

**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.

- 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)**
- 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:

- 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.
- A atividade pode ser desenvolvida em equipe, porém cada elemento da equipe deverá executar os passos e apresentar o relatório individual.
- 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'04609d88337406aacd64b10c94db317c94cadb3a43eede942eda4a0735d909415b5785e704df46ef254ae69f4034152bf2b050314123a253f45e515f0aa77b2d59db26132ec447
Decifrado: b'RSA: algoritmo dos professores do MIT: Rivest, Shamir e Adleman'
Tempo decorrido: 0.16501116752624512 segundos
```

```
-----END RSA PRIVATE KEY-----
Cifrado: b'405efcc1b89fc5251534ad1dbb064a84061c4852f90cd1dab150f90f56db7316c05abaf14096b0906d3b9d2364102a1ffc4a69a84a8cd656d3f9b9f90b0992b8d9bcfb8d83edb1
Decifrado: b'RSA: algoritmo dos professores do MIT: Rivest, Shamir e Adleman'
Tempo decorrido: 0.16301417350769043 segundos
```

```
-----END RSA PRIVATE KEY-----
Cifrado: b'24561649cb656d3f44cdca1570f1a5ceee99c9588cd7670ba226c090e13b45fc3b94e3464946da85007cb2698c4c6a9facbf8fd729e88380021798df4c356f28e3afb608f5b240
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: 0.12800346183776855 segundos
```

Process finished with exit code 0

```
-----END RSA PRIVATE KEY-----
Cifrado:  b'98859ae96c428df3819847e1d37ff82b5765fca04cdd5af29da4144efba47270f8f5b90bd7b66a8a96e6410199a6b6579c61371de503d33aefa032b5f0d2ecf0f2bef311e729e4d
Decifrado:  b'RSA: algoritmo dos professores do MIT: Rivest, Shamir e Adleman'
Tempo decorrido:  0.2160189151763916  segundos

Process finished with exit code 0
```

Tempo Médio: 0,188 segundos

2048 bits ->

```
-----END RSA PRIVATE KEY-----
Cifrado:  b'4fe84cf323af6dddee316b9dbe56fa0e9104bdfde3fdd27e14e6d6aed9d355941a2d07952b5b2aae548fd0c01dd1ef1ca0329acdc5bce4269cb7fe70cc3a65260f9a47460ad877f9
Decifrado:  b'RSA: algoritmo dos professores do MIT: Rivest, Shamir e Adleman'
Tempo decorrido:  0.6070458889007568  segundos
```

```
-----END RSA PRIVATE KEY-----
Cifrado:  b'7e683ec6dd757c61c48909f7cb4809a1a6491be26ddc999fc2680ed09eefddb954fd356e036e6bb6fdd8eff08c10fd355ba87e5a927a751443c022bf7c65adf4b1e46a2d87f57f4
Decifrado:  b'RSA: algoritmo dos professores do MIT: Rivest, Shamir e Adleman'
Tempo decorrido:  0.45803284645080566  segundos

Process finished with exit code 0
```

```
-----END RSA PRIVATE KEY-----
Cifrado:  b'87d1cb0613ab7515010febcb5b105d7cb272b9b1ccd0a362ad5271e1d7476338231d2660b9b6e8df94d9d7dee046ca2541cab499dfba679cfd3a2658b6ddc14e3af8e78d884cb0a
Decifrado:  b'RSA: algoritmo dos professores do MIT: Rivest, Shamir e Adleman'
Tempo decorrido:  1.7001261711120605  segundos

Process finished with exit code 0
```

```
-----END RSA PRIVATE KEY-----
Cifrado:  b'ce55e35ef7114903663cc82e72c7fd8b461444b5338e5b9e4442b5b6fa39037a9e0d913017f987f789c6b1bb6eef350cc30482d7df29ff399c8f1aef0ceb1d3e6dac7ed9aa2737
Decifrado:  b'RSA: algoritmo dos professores do MIT: Rivest, Shamir e Adleman'
Tempo decorrido:  0.6646816730499268  segundos

Process finished with exit code 0
```

```
-----END RSA PRIVATE KEY-----
Cifrado:  b'501d45cce1b64606b10eb70cbe500b0a05ca53b28572b5ce2d2e2c37bf8e95360304b049ce14a82df590532f759fb68310de7b5ee73ef2e95bdde20446f7e7dca0abb7a31718fc2
Decifrado:  b'RSA: algoritmo dos professores do MIT: Rivest, Shamir e Adleman'
Tempo decorrido:  1.6931254863739014  segundos
```

Tempo Médio: 1,02 segundos

4096 bits ->

```
-----END RSA PRIVATE KEY-----
Cifrado:  b'737d81744cb2788e7f27baf49674322d150fb196c4c609e4eb0cae9106ff5c8d07d8e235c5baf713073ed16e6e5140264ff295c2d432317aa200c3d4f94076813c1ecaf1c1b2071
Decifrado:  b'RSA: algoritmo dos professores do MIT: Rivest, Shamir e Adleman'
Tempo decorrido:  5.986441612243652  segundos
```

```
-----END RSA PRIVATE KEY-----
Cifrado:  b'8dd2b0ce9cd7d3310ccfe945aa15e8dc934bb62cd91ad5c218ff422e39692c75f22d7dabde5ec62d8a00b952f61c206812e304a54ccf80fcabf7425e410a081f1e0dd70a07fd00b
Decifrado:  b'RSA: algoritmo dos professores do MIT: Rivest, Shamir e Adleman'
Tempo decorrido:  3.908287286758423  segundos

Process finished with exit code 0
```

```
-----END RSA PRIVATE KEY-----
Cifrado:  b'958cca8fa7b3bd5b42b6c0032a2889ee297d7fcc2130a46f70aff296d8f2c3be776e98bb6ecef774c873403997bcdcc76caa134380d502c89f6fd7cfe77afa965bb85709b8
Decifrado:  b'RSA: algoritmo dos professores do MIT: Rivest, Shamir e Adleman'
Tempo decorrido:  15.519020318984985  segundos

Process finished with exit code 0
```

```
-----END RSA PRIVATE KEY-----
Cifrado:  b'4667c1f414fe8249353905676eae1f2f454c94e0fac22f18f2f65b025e2560f58352fe97bb86d09e95d6859d5ac595f5610ca493308d28016fa0482f9a7dbd32c5eb18af5fa5946
Decifrado: b'RSA: algoritmo dos professores do MIT: Rivest, Shamir e Adleman'
Tempo decorrido:  10.418759107589722  segundos

Process finished with exit code 0
```

```
-----END RSA PRIVATE KEY-----
Cifrado:  b'249834f333d3dea08ad30d69325f6705ad15d65d03f19723f4ddbed6e596ed18dd6bb794cda177c14ef9e74758b17efda2c755a61a7ca709160bc6d0543ec070743cf68154b0b8d
Decifrado: b'RSA: algoritmo dos professores do MIT: Rivest, Shamir e Adleman'
Tempo decorrido:  14.970106363296509  segundos
```

Tempo Médio: 11,75 segundos

8192 bits ->

```
-----END RSA PRIVATE KEY-----
Cifrado:  b'10c9442660fa896a02e8ce3f7c15fee8d417cb3319eaf4a45a0023d1cdc859599ff03d6e36dbfda439b1901d006c1abe29e5b65459ed87d5e33fb3a366c0c0395d5269d810480
Decifrado: b'RSA: algoritmo dos professores do MIT: Rivest, Shamir e Adleman'
Tempo decorrido:  208.39767026901245  segundos

Process finished with exit code 0
```

```
-----END RSA PRIVATE KEY-----
Cifrado:  b'48b421c262675de961da8babb582e051c82710d2ccb9383541b0822b5ea69ff10270070de8b47cc991b85c044feddbffc3b44332faa16c660013ef13a6ecbc86c54bd01563df2d1
Decifrado: b'RSA: algoritmo dos professores do MIT: Rivest, Shamir e Adleman'
Tempo decorrido:  112.40941572189331  segundos
```

```
-----END RSA PRIVATE KEY-----
Cifrado:  b'31b6a3edbbcb4fb8a0aa68f46d2dcd2ce4cc9ef809398071a3959d5ad7d0f3f4706c3b5ac5d1e4cd9b3b1c099efb720129c9714d3660a5543ac4eb9bafb807164cd48acc366db04a
Decifrado: b'RSA: algoritmo dos professores do MIT: Rivest, Shamir e Adleman'
Tempo decorrido:  25.52602195739746  segundos

Process finished with exit code 0
```

```
-----END RSA PRIVATE KEY-----
Cifrado:  b'06a81f40e4ad62a8393c01cb724140962b48ca284434978b3b4ff14d8c6eaa26beb3d3e613b197de9e42f0849f56de202109733744336f9dd2255f353d994415250c9491fe46
Decifrado: b'RSA: algoritmo dos professores do MIT: Rivest, Shamir e Adleman'
Tempo decorrido:  490.3132095336914  segundos

Process finished with exit code 0
```

```
-----END RSA PRIVATE KEY-----
Cifrado:  b'9b130e04842a032f5c244458ca5b2ac5d882a04cebc2ae7b2c21c6cb4c3c180c8ea6b4aea190b9ef370578fe3e8d13877603a268beba6e378246118580a4777d87509ebf8887463
Decifrado: b'RSA: algoritmo dos professores do MIT: Rivest, Shamir e Adleman'
Tempo decorrido:  504.98035311698914  segundos

Process finished with exit code 0
```

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': 'eicHiInoo5WRIf6shs6JTStrCkfxgefwdbVGuZlLZHh31lajWedn+mZe1AJ3j6y4aS8UfRYHxg0x91LYa+wr', 'salt': 'b/0Pu82vq39j5a8fkV3AvA==', 'nonce': 'rsX0D
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\3º Semestre\Segurança da informação\env\Scripts\python.exe" "C:\Users\diogo\OneDrive\Docu
Cifrado:
{'cipher_text': 'h8XqeSwVKIp9KKeiEva0b7LxjzHzo29MAcidj0pTCXtucDlvXgbkR4Hrwis24PL0iGNwbEL6xkDhV6hms04z', 'salt': 'cEzQcNI1Yx/6M7Nq6eh0aA==', '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\3º Semestre\Segurança da informação\env\Scripts\python.exe" "C:\Users\diogo\OneDrive\Docu
Cifrado:
{'cipher_text': 'Uhpy8axD01tqDTv1h+W8QEn8Ipt1LoeCiehmJNb6KtXENpse3Eft+vjijRs0QmR00jUrJ1DwamVmGo2JFv+I', 'salt': 'dSZGNMZfvWVIwONHIVh8hw==', '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\3º Semestre\Segurança da informação\env\Scripts\python.exe" "C:\Users\diogo\OneDrive\Docu
Cifrado:
{'cipher_text': 'N7vGz2ToazP9fLxt6t3+AQrGDv2PSlKPqPC4MHTUicj6PU9o3yaVL6pkrE1FiohEKpKKC6oWtEqoFnnWYMr', '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\3º Semestre\Segurança da informação\env\Scripts\python.exe" "C:\Users\diogo\OneDrive\Docu
Cifrado:
{'cipher_text': 'Vapc0FypSDX7BHN50DaH4qgmT6st8mPaGxtBox7je72VFDDWicsjqFfe8/yUVvyt5hAyWxQzd+/iAnLE4x/R', 'salt': '02NSzcFDuEuY6nBjrZ956g==', 'nonce': '4uBBg
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': '5Pvwb6Zn/8Nf/6DnjsvYRvt54e6Em208TRmlmqc4xx3LzPPmseq2w0KyNmUbqu+nY1klY47eXGp4HA6wCFa6', 'salt': 'oR6eVz388tbCQFE65XXd9A==', 'nonce': '71qny'}
Erro: A verificação MAC falhou.
Tempo decorrido: 0.15601229667663574 segundos
```

```
"C:\Users\diogo\OneDrive\Documentos\GitHub\WEB-Project\Faculdade\3º Semestre\Segurança da informação\venv\Scripts\python.exe" "C:\Users\diogo\OneDrive\Documentos\GitHub\WEB-Project\Faculdade\3º Semestre\Segurança da informação\venv\Scripts\python.exe"
Cifrado:
{'cipher_text': 'd+bFiqfgHpBqIEE4TkVpkuMpim373s8BgqibTdaw27XVBLp0bTLUHSBjIbpupl9AbjYHN4HQk4cfY8A2Kbx', 'salt': '26aHq63mYXXukNNSdiVDQ==', 'nonce': 'c'}
Tempo decorrido: 0.10300588607788086 segundos
```

Process finished with exit code 0

```
"C:\Users\diogo\OneDrive\Documentos\GitHub\WEB-Project\Faculdade\3º Semestre\Segurança da informação\venv\Scripts\python.exe" "C:\Users\diogo\OneDrive\Documentos\GitHub\WEB-Project\Faculdade\3º Semestre\Segurança da informação\venv\Scripts\python.exe"
Cifrado:
{'cipher_text': 'yJNrUQ8t87ceTktEws8/Pi4GSgKPzVp1S/QJm7EbqRjjZy1GrLBibit0sjHkftWWLXg/2THHnQsiBeSxtJnK', 'salt': 'NS0U6IuZqN6zuLdv+jfK0g==', 'nonce': 'cohsU'}
Tempo decorrido: 0.14300823211669922 segundos
```

Process finished with exit code 0

```
"C:\Users\diogo\OneDrive\Documentos\GitHub\WEB-Project\Faculdade\3º Semestre\Segurança da informação\venv\Scripts\python.exe" "C:\Users\diogo\OneDrive\Documentos\GitHub\WEB-Project\Faculdade\3º Semestre\Segurança da informação\venv\Scripts\python.exe"
Cifrado:
{'cipher_text': 'b8Pt2nk2ZWZWKW7aqZ7+llxUYR7NXe+L696a3DJ6QrtMELtuzOKZyDC7Mgshb/rfQh08IQsLnyK9NBx+GHC', 'salt': 'S2dMvF5MgW20fuPcLLicjg==', 'nonce': 'dt71m'}
Tempo decorrido: 0.08900690078735352 segundos
```

Process finished with exit code 0

```
"C:\Users\diogo\OneDrive\Documentos\GitHub\WEB-Project\Faculdade\3º Semestre\Segurança da informação\venv\Scripts\python.exe" "C:\Users\diogo\OneDrive\Documentos\GitHub\WEB-Project\Faculdade\3º Semestre\Segurança da informação\venv\Scripts\python.exe"
Cifrado:
{'cipher_text': 'v0oQp/ATZtqppb7Kmwjfu+qRC1nLSrAG/q0jlg48eSQyZy5JH1ePigvIoWt9HAaD0jXfXP3YSvLDLMBU65My', 'salt': '4Ss01v0F3j2M3gkQIc/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