4.

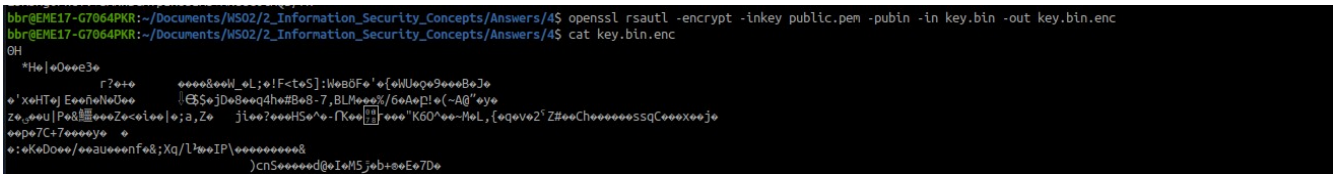
Step 1) Generate a 256 bit (32 byte) random key

openssl rand -base64 32 > key.bin

```
bbr@EME17-G7064PKR:~/Documents/WSO2/2_Information_Security_Concepts/Answers/4$ openssl rand -base64 32 > key.bin
bbr@EME17-G7064PKR:~/Documents/WSO2/2_Information_Security_Concepts/Answers/4$ cat key.bin
LJKJRg0PWeYV+sANWBGMTpIk8bIMb+MNudG0tHQB/fk=
bbr@EME17-G7064PKR:~/Documents/WSO2/2_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



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/WSO2/2_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.
```