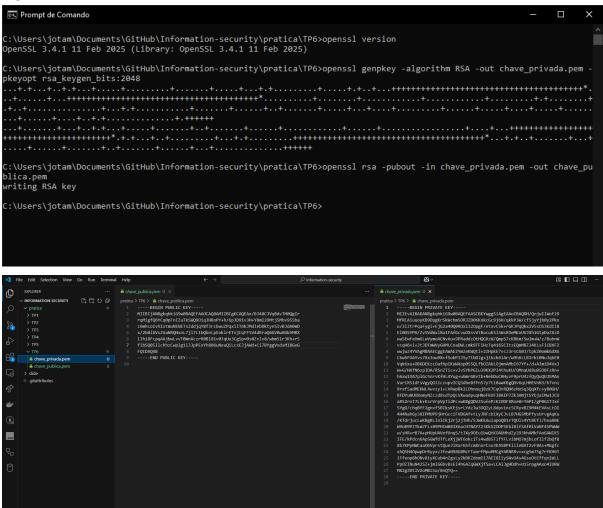
Criptografia assimétrica com o OpenSSL

a) Use o openssI para criar um par de chaves pública/privada para o algoritmo RSA com 2048 bits.



b) Visualize o conteúdo do arquivo referente a chave pública. Qual o valor do par (n,e)?

n (módulo):

```
00:c7:fd:09:e3:c0:89:56:a0:5d:bd:31:f4:42:02:
2b:ae:a3:22:81:f4:38:60:2a:b4:44:59:c8:66:e4:
1c:97:34:6d:3a:ba:96:0c:19:1f:93:f4:71:41:ae:
43:f7:5b:f7:1f:e0:3c:98:8d:82:7d:f9:31:bb:d4:
64:67:5a:cf:af:3b:e8:dd:6d:40:61:7d:df:62:41:
44:34:44:a6:cf:e7:39:a9:5f:5d:e8:7b:1b:c2:e6:
e5:5a:44:cb:92:83:a3:90:9b:5d:39:2d:c4:22:3d:
3b:8c:12:5d:03:49:83:c7:fd:95:55:d5:b1:95:a5:
04:eb:ae:56:cd:ba:a7:37:fd:6a:85:49:b5:9e:54:
44:22:49:6b:11:39:2f:a4:35:49:d6:13:d4:06:b8:
b0:a2:70:dc:19:6e:a3:6d:0b:5d:77:64:1e:03:22:
c3:b3:ad:9d:07:e1:bd:36:1d:b1:39:23:ad:1d:
2e:f3:03:45:f9:ff:69:e9:8e:8d:c3:a2:4b:4e:27:
b5:bd:b2:bd:34:ab:63:bd:ca:87:ea:f9:70:26:
e0:77:f6:6f:eb:3b:9e:2c:03:84:af:e6:69:1e:af:
4f:13:61:f3:4e:ae:35:e8:90:88:7f:31:10:90:
86:15
```

e (expoente público):

65537 (0x10001)

c) Escreva uma mensagem curta para o professor, de até 2047 bits

C:\Users\jotam\Documents\GitHub\Information-security\pratica\TP6>echo Espero que eu passe em Seguranca da Informacao, pr eciso formar rsrs > mensagem.txt

d) Cifre a mensagem criada na letra c) com o RSA usando a chave pública do professor, disponível em "Geral", "Arquivos". Dica:

https://www.openssl.org/docs/man1.1.1/man1/openssl-rsautl.html

C:\Users\jotam\Documents\GitHub\Information-security\pratica\TP6>openssl pkeyutl -encrypt -pubin -inkey chave_publica_pr ofessor.pem -in mensagem.txt -out mensagem_cifrada.bin

e) Anexe o arquivo cifrado. Ou seja, dois arquivos deverão ser anexados: o relatório e a mensagem cifrada com a minha chave pública. Caso não seja possível enviar a mensagem cifrada, envie a mesma para o e-mail: rodrigomiani@gmail.com