Pontifícia Universidade Católica do Paraná
Escola Politécnica
Bacharelado em Engenharia de Software

Disciplina: Segurança da Informação
Professor: Luis Gonzaga de Paulo
Aluno: Diogo Bonet Sobezak

Atividade Prática 07 - Análise de desempenho criptográfico

Descrição da Atividade:

Esta atividade consiste em analisar o desempenho dos algoritmos de criptografia simétrica e de criptografia de chave pública, bem como demonstrar o impacto do tamanho das chaves utilizadas no algoritmo.

Entrega:

1. Esta atividade deverá ser entregue até o dia 10/05/2023.
2. Deverá ser entregue um documento em formato ".pdf", contendo o relatório que atenda a especificação a seguir.
3. O arquivo deverá conter o nome do aluno(a).

Especificação:

Desenvolva um programa que aplique as criptografias de chave pública (assimétrica) e de chave única (simétrica) conforme requisitos abaixo:

1. O programa deve cifrar o texto:

   "RSA: algoritmo dos professores do MIT: Rivest, Shamir e Adleman".

2. O programa deve registrar o tempo de execução de cada iteração do experimento, incluindo a geração das chaves.
3. O programa deve cifrar o texto informado utilizando o algoritmo:
   a. RSA com chave pública e privada de 1024 bits.
   b. RSA com chave pública e privada de 2048 bits.
   c. RSA com chave pública e privada de 4096 bits.
   d. RSA com chave pública e privada de 8192 bits.
   e. AES com chave de 128 bits.
   f. AES com chave de 256 bits.
4. Cada uma das iterações deverá ser executada 05 (cinco) vezes. O processo de repetição não deve ser automatizado, para evitar o uso de cache.
5. Cada iteração deverá ser registrada por meio de *screen shot* (*printscreen*) apresentando o resultado obtido.

6. Os tempos registrados deverão ser colocados em uma planilha, a ser incluída no relatório, apresentando também o tempo médio obtido de execução para cada algoritmo. (Adicionado direto no PDF)
7. O relatório também deve apresentar a configuração do sistema (Sistema Operacional e versão, processador, *clock*, memória e *HD*) utilizado para a execução da atividade.

Observações:

I. O(s) programa(s) pode(m) ser desenvolvido(s) nas linguagens de programação Java ou Python. O(s) código(s) fonte(s) deve(m) constar do relatório.

II. A atividade pode ser desenvolvida em equipe, porém cada elemento da equipe deverá executar os passos e apresentar o relatório individual.

III. O relatório deve incluir as referências bibliográficas (sites, artigos, livros) utilizadas para a elaboração do código.

RSA:

1024 bits ->

```
-----END RSA PRIVATE KEY-----
Cifrado:  b'04609d88337406aacd64b10c94db317c94cadb3a43eede942eda4a40735d909415b5785e704df46ef254ae69f4034152bf2b050314123a253f45e515f0aa77b2d59db26132ec44
Decifrado:  b'RSA: algoritmo dos professores do MIT: Rivest, Shamir e Adleman'
Tempo decorrido:  0.16501116752624512  segundos
```

-

```
-----END RSA PRIVATE KEY-----
Cifrado:  b'405efcc1b89fc5251534ad1dbbb064a84061c4852f90cd1dab150f90f56db7316c05abaf14096b0906d3b9d2364102a1ffc4a69a84a8cd656d3f9b9f90b0992b8d9bcfb8d83edb1
Decifrado:  b'RSA: algoritmo dos professores do MIT: Rivest, Shamir e Adleman'
Tempo decorrido:  0.16301417350769043  segundos
```

-

```
-----END RSA PRIVATE KEY-----
Cifrado:  b'24561649cb656d3f44cdca1570f1a5ceee99c9588cd7670ba226c090e13b45fc3b94e3464946da85007cb2698c4c6a9facbf8fd729e883880021798df4c356f28e3afb608f5b240
Decifrado:  b'RSA: algoritmo dos professores do MIT: Rivest, Shamir e Adleman'
Tempo decorrido:  0.13400912284851074  segundos
```

-

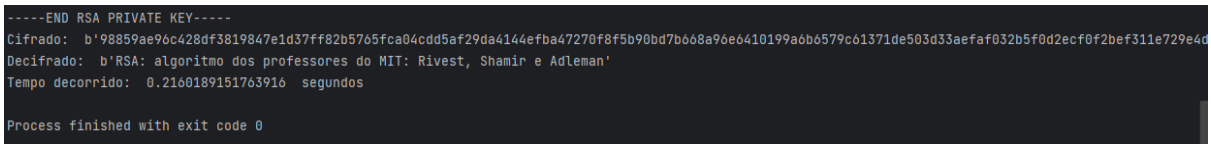
```
-----END RSA PRIVATE KEY-----
Cifrado:  b'2884b37aea5bef9c86fb2d4794a661f0f927579321faf1c819f673f58e2bca5be2c433c4c997168ae214f45a78591a8fac24a684873a07ed3d1316635fe1b6097b4ef21d93fd64f
Decifrado:  b'RSA: algoritmo dos professores do MIT: Rivest, Shamir e Adleman'
Tempo decorrido:  0.11200714111328125  segundos
```

-

```
-----END RSA PRIVATE KEY-----
Cifrado:  b'2c76ba9f1714c97e2b8a374306bc03557ca911f6f14cfa85a88f6467ac01b1732037e1efe4b572ded9acc6c485e6a6bea2690e6828b8dc98085cc6f85b9065766e43182406476d5
Decifrado:  b'RSA: algoritmo dos professores do MIT: Rivest, Shamir e Adleman'
Tempo decorrido:  0.12000346183776855  segundos

Process finished with exit code 0
```

-

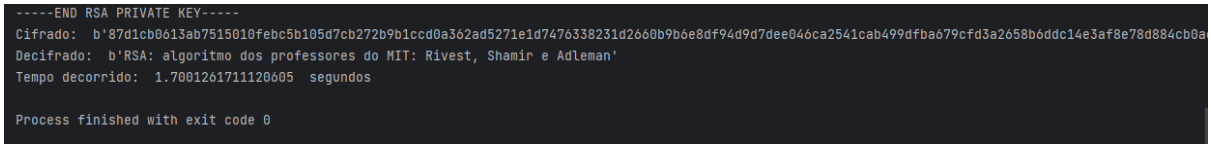


Tempo Médio: 0,188 segundos

2048 bits ->

-

-



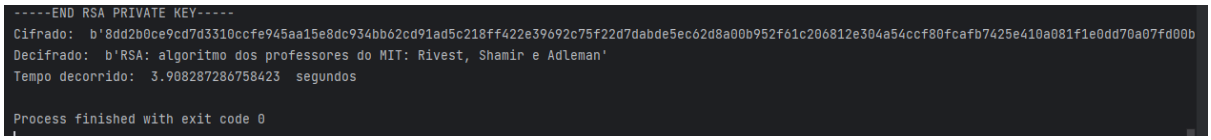
-

-

Tempo Médio: 1,02 segundos

4096 bits ->

-



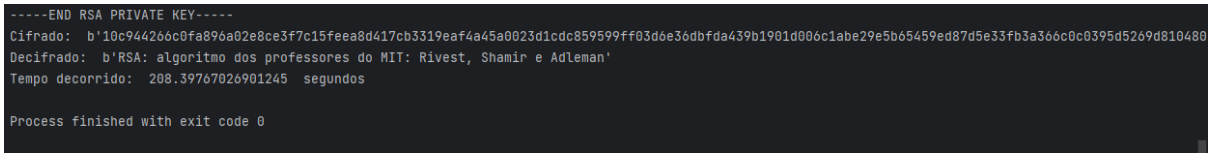
-

-

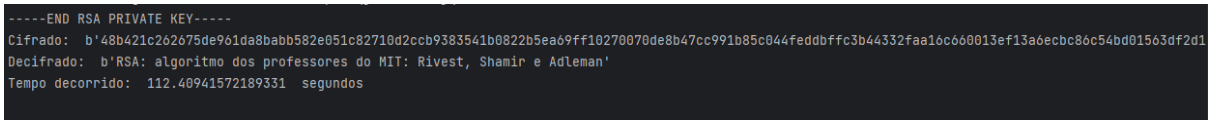
-

Tempo Médio: **11,75 segundos**

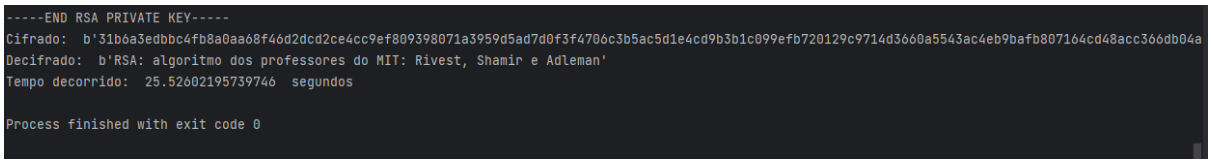
8192 bits ->



-



-



-

-

Tempo Médio: **269,92 segundos**

AES:

128 bits ->

```
Texto a ser cifrado: RSA: algoritmo dos professores do MIT: Rivest, Shamir e Adleman
Senha: 234
Cifrado:
{'cipher_text': 'eicHInioo5WRIfGshsóJTStrCkfxgefwdbVGuZlLZHh31lajWedn+mZe1AJSjGy4aS8UfRYHxg0x91lYa+wr', 'salt': 'b/OPu82vq39j5a8fkV3AvA==', 'nonce': 'rSXOD
Decifrado:
RSA: algoritmo dos professores do MIT: Rivest, Shamir e Adleman
Tempo decorrido:  0.17901253700256348  segundos
```

-

```
"C:\Users\diogo\OneDrive\Documentos\GitHub\WEB-Project\Faculdade\3° Semestre\Segurança da informação\venv\Scripts\python.exe" "C:\Users\diogo\OneDrive\Docu
Cifrado:
{'cipher_text': 'h8XqeSwVkIp9KKeiEvaOb7lxjzHzó29NAcidj0pTCXtucDlvXgbkR4Hrwis24PL0iGNwbElGxkDHVóhmsO4z', 'salt': 'cEzQcNI1Yx/6M7NqóehOaA==', 'nonce': 'PR1Xc
Decifrado:
RSA: algoritmo dos professores do MIT: Rivest, Shamir e Adleman
Tempo decorrido:  0.09800505638122559  segundos

Process finished with exit code 0
```

-

```
"C:\Users\diogo\OneDrive\Documentos\GitHub\WEB-Project\Faculdade\3° Semestre\Segurança da informação\venv\Scripts\python.exe" "C:\Users\diogo\OneDrive\Docu
Cifrado:
{'cipher_text': 'Uhpy8axD01tqDTv1h+W8QEn8Ipt1LoeCiehmJNbóKtXENpse3Eft+vjijRsOQmRO0jUrJ1DWamVmGo2JFv+I', 'salt': 'dSZGNMZfvWVIwONHIYh8hw==', 'nonce': 'j7WBs
Decifrado:
RSA: algoritmo dos professores do MIT: Rivest, Shamir e Adleman
Tempo decorrido:  0.11500835418701172  segundos

Process finished with exit code 0
```

-

```
"C:\Users\diogo\OneDrive\Documentos\GitHub\WEB-Project\Faculdade\3° Semestre\Segurança da informação\venv\Scripts\python.exe" "C:\Users\diogo\OneDrive\Docu
Cifrado:
{'cipher_text': 'N7vGz2ToazP9fLxtGt3+AqRGDv2PSlKPoQPC4MHTUiCjGPU9o3yaVLópkrE1FiohEKpKKCóoWtEqoFNnWYMr', 'salt': 'xYR54MkMFULFYGN3JzbLdQ==', 'nonce': '33Yt
Decifrado:
RSA: algoritmo dos professores do MIT: Rivest, Shamir e Adleman
Tempo decorrido:  0.10849666595458984  segundos

Process finished with exit code 0
```

-

```
"C:\Users\diogo\OneDrive\Documentos\GitHub\WEB-Project\Faculdade\3° Semestre\Segurança da informação\venv\Scripts\python.exe" "C:\Users\diogo\OneDrive\Docu
Cifrado:
{'cipher_text': 'VapcOFypSDX7BHN50DaH4qgmTGst8mPaGXtBox7je72VFDdWIcsjqFfe8/yUVvyt5hAyWxQzd+/iAnLE4x/R', 'salt': '02NSzCFDuEuYónBjrZ95Gg==', 'nonce': '4uBBp
Decifrado:
RSA: algoritmo dos professores do MIT: Rivest, Shamir e Adleman
Tempo decorrido:  0.12700748443603516  segundos

Process finished with exit code 0
```

Tempo Médio: 0,301 segundos

256 bits ->

```
Texto a ser cifrado: RSA: algoritmo dos professores do MIT: Rivest, Shamir e Adleman
Senha: 234
Cifrado:
{'cipher_text': '5PvwbGZn/8Nf/6DnjsvYRvt54e6Em2O8TRmlmqc4xx3LzPPmseq2w0KyNmUbqu+nY1k1Y47eXGp4HAowCFa6', 'salt': 'oRGeVz388tbCQFE65XXd9A==', 'nonce': '7iqny
Erro: A verificação MAC falhou.
Tempo decorrido:  0.15601229667663574  segundos
```

-

```
"C:\Users\diogo\OneDrive\Documentos\GitHub\WEB-Project\Faculdade\3° Semestre\Segurança da informação\venv\Scripts\python.exe" "C:\Users\diogo\OneDrive\
Cifrado:
{'cipher_text': 'd+bFiqfgHpBqIEE4TkVpkuMpim373s8BgqibTdaw27XVBLpObTlUHsSBjIbpupl9AbjYHN4HQk4cfY8A2kbx', 'salt': '2GaHq63mYXXukNNSdiVDbQ==', 'nonce': 'c
Tempo decorrido:  0.10300588607788086  segundos

Process finished with exit code 0
```

-

```
"C:\Users\diogo\OneDrive\Documentos\GitHub\WEB-Project\Faculdade\3° Semestre\Segurança da informação\venv\Scripts\python.exe" "C:\Users\diogo\OneDrive\Docu
Cifrado:
{'cipher_text': 'yjNrUQBt87ceTkTEws8/Pi4GSgKPzVp1S/QJm7EbqRjjZy1GrLBibit0sjHkftWWlXg/2THHnQsiBeSxtJnK', 'salt': 'NSOUG1uZqN6zuldv+jfKOg==', 'nonce': 'cohsU
Tempo decorrido:  0.14300823211669922  segundos

Process finished with exit code 0
```

-

```
"C:\Users\diogo\OneDrive\Documentos\GitHub\WEB-Project\Faculdade\3° Semestre\Segurança da informação\venv\Scripts\python.exe" "C:\Users\diogo\OneDrive\Docu
Cifrado:
{'cipher_text': 'bBPt2nK2ZWZWkW7aqZ7+llxUYR7NXe+LG96a3DJ6QrtMElTuzOKZYDC7Msgjhb/rfQhO8IQslNyK9NBx+GHC', 'salt': 'S2dMvF5MgW2OfuPcLLIcjg==', 'nonce': 'dt71m
Tempo decorrido:  0.08900690078735352  segundos

Process finished with exit code 0
```

-

```
"C:\Users\diogo\OneDrive\Documentos\GitHub\WEB-Project\Faculdade\3° Semestre\Segurança da informação\venv\Scripts\python.exe" "C:\Users\diogo\OneDrive\Do
Cifrado:
{'cipher_text': 'vOoQp/ATZtqppb7kmwjfu+qRC1nLSrAG/q0jlg48eSQyzh5JH1ePigvIoWt9HAaD0jXfXP3YSvLDLMBU65My', 'salt': '4SsO1vDFJi2M3gkQIc/P3g==', 'nonce': '9jL
Tempo decorrido:  0.09600615501403809  segundos

Process finished with exit code 0
```

Tempo Médio: 0,442 segundos

Apresentação dos Requisitos do PC

16 GB de RAM 3200 GHz (2 pentes de 8GB)
AMD Ryzen 5 3200G (8 CORES)
SSD de 1TB