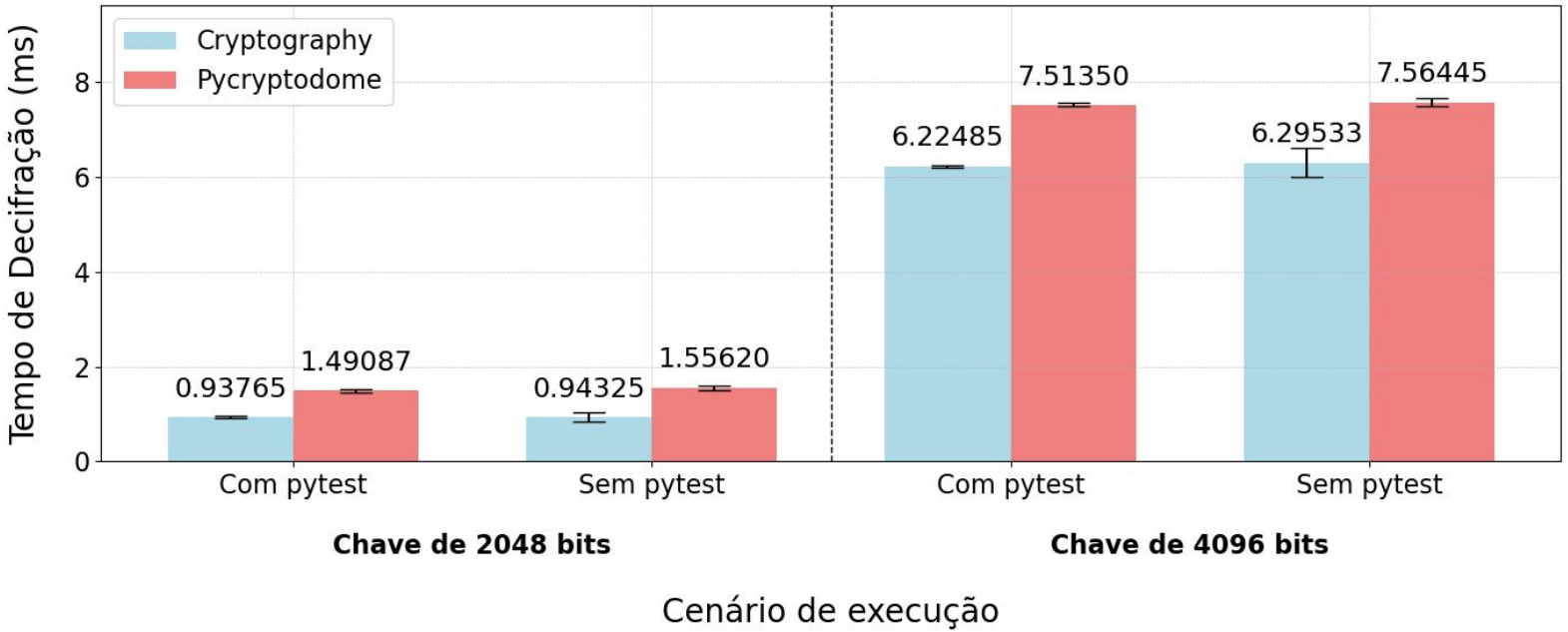
Geração de chaves

Resultados preliminares



Cifração

Resultados preliminares



Decifração

Considerações

Diferenças significativas entre as implementações do algoritmo neste contexto de avaliação.

Próximos passos

- Explorar outras linguagens de programação e abordagens;
- Identificar questões de desempenho e oportunidades de otimização;
- Avaliar os possíveis impactos na segurança.

Obrigada!

- Ana Carla Quallio Rosa (anacarlarosa@alunos.utfpr.edu.br)
- Rodrigo Campiolo (rcampiolo@utfpr.edu.br).

Acesse o repositório por meio do QR Code