Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 61
INS Practical 10

Aim : Consider a scenario where in a company two employee wants to authenticate them self as legitimate entity. Provide a solution for authentication of two parties through digital signature.

Code :

```
from prettytable import PrettyTable
from hashlib import sha1
import YSL_io as ysl

def generate_publickey(g, p, x):
    y = (g**x) % p
    return y


def generate_signature(g, p, q, M, k, x):
    r = ((g**k) % p) % q
    k_inv = modInverse(k, q)
    s = (int((int(M) + int(x) * int(r))) * int(k_inv)) % q
    return (r, s)


def modInverse(b, n):
    for z in range(0, n):
        if ((b * z) % n) == 1:
            return z


def signatureVerify(s, r, p, q, M, g, y):
    w = (modInverse(s, q)) % q
    u1 = (w * M) % q
    u2 = (w * r) % q
    v = (((g**u1) * (y**u2)) % p) % q
```

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 61
INS Practical 10

```
    return u1, u2, v


# p = 303287
# q = 151643
# g = 252
p = 283
q = 47
g = 60


message = ysl.inputGRN("\nEnter the Message : ")
text = message
text = int(sha1(text.encode()).hexdigest(), 16)

r = 0
s = 0
key = int(ysl.inputBLU("Enter the Key : "))

xr = key % q
k1 = 43
k = k1 % q
y = generate_publickey(g, p, xr)
sig = generate_signature(g, p, q, text, k, xr)
r = int(sig[0])
s = int(sig[1])
u1, u2, v = signatureVerify(s, r, p, q, text, g, y)

tab = PrettyTable()
tab.field_names = ["Variable", "value"]
tab.add_rows(
    [
        ["Message(M)", message],
```

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 61
INS Practical 10

```
        ["Hex value ", text],
        ["Key", key],
        ["p", p],
        ["q", q],
        ["g", q],
        ["k", k1],
        ["Public Key(y)", y],
        ["Signature ", sig],
    ]
)

tab2 = PrettyTable()
tab2.field_names = ["Variable", "Value"]
tab2.add_rows(
    [["Signature ", sig], ["r", r], ["s", s], ["u1", u1], ["u2", u2], ["v",
v]]
)
ysl.printMGNTA("\n------------------------------- Sender Side
-----------------------------------")
ysl.printORNG(tab)
ysl.printMGNTA("\n------------------------------- Receiver Side
-----------------------------------")
ysl.printBLU(tab2)
if v == r:
    ysl.printMGNTA('\n------------------------------- Signature
Verification -----------------------------------')
    ysl.printGRN("\n\t\t\t\t\u2713 SIGNATURE IS VALID")
else:
    ysl.printMGNTA('\n------------------------------- Signature
Verification -----------------------------------')
    ysl.printRED("\n\t\t\t\t\u2717 SIGNATURE IS INVALID")
```

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 61
INS Practical 10

Output :