Nome: Gustavo Hammerschmidt.

RSA:

Chave pública 1024 bits: teste1: 705ms; teste2: 969ms; teste3: 714ms; média: 796ms.

Chave privada 1024 bits: teste1: 1265ms; teste2: 966ms; teste3: 832ms; média: 1021ms.

Chave pública 2048 bits: teste1: 2870ms; teste2: 1006ms; teste3: 1196ms; média: 1690ms.

Chave privada 2048 bits: teste1: 1537ms; teste2: 2002ms; teste3: 1136ms; média: 1558ms.

Chave pública 4096bits: teste1: 2579ms; teste2: 5240ms; teste3: 3172ms; média: 3663ms.

Chave privada 4096 bits: teste1: 2617ms; teste2: 4279ms; teste3: 2205ms; média: 3033ms.

Chave pública 8192 bits: teste1: 39772ms; teste2: 24058ms; teste3: 28226ms; média: 30685ms.

Chave privada 8192 bits: teste1: 59767ms; teste2: 24344ms; teste3: 11981ms; média: 32030ms.

AES:

Teste1: 489ms; teste2: 586ms; teste3: 708ms; média: 594ms.

RSA (chave de 512 bits):

```
run:
javax.crypto.IllegalBlockSizeException: Data must not be longer than 53 bytes
        at com.sun.crypto.provider.RSACipher.doFinal(RSACipher.java:344)
        at com.sun.crypto.provider.RSACipher.engineDoFinal(RSACipher.java:389)
        at javax.crypto.Cipher.doFinal(Cipher.java:2164)
        at SI_dupla_chave.encrypt(SI_dupla_chave.java:20)
        at SI_dupla_chave.main(SI_dupla_chave.java:70)
java.lang.IllegalArgumentException: Null input buffer
        at javax.crypto.Cipher.doFinal(Cipher.java:2160)
        at SI_dupla_chave.decrypt(SI_dupla_chave.java:34)
        at SI_dupla_chave.main(SI_dupla_chave.java:71)
java.lang.NullPointerException
        at java.lang.String.<init>(String.java:566)
        at SI_dupla_chave.decrypt(SI_dupla_chave.java:40)
        at SI_dupla_chave.main(SI_dupla_chave.java:71)
CONSTRUÍDO COM SUCESSO (tempo total: 1 segundo)
```

O número de caracteres excede o tamanho de bits (53 bytes) possíveis de serem criptografados pela chave 512 bits. O tamanho da chave tem a ver com o tamanho da mensagem.

Relatório: Conforme o número de bits da chave aumenta o tempo para criptografá-la também aumenta. Dependendo da mensagem a ser criptografada e seu tamanho, convém usar chaves com menos bits, pois, assim a relação tempo e execução é amenizada. Portanto, se é necessário usar uma chave com uma maior segurança, terá que se esperar mais tempo para

obter a mensagem criptografada. Não observei, pelos testes, uma diferença significativa de tempo entre as chaves públicas e privadas; exceto pela as chaves de 1024 e 8192 bits, as chaves privadas levaram menos tempo do que as chaves públicas para serem criptografadas. Essa relação de tempo para a mensagem ser criptografada se deve justamente pelo tamanho da mensagem e da chave em que irá criptografá-la.