Ex3

May 27, 2024

1 Trabalho Prático 4

André Freitas PG54707

Bruna Macieira PG54467

1.1 Exercício 3

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
```

```
Defaulting to user installation because normal site-packages is not writeable
Requirement already satisfied: pandas in
/home/fura/.sage/local/lib/python3.10/site-packages (2.2.2)
Requirement already satisfied: python-dateutil>=2.8.2 in
/home/fura/.sage/local/lib/python3.10/site-packages (from pandas) (2.9.0.post0)
Requirement already satisfied: pytz>=2020.1 in /usr/lib/python3/dist-packages
(from pandas) (2022.1)
Requirement already satisfied: tzdata>=2022.7 in
/home/fura/.sage/local/lib/python3.10/site-packages (from pandas) (2024.1)
Requirement already satisfied: numpy>=1.22.4 in
/home/fura/.sage/local/lib/python3.10/site-packages (from pandas) (1.26.4)
Requirement already satisfied: six>=1.5 in /usr/lib/python3/dist-packages (from
python-dateutil>=2.8.2->pandas) (1.16.0)
Note: you may need to restart the kernel to use updated packages.
```

Tabela de resultados do Exercício 1

[ ]:
```
# Define the data for the table
data = {
    'Level 2': ['232 bytes', '360 bytes', '232 bytes', '70.245 ms', '17.028␣
 ↪ms', '18.289 ms'],
    'Level 3': ['232 bytes', '360 bytes', '232 bytes', '80.922 ms', '480.200␣
 ↪ms', '17.019 ms'],
```

```
    'Level 5': ['232 bytes', '360 bytes', '232 bytes', '50.935 ms', '61.655␣
 ↪ms', '15.317 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
```

[ ]:

	Level 2	Level 3	Level 5
Tamanho Chave Pública	232 bytes	232 bytes	232 bytes
Tamanho Chave Privada	360 bytes	360 bytes	360 bytes
Tamanho de Assinatura	232 bytes	232 bytes	232 bytes
Tempo de Geração de Chaves	70.245 ms	80.922 ms	50.935 ms
Tempo de Produção da Assinatura	17.028 ms	480.200 ms	61.655 ms
Tempo de Verificação de Assinatura	18.289 ms	17.019 ms	15.317 ms

Tabela de resultados do Exercício 2

[ ]:
```
# Define the data for the table
data = {
    'SLH-DSA-SHA2-128f': ['32 bytes', '64 bytes', '17121 bytes', '0.0871074␣
 ↪ms', '1.32689 ms', '0.0482664 ms'],
    'SLH-DSA-SHA2-128s': ['32 bytes', '64 bytes', '7889 bytes', '3.50418 ms',␣
 ↪'27.2929 ms', '0.0225248 ms'],
    'SLH-DSA-SHA2-192f': ['48 bytes', '96 bytes', '35697 bytes', '0.0664964␣
 ↪ms', '1.8832 ms', '0.10592 ms'],
    'SLH-DSA-SHA2-192s': ['48 bytes', '96 bytes', '16257 bytes', '4.59455 ms',␣
 ↪'41.3526 ms', '0.0293076 ms'],
    'SLH-DSA-SHA2-256f': ['64 bytes', '128 bytes', '49889 bytes', '0.187162␣
 ↪ms', '3.94006 ms', '0.0975442 ms'],
    'SLH-DSA-SHA2-256s': ['64 bytes', '128 bytes', '29825 bytes', '3.64639 ms',␣
 ↪'38.8773 ms', '0.0501485 ms'],
    'SLH-DSA-SHAKE-128f': ['32 bytes', '64 bytes', '17121 bytes', '0.0370972␣
 ↪ms', '0.763631 ms', '0.0539906 ms'],
```

```
    'SLH-DSA-SHAKE-128s': ['32 bytes', '64 bytes', '7889 bytes', '2.21355 ms',␣
 ↪'16.4512 ms', '0.0215425 ms'],
    'SLH-DSA-SHAKE-192f': ['48 bytes', '96 bytes', '35697 bytes', '0.0583994␣
 ↪ms', '1.25171 ms', '0.0636024 ms'],
    'SLH-DSA-SHAKE-192s': ['48 bytes', '96 bytes', '16257 bytes', '3.28588 ms',␣
 ↪'30.6214 ms', '0.0340853 ms'],
    'SLH-DSA-SHAKE-256f': ['64 bytes', '128 bytes', '49889 bytes', '0.127304␣
 ↪ms', '2.81806 ms', '0.0678008 ms'],
    'SLH-DSA-SHAKE-256s': ['64 bytes', '128 bytes', '29825 bytes', '2.11156␣
 ↪ms', '26.6165 ms', '0.0339012 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
```

[ ]:

	SLH-DSA-SHA2-128f	SLH-DSA-SHA2-128s	\
Tamanho Chave Pública	32 bytes	32 bytes	
Tamanho Chave Privada	64 bytes	64 bytes	
Tamanho de Assinatura	17121 bytes	7889 bytes	
Tempo de Geração de Chaves	0.0871074 ms	3.50418 ms	
Tempo de Produção da Assinatura	1.32689 ms	27.2929 ms	
Tempo de Verificação de Assinatura	0.0482664 ms	0.0225248 ms	

	SLH-DSA-SHA2-192f	SLH-DSA-SHA2-192s	\
Tamanho Chave Pública	48 bytes	48 bytes	
Tamanho Chave Privada	96 bytes	96 bytes	
Tamanho de Assinatura	35697 bytes	16257 bytes	
Tempo de Geração de Chaves	0.0664964 ms	4.59455 ms	
Tempo de Produção da Assinatura	1.8832 ms	41.3526 ms	
Tempo de Verificação de Assinatura	0.10592 ms	0.0293076 ms	

	SLH-DSA-SHA2-256f	SLH-DSA-SHA2-256s	\
Tamanho Chave Pública	64 bytes	64 bytes	

Tamanho Chave Privada	128 bytes	128 bytes
Tamanho de Assinatura	49889 bytes	29825 bytes
Tempo de Geração de Chaves	0.187162 ms	3.64639 ms
Tempo de Produção da Assinatura	3.94006 ms	38.8773 ms
Tempo de Verificação de Assinatura	0.0975442 ms	0.0501485 ms

	SLH-DSA-SHAKE-128f	SLH-DSA-SHAKE-128s \
Tamanho Chave Pública	32 bytes	32 bytes
Tamanho Chave Privada	64 bytes	64 bytes
Tamanho de Assinatura	17121 bytes	7889 bytes
Tempo de Geração de Chaves	0.0370972 ms	2.21355 ms
Tempo de Produção da Assinatura	0.763631 ms	16.4512 ms
Tempo de Verificação de Assinatura	0.0539906 ms	0.0215425 ms

	SLH-DSA-SHAKE-192f	SLH-DSA-SHAKE-192s \
Tamanho Chave Pública	48 bytes	48 bytes
Tamanho Chave Privada	96 bytes	96 bytes
Tamanho de Assinatura	35697 bytes	16257 bytes
Tempo de Geração de Chaves	0.0583994 ms	3.28588 ms
Tempo de Produção da Assinatura	1.25171 ms	30.6214 ms
Tempo de Verificação de Assinatura	0.0636024 ms	0.0340853 ms

	SLH-DSA-SHAKE-256f	SLH-DSA-SHAKE-256s
Tamanho Chave Pública	64 bytes	64 bytes
Tamanho Chave Privada	128 bytes	128 bytes
Tamanho de Assinatura	49889 bytes	29825 bytes
Tempo de Geração de Chaves	0.127304 ms	2.11156 ms
Tempo de Produção da Assinatura	2.81806 ms	26.6165 ms
Tempo de Verificação de Assinatura	0.0678008 ms	0.0339012 ms