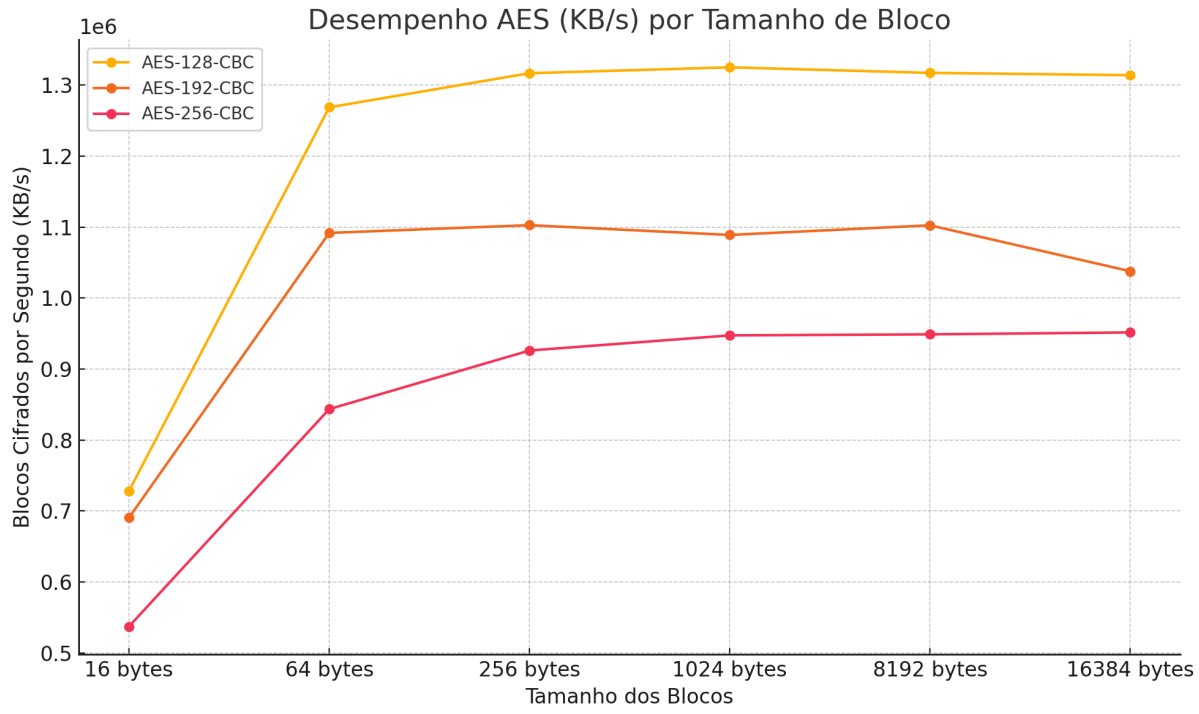
3. Execute o comando "openssl speed aes rsa". Analise os resultados e responda as seguintes perguntas.

```
Prompt de Comando
Doing 7680 bits public rsa encrypt ops for 10s: 43846 7680 bits public RSA encrypt ops in 9.80s
Doing 7680 bits private rsa decrypt ops for 10s: 262 7680 bits private RSA decrypt ops in 9.91s
Doing 15360 bits private rsa sign ops for 10s: 52 15360 bits private RSA sign ops in 9.78s
Doing 15360 bits public rsa verify ops for 10s: 11856 15360 bits public RSA verify ops in 9.78s
Doing 15360 bits public rsa encrypt ops for 10s: 11221 15360 bits public RSA encrypt ops in 9.53s
Doing 15360 bits private rsa decrypt ops for 10s: 53 15360 bits private RSA decrypt ops in 9.75s
version: 3.4.1
built on: Tue Feb 11 22:22:01 2025 UTC
options: bn(64,64)
compiler: cl  /Z7 /Fdossl_static.pdb /Gs0 /GF /Gy /MD /W3 /wd4090 /nologo /O2 -DL_ENDIAN -DOPENSSL_PIC -D"OPENSSL_BUILDI
NG_OPENSSL" -D"OPENSSL_SYS_WIN32" -D"WIN32_LEAN_AND_MEAN" -D"UNICODE" -D"_UNICODE" -D"_CRT_SECURE_NO_DEPRECATE" -D"_WINS
OCK_DEPRECATED_NO_WARNINGS" -D"NDEBUG" -D_WINSOCK_DEPRECATED_NO_WARNINGS -D_WIN32_WINNT=0x0502
CPUINFO: OPENSSL_ia32cap=0xfedaf387ffebffff:0x9c67ab
The 'numbers' are in 1000s of bytes per second processed.
type             16 bytes     64 bytes    256 bytes   1024 bytes   8192 bytes  16384 bytes
aes-128-cbc     728105.35k  1268628.74k  1316690.62k  1324999.72k  1317166.69k  1313906.51k
aes-192-cbc     690473.15k  1091684.67k  1102639.96k  1088829.25k  1102408.63k  1037729.44k
aes-256-cbc     537213.39k   843482.90k   926049.12k   947328.55k   948809.15k   951484.42k
                  sign    verify    encrypt   decrypt   sign/s verify/s  encr./s  decr./s
rsa   512 bits 0.000051s 0.000003s 0.000004s 0.000066s  19797.1 287395.7 237593.9  15109.0
rsa  1024 bits 0.000096s 0.000008s 0.000009s 0.000113s  10435.0 131687.2 116210.5   8816.3
rsa  2048 bits 0.000624s 0.000019s 0.000021s 0.000630s   1602.4  51683.1  48381.1   1587.8
rsa  3072 bits 0.001800s 0.000039s 0.000042s 0.001795s    555.4  25442.7  23621.6    557.0
rsa  4096 bits 0.004062s 0.000066s 0.000068s 0.004082s    246.2  15118.8  14694.9    245.0
rsa  7680 bits 0.037842s 0.000215s 0.000223s 0.037810s     26.4   4645.4   4475.5     26.4
rsa 15360 bits 0.188101s 0.000825s 0.000849s 0.183962s      5.3   1212.1   1177.3      5.4

C:\Users\jotam\Documents\GitHub\Information-security\pratica\TP6>
```

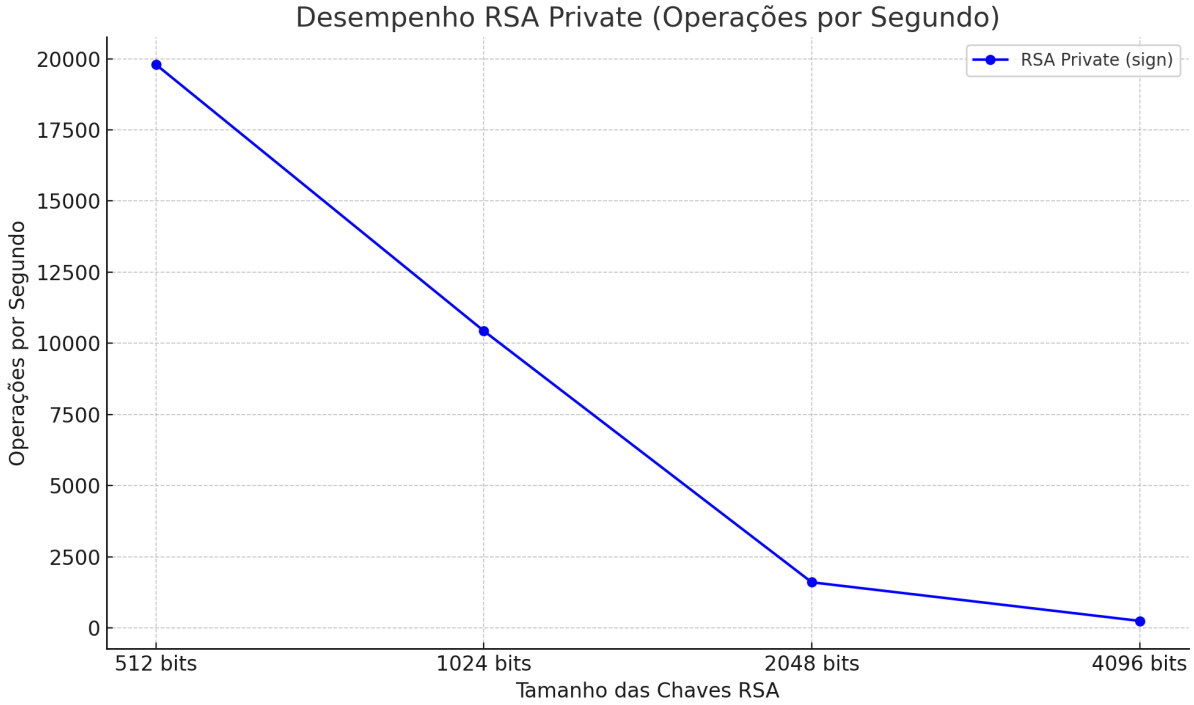
a) Faça um gráfico que associe a quantidade e o tamanho de blocos cifrados por segundo para cada versão do AES (128, 192 e 256). Com o auxílio do gráfico discuta as diferenças entre cada uma das versões do AES.



O gráfico mostra que o desempenho do AES-128 é superior, seguido pelo AES-192 e, por último, o AES-256. Isso ocorre devido ao tamanho da chave: quanto maior a chave (mais segura), menor é a taxa de blocos cifrados por

segundo, já que exige mais cálculos. Observa-se também que o desempenho melhora com o aumento do tamanho dos blocos até se estabilizar próximo aos blocos maiores (1024 bytes em diante).

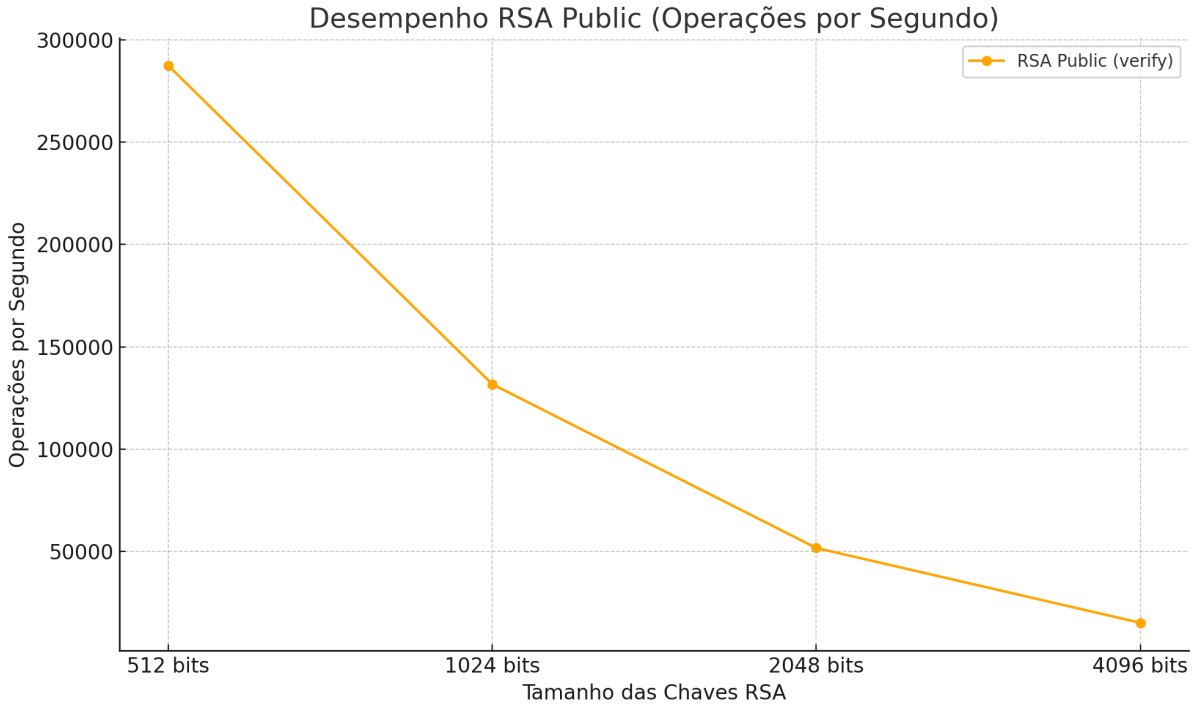
b) Faça um gráfico que associe a quantidade e o tamanho de blocos cifrados por segundo para cada versão do RSA (512, 1024, 2048 e 4096). Considere somente o "private", ou seja, o processo de cifrar um arquivo com a chave privada. Com o auxílio do gráfico discuta as diferenças entre cada uma das versões do RSA.



No gráfico da cifragem RSA com chave privada, fica claro que o desempenho cai drasticamente conforme aumenta o tamanho da chave. Chaves menores, como 512 bits e 1024 bits, possuem taxas muito mais altas comparadas às chaves maiores (2048 e 4096 bits). Isso acontece porque a complexidade matemática é crescente com o aumento do tamanho da chave RSA.

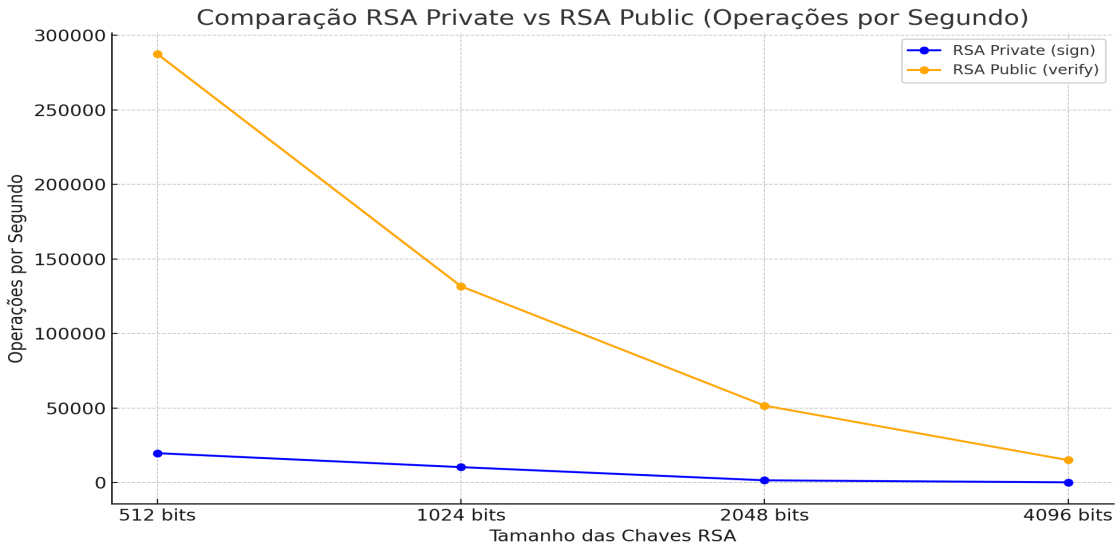
c) Faça um gráfico que associe a quantidade e o tamanho de blocos cifrados por segundo para cada versão do RSA (512, 1024, 2048 e 4096). Considere somente o "public", ou seja, o processo de cifrar um arquivo com a chave pública. Com o

auxílio do gráfico discuta as diferenças entre cada uma das versões do RSA.



Para a cifragem RSA usando a chave pública, o gráfico mostra que as taxas de operações por segundo são bem mais altas do que quando usamos a chave privada. Isso acontece porque, no RSA, a operação com a chave pública (como a cifragem ou verificação de assinatura) utiliza um expoente pequeno, o que torna os cálculos muito mais rápidos. Já a operação com a chave privada (como assinatura ou decifragem) usa um expoente maior, o que exige muito mais processamento. Ao observar o gráfico, dá pra ver que quanto maior o tamanho da chave RSA, menor o desempenho da operação com a chave pública. Por exemplo, a versão de 512 bits realiza as operações com muito mais velocidade do que a de 4096 bits. Isso acontece porque o número de bits influencia diretamente na complexidade dos cálculos matemáticos realizados. Quanto maior a chave, maior a segurança mas também maior o tempo necessário pra completar a operação.
Ou seja, há um equilíbrio entre segurança e desempenho: chaves menores são mais rápidas, mas menos seguras; chaves maiores são mais seguras, mas mais lentas. É por isso que, na prática, se escolhe o tamanho da chave com base no nível de segurança necessário para cada aplicação.

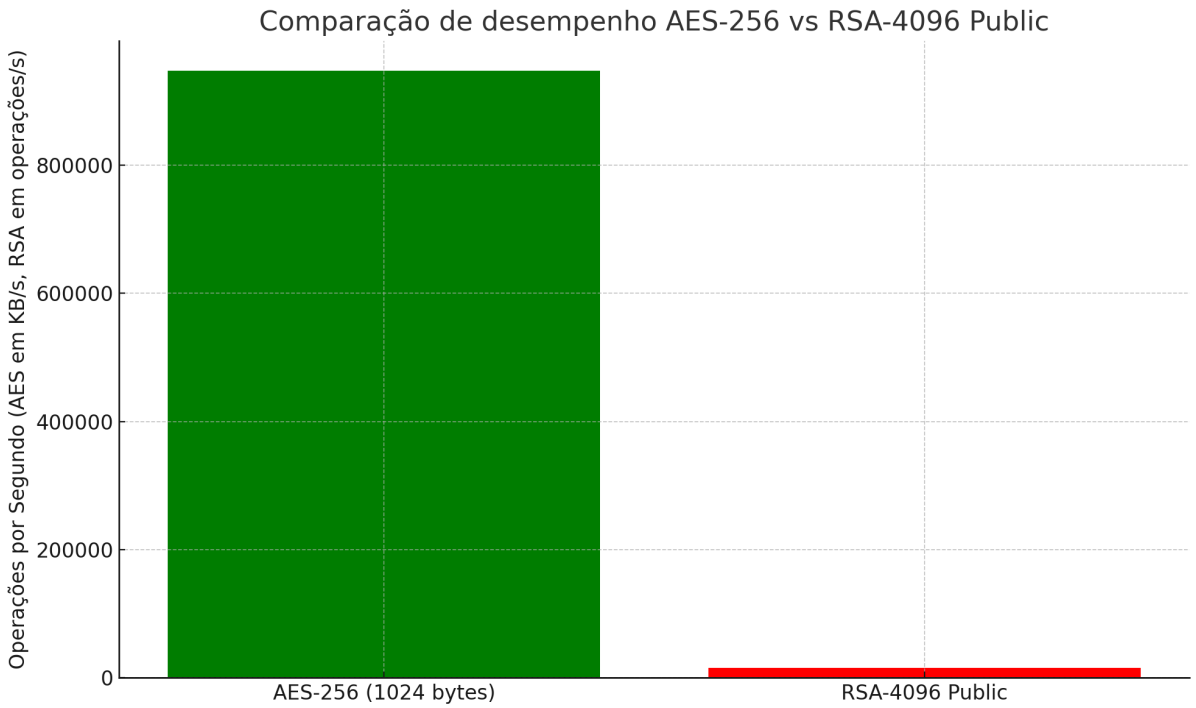
d) Compare os resultados obtidos nas letras b) e c) e discuta/justifique eventuais diferenças/semelhanças entre os processos de cifragens.



Quando a gente compara o RSA usando a chave privada com o RSA usando a chave pública, dá pra perceber que as operações com a chave pública são muito mais rápidas. Isso acontece porque, no RSA, a operação com a chave privada (que é usada pra assinar ou decifrar) envolve cálculos matemáticos bem mais pesados, como a exponenciação modular com um expoente grande. Já as operações com a chave pública (usadas pra verificar a assinatura ou cifrar) são mais simples e usam um expoente menor, por isso são muito mais rápidas.

Essa diferença de desempenho é importante porque mostra como o RSA foi pensado: garantir segurança mesmo que isso signifique sacrificar desempenho em algumas partes. É por isso também que, em sistemas reais, a assinatura digital (que usa a chave privada) é feita só quando realmente precisa, e as partes mais pesadas do processamento são deixadas para os momentos certos.

e) Compare os resultados obtidos nas letras a), b) e c), ou seja, o desempenho do AES é realmente melhor do que o do RSA? Escolha um caso para facilitar a comparação - AES-256 para blocos de 1024 bytes x RSA de 4096 bits no modo "public".



Na comparação direta entre AES-256 e RSA-4096 no modo público, fica evidente uma enorme superioridade do desempenho do AES. O AES é um algoritmo simétrico, projetado especificamente para alta velocidade e eficiência na cifragem de grandes volumes de dados, enquanto o RSA, sendo um algoritmo assimétrico, envolve operações matemáticas mais complexas e lentas. Por causa dessa diferença de desempenho e das propriedades de cada tipo de criptografia, os sistemas modernos de segurança geralmente utilizam uma abordagem híbrida. Inicialmente, usa-se algoritmos assimétricos (como RSA) para realizar a troca segura das chaves simétricas, garantindo a confidencialidade inicial da comunicação. Após a criação de um canal seguro, as mensagens seguintes são cifradas utilizando algoritmos simétricos (como AES), aproveitando sua alta performance e eficiência para lidar com grandes quantidades de dados. Essa abordagem combina o melhor dos dois métodos: segurança robusta na troca de chaves com a agilidade e eficiência no fluxo contínuo dos dados cifrados.Respondi isso na prova também na questão 3 kkkk