1. Launch any ec2 server configure aws cli and login using secret key and access key
2. Open kms in console
3. Customer managed keys
4. Create key 🡪 symmetric
5. Advanced options 🡪 external 🡪 check check box 🡪 next
6. Alias🡪 shubh\_key 🡪 next
7. Select key admin 🡪 next
8. Define key usage permission 🡪 select user 🡪 next
9. Finish 🡪 select: RSAES……….1: download wrapping key and import token
10. Set key material expires date if you want
11. Create any empty folder in your local machine and copy downloaded zip folder in that folder
12. Extract here
13. Open git bash here in same folder
14. Run following command to get plain\_text\_key.bin

openssl rand -out plain\_text\_aes\_key.bin 32

1. Run following command by replacing wrapping key name

openssl rsautl -encrypt \

-in plain\_text\_aes\_key.bin \

-oaep \

-inkey wrappingKey\_206d798f-c32e-47e6-a91d-e84c38a249d9\_05152109\

-pubin \

-keyform DER \

-out enc.aes.key

enc.aes.key file will get created in same folder

1. Go to console 🡪 wrapped key material: enc.aes.key
2. Import token: importToken\_725b92f7-4e3f-4a50-ab57-16f0d4227123\_05152018
3. Go to server and run following command

openssl rand -out plaintext.bin 32

aws kms encrypt --key-id alias/dom\_key --plaintext fileb://plaintext.bin

aws kms encrypt --key-id alias/dom\_key --plaintext fileb://file\_name.txt --query CiphertextBlob --output text | base64 -d > encrypted.txt

1. Now you may delete your original file
2. Do decrypt run following command

aws kms decrypt --ciphertext-blob fileb://encrypted.txt --query Plaintext --output text | base64 -d > decrypted.txt