Gerando chaves assimétricas com OPENSSL.

Questão 2 da VP2 de Segurança de Informação – Gabriel Bezerra Rodrigues

Uma ferramenta capaz de gerar chaves assimétricas por linha de comando é a OpenSSL,um programa de código aberto que é um toolkit de criptografias, com ele podemos gerar as chaves públicas e privadas, normalmente o mesmo vem instaladojunto com o git no Windows.

Para gerar uma chave privada com ele é bem simples.

basta utilizar o comando:

openssl genrsa -out DIRETORIO | TAMANHO DA CHAVE

tendo como exemplo:

openssl genrsa -out desktop/keyprivada.pem 2048

nisto irá gerar um arquivo .pem contendo uma chave pública na output escolhida, no meu caso, área de trabalho.

Abrindo o mesmo com algum editor de texto, temos aqui a nossa chave privada.

keyprivada.pem

```
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEA0SBMcMor7Evi3QTBJTep44Oi/78nQOCGVhrnlbA1Q11OAIA6
V3n56XFuDHvI9MGkYjHpqih2EB0zLJufOQXQAlhQPgjZ/Sm4B1T9ffk0YcuHhskg
TXs1ct7t9hG/2n54z4UbeWqU62lC6a28G0QoXonun7mAyd5Y1zLKSpKjeGwzLvfT
VKHt9Eo+KkA4xWUfa1CSolXrlkec41BsSldT2EEFq86C3tDFKDpjzd+q5/+OBpUB
05fYKZY5wOTbAD8bwx4QFLVJ6gJYEdL/DJHq+YGMejWsKZAI6bwarHjvdZdO897F
pAVybwtkNMiJakIyBxHMoUnZVjYlIzUEnOYk2QIDAQABAoIBACBmqrFHAasozsuD
sxE7IJ1ZheWuDjzlDKtGm977YCVBzZYSR/fJtEjRBEX239ncLsXwCc4NWs2AWK9u
pSrGlcXnPPd/k5a/4f1w052zAMSuLh9aBiE7F7rmg2P+uAT4V2t/qhQTyWL3+iAO
hPiMhNyw7kHdEfE0+/rLqcAIHD/J69zzNfENP9tx1N227bvL9Ms73XbdcTkL+ySe
S3xIJ++2hQwt1yaa0BUOW49aBr+a/jxLhBX6VVt4H29J1ew4IaDAW3iGxB1OQpm8
vqyyHGT70QorHq2JKLnOT9xNX5iUT2PTSO8dn1DID9koKjWR5kk22FgEYQCa+mqX
E+JVAKECgYEA/XmyN7uZp6Sg9kkWJuf7+MfGzIuH58OIBTS+UtDq9ibay24plVb+
A24PnWrNxACfXX/+ai2MXsM2sDhUuDgYOq7mOucAMSLaezAOn5KxorANOONhZUWW
gWadsiF8ZTlnjdMVdA8ZP9lBw19LwwZ8iDPO0rHPvpz8ZqzHERqNS8UCgYEA0zWF
rG6/VuIMZ88eLwqy59Ti2r6Kcfx3/IOF8eCZSa2bJynBSGHn3erQjUO3imLRpXnJ
dcbcJLGEbKfYD0Q+INeo7U8h2BUzqg4bF0ikmpnS+IZWMmbtuUF93lERuGyYby++
wtKggEcKtYb6S4Ov/COB3ZNirqQmJ2eeJON9ogUCgYBdyX6YwpA7CF4KYsaQhLul
tH2pR2N07NNSYc6eI/EcPQotxUgbmsGIEVwzucYC5NwSo35GWS4cDg0ZLO6j7xV/
+SD04G4gwC2o8QIoJwYVFSD/UJrD9viWTprAw0Ucyx22y0if1cpY5pE/se39blP7
rXe0W9hrRfjaIMnTWUi4pQKBgBfj5PPlLwVv2kFfvyVJC4WHogVmKhjMmvHYGq2K
XyxjU7pxUaiTUnvalK5162ve06HpDa2hycLoxXbY4WqQqIpkenolSkm71DU3FT9j
+yJ1pdRwtY1L8TXUP52HA/8dYXyqJOS6mGcKIh74XpVuFtjpV0Yt5qqkbKBmaw/3
H33VAoGATYTZ/rXBu6FPPWwvEXHaoLhPw/KdBXwvjHWfEMK3RH/IEki5X3gzRXuZ
GBMXO88AmWjKumksQas4ryum/s+SC0kzs+wKT6OINEBiglWoKabGDGWcXWprgFJn
BhTRMes/NBByg8suJhCsilsQt8HlGnutV/favvReUWcKmrk80IA=
-----END RSA PRIVATE KEY-----
```

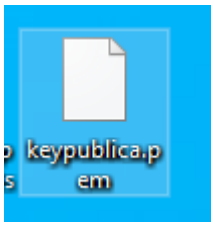
Agora para gerarmos uma chave publica com o openssl, precisaremos da chave privada e usaremos o seguinte comando:

openssl rsa -in localização chave privada -pubout -out diretório de saída chave publica

exemplo:

openssl rsa -in desktop/keyprivada.pem -pubout -out desktop/keypublica.pem

assim gerando o arquivo no local desejado:



E abrindo o mesmo em um editor de texto temos assim nossa chave publica: