

4.

Step 1) Generate a 256 bit (32 byte) random key

openssl rand -base64 32 > key.bin

```
bbr@EME17-G7064PKR:~/Documents/WS02/2_Information_Security_Concepts/Answers/4$ openssl rand -base64 32 > key.bin
bbr@EME17-G7064PKR:~/Documents/WS02/2_Information_Security_Concepts/Answers/4$ cat key.bin
LJKJRg0PWeyV+sANWBGMTpIk8bIMb+MNudG0tHQB/fk=
bbr@EME17-G7064PKR:~/Documents/WS02/2_Information_Security_Concepts/Answers/4$
```

Step 2) Encrypt the key using public key

openssl rsautl -encrypt -inkey public.pem -pubin -in key.bin -out key.bin.enc

```
bbr@EME17-G7064PKR:~/Documents/WS02/2_Information_Security_Concepts/Answers/4$ openssl rsautl -encrypt -inkey public.pem -pubin -in key.bin -out key.bin.enc
bbr@EME17-G7064PKR:~/Documents/WS02/2_Information_Security_Concepts/Answers/4$ cat key.bin.enc
0H
  *H0|000030
    r?+00      000000H_0L;0!F<0S]:W00F0'0{0H0009000B0J0
  0'x0HT0j E000N0U00      0ES0jD0800qdh0#B08-7,BLM0000/G0A0P!0(-A0'0yo
  z0,00u|P080000Z0c000|0;0,00      j100?000H00^0-0K000000'K60^00-00L,{0q0v02^Z000Ch000000ssqC000x00j0
  00p07C+70000y0 0
  0:0K0D000/000000nf08;Xq/L^00IP\000000000008
                                )cnS00000d0000MS;0b+00E07D0
```

Step 3) Encrypt the PDF using random key

openssl enc -aes-256-cbc -salt -in nistspecialpublication800-100.pdf -out nistspecialpublication800-100.pdf.enc -pass file:./key.bin

```
bbr@EME17-G7064PKR:~/Documents/WS02/2_Information_Security_Concepts/Answers/4$ openssl enc -aes-256-cbc -salt -in nistspecialpub
lication800-100.pdf -out nistspecialpublication800-100.pdf.enc -pass file:./key.bin
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
bbr@EME17-G7064PKR:~/Documents/WS02/2_Information_Security_Concepts/Answers/4$
```