Practical.no - 6

Title - Generate Digital Signature and verify it using DSA / RSA / ECC.

```
from Crypto.PublicKey import DSA
from Crypto.Signature import DSS
from Crypto.Hash import SHA256

#Create a new DSA key
key = DSA.generate(2048)
f = open("public_key.pem","wb")
f.write(key.publickey().export_key())
f.close()

#Sign a message
message = b"Hello"
hash_obj = SHA256.new(message)
signer = DSS.new(key,'fips-186-3')
signature = signer.sign(hash_obj)

#Load the public key
f = open("public_key.pem","rb")
hash_obj = SHA256.new(message)
pub_key = DSA.import_key(f.read())
verifier = DSS.new(pub_key,'fips-186-3')

#Verify the authenticity of the message
try:
    verifier.verify(hash_obj,signature)
    print("The message is Authentic.")
except ValueError:
    print("The message is not Authentic.")
```

Output:

```
The message is Authentic.
```