

## Assignment Name: Introduction to Information Security Concepts

Execute following command with AES 256 encryption algorithm and SHA 256 message digest.

```
openssl enc -aes-256-cbc -in nistspecialpublication800-100.pdf -out  
nistspecialpublication800-100.pdf.enc -p -md sha256
```

Pass the password as wso2training as input to above command.

```
bbr@EME17-G7064PKR:~/Documents/WS02/2. Introduction to Information Security Concepts$ openssl enc -aes-256-cbc -in  
nistspecialpublication800-100.pdf -out nistspecialpublication800-100.pdf.enc -p -md sha256  
enter aes-256-cbc encryption password:  
Verifying - enter aes-256-cbc encryption password:  
*** WARNING : deprecated key derivation used.  
Using -iter or -pbkdf2 would be better.  
salt=4A75B30ECE3B9EED  
key=2D924384C44B575CB182FF799F78D51E82437005EC21929AC7D52F0E2E44896C  
iv =9B977288D51D5784225F3F68CF5CA9DE
```