TP4_Exercicio3

May 27, 2024

1 TP4 - Exercício 3

1.0.1 Autores

Afonso Ferreira - pg52669
Tiago Rodrigues - pg52705

1.0.2 Enunciado

Construir tabelas de comparações das suas implementações, para os vários níveis de segurança NIST e em termos dos seguintes parâmetros - Tempos: geração das chaves, produção da assinatura e verificação da assinatura. - Tamanhos: da chave pública, da chave privada e da assinatura.

[ ]:
```
%pip install pandas
import pandas as pd
```

```
Requirement already satisfied: pandas in
/Users/afonsoni/miniconda3/envs/EC/lib/python3.11/site-packages (2.2.2)
Requirement already satisfied: numpy>=1.23.2 in
/Users/afonsoni/miniconda3/envs/EC/lib/python3.11/site-packages (from pandas)
(1.26.4)
Requirement already satisfied: python-dateutil>=2.8.2 in
/Users/afonsoni/miniconda3/envs/EC/lib/python3.11/site-packages (from pandas)
(2.8.2)
Requirement already satisfied: pytz>=2020.1 in
/Users/afonsoni/miniconda3/envs/EC/lib/python3.11/site-packages (from pandas)
(2024.1)
Requirement already satisfied: tzdata>=2022.7 in
/Users/afonsoni/miniconda3/envs/EC/lib/python3.11/site-packages (from pandas)
(2024.1)
Requirement already satisfied: six>=1.5 in
/Users/afonsoni/miniconda3/envs/EC/lib/python3.11/site-packages (from python-
dateutil>=2.8.2->pandas) (1.16.0)
Note: you may need to restart the kernel to use updated packages.
```

1.0.3 Tabela de resultados

[ ]:
```
# Define the data for the table
data = {
    'DILITHIUM-2': ['56 bytes', '72 bytes', '56 bytes', '7.437 ms', '30.880␣
 ↪ms', '5.865 ms'],
    'DILITHIUM-3': ['56 bytes', '72 bytes', '56 bytes', '12.366 ms', '45.001␣
 ↪ms', '15.618 ms'],
    'DILITHIUM-5': ['56 bytes', '72 bytes', '56 bytes', '26.165 ms', '129.374␣
 ↪ms', '19.623 ms'],
    'SPHINCS+': ['88 bytes', '72 bytes', '120 bytes', '406.602 ms', '1194.553␣
 ↪ms', '38.300 ms']
}

# Define the rows for the table
rows = [
    'Tamanho Chave Pública',
    'Tamanho Chave Privada',
    'Tamanho de Assinatura',
    'Tempo de Geração de Chaves',
    'Tempo de Produção da Assinatura',
    'Tempo de Verificação de Assinatura'
]

# Create the dataframe
df = pd.DataFrame(data, index=rows)

# Display the dataframe
df
```

[ ]:
```
                                  DILITHIUM-2 DILITHIUM-3 DILITHIUM-5  \
Tamanho Chave Pública               56 bytes    56 bytes    56 bytes
Tamanho Chave Privada               72 bytes    72 bytes    72 bytes
Tamanho de Assinatura               56 bytes    56 bytes    56 bytes
Tempo de Geração de Chaves           7.437 ms   12.366 ms   26.165 ms
Tempo de Produção da Assinatura     30.880 ms   45.001 ms  129.374 ms
Tempo de Verificação de Assinatura   5.865 ms   15.618 ms   19.623 ms

                                    SPHINCS+
Tamanho Chave Pública               88 bytes
Tamanho Chave Privada               72 bytes
Tamanho de Assinatura              120 bytes
Tempo de Geração de Chaves         406.602 ms
Tempo de Produção da Assinatura   1194.553 ms
Tempo de Verificação de Assinatura  38.300 ms
```